CONCESSION CONTRACT

CONTRACT REGARDING A CONCESSION FOR THE PROVISION OF CONNECTIVITY SERVICES TO ACCESS THE EUROSYSTEM SINGLE MARKET INFRASTRUCTURE GATEWAY

between

THE EUROSYSTEM

and

S.W.I.F.T. SCRL

Table of Contents

This Contract regarding a Concession for the Provision of Connectivity Services for the European Single Market Infrastructure Gateway (the "**Contract**") was entered into between

(1) **the Eurosystem Central Banks**, represented by **the Banca d'Italia,** with registered offices at Via Nazionale, 91, 00184 Roma, (hereinafter the "**Eurosystem**")

and

(2) **S.W.I.F.T SCRL**, (VAT no. BE 0413330856) with registered offices at Avenue Adele, 1 - 1310 La Hulpe Belgium (hereinafter the "**Network Service Provider**")

The Eurosystem and the Network Service Provider are hereinafter together referred to as the "**Parties**" and individually as a "**Party**".

WHEREAS

A) The Eurosystem Single Market Infrastructure Gateway (ESMIG) is a technical component delivered as part of the T2-T2S Consolidation project that shall consolidate the access to all market infrastructures that the Eurosystem provides. Via the ESMIG a market participant can use the same technical setup for accessing T2, T2S, TIPS, ECMS and potentially other market infrastructure services and applications.

B) In its meeting on 23/24 April 2018 the Market Infrastructure Board decided that the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d'Italia (hereinafter the '4CB') would make necessary preparations to have up to three network service providers to provide connectivity services to the ESMIG and that the Banca d'Italia would lead the selection procedure.

C) In its meeting on the 23/24 April the Market Infrastructure Board decided that the Banca d'Italia would act as the operating arm of the Eurosystem for the selection procedure. It also decided that the Market Infrastructure Board would be responsible for designating the selection panel members since the Eurosystem central banks would be responsible and liable for the selection criteria and for the outcome of the selection panel's decision based on the selection criteria. The Banca d'Italia would be responsible for correctly conducting the selection procedure and its specific liability related to the selection procedure would be separate from the liability assumed by the 4CB under the Level 2-Level 3 agreement.

D) The purpose of the selection procedure is to entrust network service providers to provide a set of predefined connectivity services, on the basis of which the ESMIG network service

providers design, implement, deliver and operate connectivity solutions intended to securely exchange business information between the market participants connected via them and the Eurosystem market infrastructures via the ESMIG.

E) The selection procedure for ESMIG network service providers falls under the scope of Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts[1] as implemented in the mandated Central Bank's national law.

F) Banca d'Italia has been appointed by the Governing Council to carry out the selection procedure for the network service providers.

G) Banca d'Italia had accepted the appointment and has confirmed its willingness to act in accordance with this Decision.

H) Acting on behalf of the Eurosystem, the Banca d'Italia, on the basis of the Decision ECB/2019/2, has conducted a procedure governed by the Italian law for the selection of the provider of Connectivity Services between the European Single Market Infrastructure Gateway (ESMIG) and the Directly Connected Actors (Di.Co.A.). On the basis of said Decision, the Banca d'Italia has also been authorised to enter into this Contract with the Network Service Provider(s) in the name and interest of the Eurosystem. The Network Service Provider(s) selected by the Banca d'Italia shall compete among each other to provide their Connectivity Services to the Di.Co.A.

I) Taking into account the systemic relevance of the European market infrastructure services and applications, the Network Service Provider(s) might be subject to the oversight by a Competent Authority as a consequence of the provision of the Connectivity Services on the basis of this Contract.

NOW THEREFORE THE PARTIES AGREE AS FOLLOWS

Article 1
Defined Terms and Construction

1.1 Defined Terms. As used herein, the following terms shall have the meaning ascribed to them in the Articles set forth next to such term below:

4CB has the meaning set out in Recital B;

[1] OJ L 94, 28.3.2014, p. 1–64.

4CB Hosting has the meaning set out in Article 5.1;

Attachment has the meaning set out in Article 1.2;

Archival Information has the meaning set out in Article 10.1;

Awarding Rules means the awarding rules for the public procurement procedure conducted by the Banca d'Italia for the selection of the Network Service Providers;

Business Requirements has the meaning set out in Article 3.3(c);

Central Bank or **CB** means the ECB or any national central bank of any Member State of the European Economic Area or of Switzerland or any other national central bank that makes its currency available for central bank money settlement in the ESMIG Services;

Change has the meaning set out in Article 9.2;

Change Request has the meaning set out in Article 9.2;

Concession means the right granted to the Network Service Provider by the Eurosystem to design, develop, implement and operate the Network and to provide the Connectivity Services;

Confidential Information has the meaning set out in Article 19.2;

Connection Availability means the availability of the connection of the Di.Co.A. with the ESMIG Services expressed as a percentage and calculated as more specifically described in the Technical Requirements;

Connectivity Services means any or all of the following services: (i) the Physical Connectivity Services, (ii) the Messaging Services, (ii) the Security Services and (iii) the Operational Services, in each case as more specifically described in the Technical Requirements;

Contract has the meaning set out on the first page of this Contract;

Concession Notice means the concession notice published in the Supplement to the Official Journal of the European Union on [*date of publication*] in connection with the procedure for awarding the Concessions;

Contract Year means the one-year period commencing on the Effective Date and any one-year period commencing on an anniversary of the Effective Date;

Data has the meaning set out in Article 10.4;

Data Protection Laws has the meaning set out in Article 10.5;

Data Protection Policy has the meaning set out in Article 10.5;

Delay has the meaning set out in Article 3.2;

Development Phase has the meaning set out in Article 4.1;

Development Reviews has the meaning set out in Article 9.1;

Directly Connected Actor (or Di.Co.A.) means any entity that is authorised to exchange electronic data with a Eurosystem market infrastructure;

Disclosing Party has the meaning set out in Article 19.2;

ECB means the European Central Bank;

Effective Date has the meaning set out in Article 17.1;

Embedded Software means any third-party software used by the Network Service Provider to implement or operate the Network or to provide the Connectivity Services, including any updates, upgrades and new releases thereof;

Escalation Procedure has the meaning set out in Article 22.2;

ECMS is the Eurosystem Collateral Management System;

ESMIG Connectivity Services Agreement has the meaning set out in Article 7.1;

Eurosystem Single Market Infrastructure Gateway (ESMIG) is the single gateway to access the European market infrastructure services and applications;

Feasibility Assessment has the meaning set out in Article 9.3;

Failure has the meaning set out in Article 6.6;

File means a data structure in an XML format containing two or more Messages as more specifically described in the Technical Requirements;

Force Majeure Event has the meaning set out in Article 15.1;

Go-Live Date means the date on which the first Eurosystem market infrastructure starts using the connectivity services;

Hosting Terms and Conditions has the meaning set out in Article 3.3(d);

Implementation Phase has the meaning set out in Article 5.1;

Infringement Claim has the meaning set out in Article 16.3;

Intellectual Property Rights means any (a) patents, patent applications, patent disclosures and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, Internet domain names and registrations and applications for the registration thereof together with all of the goodwill associated therewith; (c) copyrights and copyrightable works (including computer programs and mask works) and registrations and applications thereof; (d) trade secrets, know-how and other proprietary information of a like kind; (e) waivable or assignable rights of publicity, waivable or assignable moral rights; and (f) all other forms of intellectual property, such as data and databases;

Italian Civil Code means the Royal Decree of 16 March 1942, no. 262;

Italian Code of Public Contracts means Legislative Decree of 18 April 2016, no. 50;

Liability Cap has the meaning set out in Article 14.2;

Logical Demarcation means (i) the point of separation of responsibility between the Eurosystem and the Network Service Provider as more specifically described in the Technical Requirements and (ii) the point of separation between the Network Service Provider and the technical infrastructure of a Di.Co.A. as agreed between the Network Service Provider and the Di.Co.A. in the ESMIG Connectivity Services Agreement;

Loss means any loss, including loss of interest, liability, damage, cost and expense, including any cost and expense for the assertion or enforcement of rights and claims;

Mandatory Change has the meaning set out in Article 9.4;

Message is a data structure in an XML format containing an instruction or information with respect to a single securities transaction or position or a single static date item as more specifically described in the Technical Requirements;

Messaging Services means the messaging services more specifically described in the Specifications, in particular in chapter 6 of the Technical Requirements, and shall include the application to application mode (the "**A2A Service**") and the user to application mode (the "**U2A Service**"), each as more specifically described from paragraph 6.1 to the paragraph 6.4 of the Technical Requirements ;

Milestone has the meaning set out in Article 3.1;

Network means the technical infrastructure, including hardware and software, operated

by the Network Service Provider to provide the Connectivity Services to the Directly connected market participants and shall include any interfaces between ESMIG and the Network, on the one hand, and between the Network and the technical infrastructure of the Di.Co.A., on the other hand;

Network Disaster has the meaning set out in Article 11.3;

Network Operational Phase has the meaning set out in Article 6.1;

Network Service Provider or NSP has the meaning set out on the first page of this Contract;

Network Service Providers means the Network Service Providers selected in the context of the procedure for awarding the Concessions conducted by the Banca d'Italia;

Offer means the offer submitted by the Network Service Provider in the selection procedure conducted by the Banca d'Italia for the selection of the Network Service Provider;

Operational Services means the operational services more specifically described in the Specifications, in particular in Section 3 of the Technical Requirements;

Parties has the meaning set out on the first page of this Contract;

Party has the meaning set out on the first page of this Contract;

Physical Connectivity Services means implementing, maintaining and keeping available the Network for the purpose of exchanging Files and Messages between the Di.Co.A., on the one hand, and ESMIG, on the other hand, as more specifically described in the Specifications, in particular Section 4 of the Technical Requirements;

Project Manager has the meaning set out in Article 8.2;

Receiving Party has the meaning set out in Article 19.2;

Recovery Plan has the meaning set out in Article 3.2;

Security Services means the security services more specifically described in the Specifications, in particular in Section 5 of the Technical Requirements;

Service Availability means the availability of the A2A Service and the U2A Service for the purpose of sending and receiving Messages and Files expressed as a percentage and calculated as more specifically described in the Technical Requirements;

Service Desk has the meaning set out in Article 6.3;

Service Levels means the key performance indicators defined in this Contract and the Specifications with respect to Connection Availability and Service Availability and any other service levels defined in the Specifications or the service level agreement to be concluded between the Parties pursuant to Section 3 of the Technical Requirements;

Solution has the meaning set out in Article 4.1;

Specifications has the meaning set out in Article 3.3;

Steering Committee has the meaning set out in Article 8.3;

Subcontractors has the meaning set out in Article 12.2;

Successor Network Service Provider has the meaning set out in Article 17.4;

TARGET2 means Trans-European Automated Real-time Gross Settlement Express Transfer System for the settlement of money transfers within the European Union;

TARGET2-Securities (or "T2S") is the Eurosystem technical platform for settling securities transactions in central bank money;

TIPS means TARGET Instant Payment Settlement, i.e. the Eurosystem settlement service for instant payments in the TARGET2 framework;

TARGET Services means TARGET2-Securities, TARGET2, TIPS;

Target Date has the meaning set out in Article 3.1;

Technical Requirements has the meaning set out in Article 3.3(b);

Technical Solution has the meaning described in the Technical Requirements and Compliance Check (Requirement ID ESMIG.30070);

Transition Period has the meaning set out in Article 17.4;

User Documentation has the meaning set out in Article 6.4.

1.2 List of Attachments. The following annexes (the "**Attachments**") are attached to and form an integral part of this Contract:

Attachment 1	–	Awarding Rules
Attachment 1.1	–	Technical Requirements and Compliance Check
Attachment 1.2	–	Business Requirements
Attachment 1.3	–	Hosting Terms and Conditions
Attachment 1.4	–	Economic Offer (maximum prices)

1.3 Construction.

(a) Unless the context requires otherwise, any reference to this Contract includes this Contract and the Attachments as a whole. Where this Contract refers to provisions of the Attachments, such provisions shall be legally binding upon the Parties as if they were set out in this Contract.

(b) References in this Contract to an Attachment hereto shall, unless the context requires otherwise, be construed as a reference to the Attachment as amended in accordance with this Contract from time to time irrespective of whether the Attachment (as amended) is attached hereto or not.

(c) The headings of the sections and subsections in this Contract are for convenience purposes only and shall not affect the interpretation of any of the provisions hereof.

(d) Words such as "hereof", "herein" or "hereunder" shall, unless the context requires otherwise, refer to this Contract as a whole and not to a specific provision of this Contract. The term "including" shall mean "including, without limitation".

(e) Terms starting with a capital letter shall have the meaning defined in Article 1.1. Terms defined in the singular have a comparable meaning when used in the plural, and vice versa.

(f) Any reference to "applicable law" or "applicable laws" contained in this Contract shall include any statute, code, regulation, directive, ordinance, binding guideline or other legally binding general rule or decree, applicable in any jurisdiction and relating to any matter whatsoever.

(g) For the purpose of this Contract, a "Business Day" shall be any calendar day which is not a Saturday, Sunday or public holiday in Frankfurt am Main, Germany or at the seat of the Network Service Provider.

(h) Any reference in this Contract to a person or entity shall, unless the context requires otherwise, be construed as a reference to that person or entity and any other person for which it is vicariously responsible. This includes without limitation its employees, directors, consultants, counsel and agents.

1.4 **Priority of Documents.** In the event of any conflict or inconsistency between relevant provisions of this Contract and the Attachments hereto, the Contract shall prevail over any relevant provision of the Attachments with the sole exception of the Awarding Rules, which shall prevail over this Contract. In the event of any conflict or inconsistency between relevant provisions of several Attachments to this Contract, the relevant provisions of that Attachment shall prevail which are consistent with (or more precisely reflect) this Contract or the purposes of this Contract.

Article 2

Scope of the Contract; Main Obligations of the Parties

2.1 **Scope of the Contract.** This Contract sets out the rights and obligations of the Parties in relation to the Concession.

2.2 **Main Obligations of the Network Service Provider.** Without prejudice to its other obligations under this Contract, the Network Service Provider shall

(a) timely design, develop and implement the Network;

(b) provide the Connectivity Services to the Di.Co.A. who have entered into an ESMIG Connectivity Services Agreement with the Network Service Provider at terms and conditions which are consistent with the minimum requirements set out in this Contract and in the Specifications;

(c) provide the Connectivity Services to the Eurosystem in accordance with this Contract and the Specifications and to ensure that the Connectivity Services meet the Service Levels;

(d) comply with all laws which are applicable to the subject matter of this Contract.

2.3 **Main Obligations of the Eurosystem.** Without prejudice to its other obligations under this Contract, the Eurosystem shall procure that the 4CB

(a) grant the Network Service Provider access to the ESMIG Services as more specifically described in the Specifications for the purpose of establishing a connection with the ESMIG Services;

(b) permit the Network Service Provider to install and to maintain certain equipment (e.g., routers and VPN devices) at the premises of the 4CB;

(c) provide to the Network Service Provider the technical and operational support as more specifically described in the Specifications.

The Parties agree that the Eurosystem shall have no obligation under this Contract to ensure that the project for the design, development or implementation of ESMIG will be completed or will be completed on time or that the ESMIG Services will be made available to the Di.Co.A.. Accordingly, and without limiting the generality of the foregoing, the Eurosystem shall, except to the extent required by mandatory law, have no liability under or in connection with this Contract towards the Network Service Provider for any Losses incurred as a result of a failure, discontinuation or delay of the project for the design, development or implementation of ESMIG or of any events or circumstances which have a similar effect.

2.4 **Cooperation.** Without prejudice to either Party's obligations under this Contract, the Parties shall cooperate closely and transparently in order to enable each other to perform their respective obligations under this Contract in a timely and orderly manner. Each Party shall perform its obligations and exercise its rights and remedies under this Contract in good faith. Each Party shall, without undue delay, give the other Party notice of any facts, events, circumstances or other information that may reasonably be expected to materially affect its or the other Party's ability to perform its obligations under this Contract.

2.5 **Scope of exclusivity.** The Network Service Provider is aware that the Eurosystem has awarded concessions to provide Connectivity Services to [*number of additional NSPs*] additional Network Service Providers. The Eurosystem may in the future, in its sole discretion, award further concessions to other third parties to provide the Connectivity Services if existing concessions are revoked, withdrawn or declared unlawful, invalid or unenforceable. In any case, the number of Concessions will not exceed three during the term of this Contract.

2.6 **No Remuneration.** The Eurosystem, in its capacity as the owner and operator of the ESMIG Services, shall not be obligated to pay the Network Service Provider, and the

Network Service Provider shall not be entitled to claim or receive, a remuneration or compensation from the Eurosystem for the performance of its obligations under this Contract.

2.7 **Non-discrimination.** In respect of supply contracts which the Network Service Provider enters into with third-party suppliers as part of or in connection with the activities contemplated in this Contract, the Network Service Provider must comply with the principle of non-discrimination on the basis of nationality.

2.8 **Performance Guarantee.** Before the execution by the Parties of this Contract, the Network Service Provider has delivered to the Banca d'Italia, acting in the interest and in the name of the Eurosystem, a guarantee for the compliance by the Network Service Provider with the terms and conditions of the Concession and the timely and orderly performance by the Network Service Provider of its obligations under this Contract including its obligation to pay penalties.

2.9 **No Third-Party Rights.** This Contract is made between the Eurosystem and the Network Service Provider and, except as otherwise expressly provided herein, nothing contained herein shall, or shall be construed to, confer any rights or remedies on any third party. Without limiting the generality of the foregoing, nothing contained in this Contract shall be construed as an agreement for the benefit of third parties or an agreement with protective effect for the benefit of third parties. Except as otherwise expressly provided herein, the Network Service Provider shall have no rights or remedies against the Eurosystem in respect of any act or omission of any third party, in particular a Di.Co.A..

Article 3
Timing and Specifications

3.1 **Timing.** The Network Service Provider agrees to design, develop and implement the Network and the Connectivity Services such that the milestones described in the schedule below (each a "**Milestone**") are reached by the dates set out in the schedule below (each a "**Target Date**"):

	Milestone	**Target Date**
1	Delivery of the written description of the "Technical Solution"	15 Calendar days after the Effective Date
2	Availability of the Network and the Connectivity Services in a 4CB Test Environment (i.e. two sites within one region)	60 Calendar days from the Effective Date

3	Availability of the Network and the Connectivity Services in up to four (at the choice of the Eurosystem) 4CB Test Environments (i.e. four sites within two regions)	120 Calendar days from the Effective Date
4	Successful Completion of the Compliance Check	180 Calendar days from the Effective Date

3.2 **Delays and Recovery Plan.** Without prejudice to any rights or remedies the Eurosystem may have under this Contract or applicable law, failure by the Network Service Provider to reach a Milestone by the respective Target Date or to otherwise meet any timeline agreed between the Parties or set forth in this Contract with respect to the design, development, implementation and making available of the Network and the Connectivity Services (each such failure a "**Delay**") shall not relieve the Network Service Provider of its obligation to design, develop, implement and make available, as the case may be, the Network or the Connectivity Services. In the event of a Delay, the Parties shall, without undue delay, agree and implement a plan to recover any lost time (the "**Recovery Plan**"). The Network Service Provider shall be required to make available any additional resources required to implement the Recovery Plan.

3.3 **Specifications.** Without limitation to the foregoing, and subject to the provisions of this Contract, the Network Service Provider shall design, develop, implement and make available the Network and shall provide the Connectivity Services in accordance with the technical specifications of, and the functional requirements and operational procedures for, the Network and the Connectivity Services more specifically described in the following documentation:

(a) the awarding rules attached hereto as **Attachment 1** (the " **Awarding Rules** ");

(b) the technical requirements attached hereto as **Attachment 1.1** (the "**Technical Requirements and Compliance Check**");

(c) the business requirements attached hereto as **Attachment 1.2** (the "**Business Requirements**");

(d) the hosting terms and conditions attached hereto as **Attachment 1.3** (the "**Hosting Terms and Conditions**");

(e) the economic offer attached hereto as **Attachment 1.4** (the "**Economic Offer (maximum prices)**")

or which are set out in the operations manual and the escalation manual to be agreed between the Parties in accordance with Section 3 of the Technical Requirements and Compliance Check document.

Article 4
Development Phase

4.1 **Development Phase.** The Network Service Provider shall present to the Eurosystem a solution for the Network and the Connectivity Services which complies with the current state of science and technology regarding the speed, functionality, security and resilience of virtual private networks (VPN) and which is scalable and has the features and functionalities and complies with the technical operational and business requirements more specifically described in the Specifications (the "**Solution**"). The Solution must, in particular, provide for a stable and resilient connection of the Network to the unique communication interface of ESMIG. The Eurosystem shall provide the Network Service Provider with the information regarding the unique communication interface of ESMIG which is reasonably required by the Network Service Provider for the design and development of the Solution. The Network Service Provider agrees to cooperate with the Eurosystem to identify best industry practice for increasing, and to agree concrete measures to increase, the stability and resilience of the connection between the Network and the unique communication interface of ESMIG and to include such measures in the Solution. The Solution must also allow for a timely, cost-effective and resilient implementation by the Di.Co.A. For purposes of this Contract, the "**Development Phase**" shall be the period from the Effective Date until the commencement of the Implementation Phase.

4.2 **Description of the Technical Solution.** Without undue delay, but in no event later than ten (15) Calendar Days after the Effective Date, the Network Service Provider shall deliver to the Eurosystem a detailed written description of the Technical Solution.

4.3 **Compliance Check.** In accordance with the milestone table in Article 3, during the development phase, the Network Service Provider shall demonstrate to the Eurosystem that the presented Technical Solution has the features and functionalities and complies with the technical requirements by performing a Compliance Check workflow more specifically described in Section 2 of Attachment 1.1 ("Technical Requirements and Compliance Check").

Article 5

Implementation Phase

5.1 **Implementation Phase.** After the successful completion of the Compliance Check the Network Service Provider shall deliver a plan regarding the final implementation of the technical setup in line with the schedule of the T2-T2S Consolidation project that will be provided by the Eurosystem. The Eurosystem shall be entitled to request changes to the plan, in particular regarding the priorities of any tasks identified therein. Without undue delay after the Plan has been agreed by the Parties, the Network Service Provider shall implement the Technical Solution in accordance with the Implementation Plan and as more specifically described in the Specifications. The Network Service Provider shall, in particular, install certain equipment (more specifically described in the Specifications) in the premises of the 4CB. The Eurosystem agrees to ensure that the 4CB will make their premises available to the Network Service Provider to allow the Network Service Provider to install the aforementioned equipment and to maintain such equipment at such premises during the term of this Contract (the "**4CB Hosting**") in accordance with **Attachment 1.3**. The Network Service Provider agrees to adhere to and comply with the **Hosting Terms and Conditions** set out in **Attachment 1.3**.

5.2 **Testing Environments.** During the term of this Contract the Network Service Provider shall make available the Solution in the testing environments more specifically described in the Specifications, which testing environments allow the Eurosystem to assess whether the Network and the Connectivity Services have the features and functionalities and comply with the technical, operational and business requirements more specifically described in the Specifications and to train the Eurosystem's employees with respect to the use of the Network and the Connectivity Services. The testing environments shall be modified to reflect any change agreed between the Parties.

5.3 **Cooperation during Implementation Phase.** Without prejudice to Article 2.4, the Parties shall cooperate during the Implementation Phase to ensure a stable and resilient implementation of the Network and, in particular, of the connection between the Network and the unique communication interface of ESMIG. For this purpose, the Network Service Provider agrees to meet and consult with the Eurosystem, upon the Eurosystem's request, to identify best industry practice for increasing, and to agree concrete measures to increase, the stability and resilience of the connection between the Network and the unique communication interface of ESMIG, and to implement such measures during the Implementation Phase.

Article 6

Network Operational Phase

6.1 **Network Operational Phase.** Without undue delay after successful completion of the Compliance Check process and in line with the Implementation Plan, the Network Service Provider shall make available the Network and the Connectivity Services in all environments of the ESMIG Services in a manner which allows the Eurosystem and the Di.Co.A. to use the Network and the Connectivity Services for their respective ESMIG Services testing and production activities. For purposes of this Contract, the "**Network Operational Phase**" of the Network and the Connectivity Services shall be the period commencing on the date on which the Eurosystem has notified the Network Service Provider of the successful completion of the Compliance Check and shall end upon the expiration or termination of this Contract.

6.2 **Availability of the Network and the Connectivity Services.** As from the Target Date for Milestone No. 4 (as defined in Article 3.1), the Network Service Provider shall ensure that, except as otherwise agreed by the Parties, the Network and the Connectivity Services are available between the Points of Demarcation 24 hours per day, seven days per week. The availability of the Network and the Connectivity Services shall be measured by the Network Service Provider in accordance with the indicators more specifically described in the Specifications. The Network Service Provider's obligation to ensure the availability of the Network and the Connectivity Services shall be deemed fulfilled if, calculated on a monthly basis, during the Network Operational Phase,

a) the Connection Availability is not less than 99.999%, and

b) the Service Availability is not less than 99.98%.

6.3 **Operational Support; Service Desk.** During the Network Operational Phase, the Network Service Provider shall provide to the Eurosystem and the Di.Co.A. operational support in relation to the use of the Network and the Connectivity Services as more specifically described in the Specifications. Without limiting the generality of the foregoing, the Network Service Provider shall provide the Eurosystem and the Di.Co.A. with remote support in the English language by telephone, e-mail, or facsimile to answer operational questions and to report irregularities within, and Failures of, the Network or the Connectivity Services 24 hours per day, seven days per week as more specifically described in the Technical Requirements (the "**Service Desk**").

6.4 **User Documentation.** The Network Service Provider shall prepare and deliver to the Eurosystem and to the Di.Co.A., at the latest upon the commencement of the Network Operational Phase, a comprehensive written user documentation describing all necessary

procedures, required equipment and options available for Di.Co.A. to use the Network and the Connectivity Services, as well as the features and functionalities of the Network and the Connectivity Services in a clear and transparent manner (the "**User Documentation**" see Section 2.1 of the Business). During the Network Operational Phase, the Network Service Provider shall maintain and keep the User Documentation current and update it to reflect any modifications of the Network and the Connectivity Services, in particular any Changes.

6.5 **Monitoring.** The Network Service Provider shall continuously monitor the performance of the Network and the Connectivity Services, including its connection with the ESMIG Services and the technical infrastructure of the Di.Co.A., and the Connectivity Services 24 hours per day, seven days per week as more specifically described in the Technical Requirements. If the annual volume of transactions or the average daily volume of transactions increases during the operational phase, the Network Service Provider shall adapt the Network or the Connectivity Services in order to ensure that they continue to meet the requirements regarding speed, functionality, security and resilience more specifically described in this Contract and the Specifications.

6.6 **Failures.** In the event of any problem with the Network or the Connectivity Services or any failure of the Network or the Connectivity Services to perform in accordance with the Specifications (each a "**Failure**"), the Network Service Provider shall remedy the Failure within the time period provided for such Failure (depending on its severity) in the Specifications(the "**Failure Resolution Time**"). In the event of any Failure, the Network Service Provider shall further follow the incident management and escalation procedure more specifically described in Section 3.3 of the Technical Requirements. The Network Service Provider shall perform its obligations under this Article 6.6 irrespective of whether the Failure was reported to it by the Eurosystem or a Di.Co.A. or was detected by the Network Service Provider as a result of its monitoring of the Network and the Connectivity Services.

Article 7

ESMIG Connectivity Services Agreements

7.1 **Non-discriminatory Access to the Connectivity Services.** The Network Service Provider shall – on a non-discriminatory basis – grant Di.Co.A. access to the Connectivity Services in order to allow them to have direct access to the ESMIG Services. For this purpose, the Network Service Provider shall offer to Di.Co.A. to enter into agreements regarding the provision of the Connectivity Services (each such agreement a " **ESMIG Connectivity Services Agreement**"). The Network Service Provider shall cooperate in a timely and constructive manner with any Di.Co.A. which have expressed an interest in receiving the Connectivity Services (or any part thereof) to ensure that such Di.Co.A. may

enter into a ESMIG Connectivity Services Agreement and receive the Connectivity Services without undue delay after they have expressed their interest.

7.2 **Terms and Conditions.** The Network Service Provider shall be free to negotiate the terms and conditions of the ESMIG Connectivity Services Agreements with the Di.Co.A., provided that the terms and conditions are clear and transparent, ensure equal treatment of the Di.Co.A., and further provided that each ESMIG Connectivity Services Agreement meets the minimum requirements more specifically described in, and be otherwise consistent with, this Contract (including its Attachments) and the Specifications.

7.3 **Charges.** The Network Service Provider may not, at any time during the term of this Contract, charge the Di.Co.A. fees or charges for the operation of the Network and the provision of the Connectivity Services which are higher than those indicated by the Network Service Provider in the Offer and are set out in **Attachment 1.4** (**Economic Offer (maximum prices)**). The fees and charges payable by the Di.Co.A. must be transparent, as more specifically described in the Business Requirements. In particular the Network Service Provider shall publish the maximum prices set out in **Attachment 1.4** as more specifically described in the Business Requirements. The maximum prices set out in **Attachment 1.4** shall constitute the Network Service Provider's sole and entire compensation regarding the provision of the services more specifically described in **Attachment 1.4** including (1) the provision of any tasks which are incidental to, or inherent in, or are a necessary part of the proper discharge of such services and (2) the procurement, provision, licensing or otherwise making available to the Di.Co.A. of any software, hardware or other equipment which are necessary to enable the Di.Co.A. to receive, and enjoy the full benefit of the Connectivity Services. In order to allow the Eurosystem to monitor the Network Service Provider's compliance with the obligations provided for in this Article 7.3, the Network Service Provider may not prohibit the Di.Co.A. from disclosing to the Eurosystem the fees and charges paid by them for the Connectivity Services. If and to the extent Di.Co.A. require the Network Service Provider to provide any or all of the connectivity Services at higher service levels than those envisaged by this Contract, then the Network Service Provider is not bound by the maximum price specified in its Offer with respect to these Connectivity Services. Services not listed in **Attachment 1.4** are not subject to a maximum price. The NSP should be aware that the Eurosystem shall not be charged for any of the services listed in **Attachment 1.4**, which are required for the provision of the Connectivity Services to ESMIG, according to the Concession Contract and its Attachments. The maximum prices shall therefore also include all the costs incurred by the NSP to deliver the Connectivity Services to ESMIG[2]. For the avoidance of doubt, the maximum prices indicated in

[2] For more detail please refer to **Attachment 1.1** ("**Technical Requirements and Compliance Check**").

Attachment 1.4 for the services C1 to C7 and F1 apply to the data traffic both sent and received by a Di.Co.A.

7.4 **Scope of the maximum prices.** Unless explicitly stated otherwise, the maximum prices shall cover all activities and components that allow a Di.Co.A. to make efficiently and securely use of the Connectivity Services, according to service levels that are equal to those required by the Eurosystem for ESMIG, as described in the Concession Contract and its Attachments, in particular **Attachment 1.1**.

7.5 **Obligations of the NSP in the ESMIG Connectivity Services Agreements.** The NSP shall be obliged to supply, but shall not charge for any other services not included in the below list, but which are necessary for a Di.Co.A. to make efficiently and securely use of the Connectivity Services as further specified in **Attachment 1.1** to the Concession Contract. The NSP shall consider all Connectivity Services and their prices in its area of responsibility. The boundaries of this responsibility between the NSP and ESMIG are defined in the Concession Contract and its attachments, in particular **Attachment 1.1**. The boundaries of responsibility between the NSP and its Di.Co.A., for the purpose of the below pricing list, shall be in the same logical point of the technical infrastructure as the one defined for ESMIG (but on the side of the Di.Co.A.). The maximum prices specified in **Attachment 1.4** shall apply for a connection with a basic bandwidth of 10 Mb/s between any data centres of a Di.Co.A., located in the EEA or Switzerland to the ESMIG data centres, except for items D.1, D.2, E1,E.2, F.1[3], where a basic bandwidth of 1 Mb/s is assumed. All relevant components in the list shall be sized to allow at minimum full utilisation of that basic bandwidth. Should Di.Co.A. require higher service levels for certain services, than the ones specified in the Concession Contract and its Attachments as the basis for the maximum prices, the NSP shall not be bound by the maximum price specified for these services. If a Di.Co.A. shall require a higher basic bandwidth the NSP is only bound by the maximum price for service A.4, B.4, and C.5. In all other cases, the NSP cannot charge higher prices to any Di.Co.A. than the ones specified in this Attachment.

7.6 **Penalties.** If the NSP has charged more than the relevant amounts published as indicated in the list presented below, the NSP shall within one month indemnify the Di.Co.A. at least for the amounts charged above the maximum price, to be increased – as the case may be – with any additional indemnity agreed between the Di.Co.A. and the NSP in their ESMIG Connectivity Services Agreement. In addition, the NSP shall – within the same time frame – pay the same amount to the Eurosystem as a penalty. For each month delay in the payment of the indemnification, the NSP shall pay at least an additional 10% of the indemnification amount, to be increased – as the case may be – with any penalties agreed

[3] **Attachment 1.4 (Economic Offer (maximum prices))**.

between the Di.Co.A. and the Network Service Provider in their ESMIG Connectivity Services Agreement.

7.7 **Licence.** The Network Service Provider shall grant the Di.Co.A. a non-exclusive, royalty-free licence or sub-licence, as the case may be, to use any Intellectual Property Rights in any materials, work results or software, including Embedded Software (in each case, including updates, upgrades, and new releases thereof) required to be used by the Di.Co.A. in order to use, and enjoy the benefit of, the Connectivity Services.

7.8 **Service Availability, Failure Resolution Time.** The ESMIG Connectivity Services Agreements must contain provisions regarding the availability of the Network and the Connectivity Services and the time periods within which Failures of the Network and the Connectivity Services must be remedied which shall be no less favourable to the Di.Co.A. than the provisions regarding Service Availability and Failure Resolution Times contained in this Contract.

7.9 **Liability.** A ESMIG Connectivity Services Agreement may provide, in accordance with and to the extent allowed by the applicable law, that the Network Service Provider's liability shall be limited. However, in no event the Network Service Provider's liability for Losses incurred by an individual Di.Co.A. during any twelve-month period shall be limited: a) to less than 25% of the charges payable to the Network Service Provider for that twelve-month period by that Di.Co.A., if the Losses are due to the Network Service Provider's gross negligence; and b) to less than 2.5% of the charges payable to the Network Service Provider by that Di.Co.A. for that twelve-month period, if the Losses are due to the Network Service Provider's ordinary negligence.

Article 8

Contract Management; Reporting

8.1 **Contract Management Structure.** In order to facilitate the cooperation and communication between the Parties and to ensure the timely and orderly performance by each Party of its obligations hereunder, the Parties have agreed to implement the contract management structure described in this Article 8.

8.2 **Project Managers.** The Eurosystem and the Network Service Provider shall each designate, in accordance with the Specifications, an individual to serve as the other Party's primary contact person with respect to all matters relating to the performance of this Contract (each a "**Project Manager**" and together the "**Project Managers**"). Each Party shall without undue delay notify the other Party of the name and contact details of any individual which it has designated to replace its Project Manager, provided, however, that the Network Service Provider shall not be entitled to replace its Project Manager without

the Eurosystem's express prior consent which consent shall not be unreasonably withheld. The Project Managers shall have the responsibilities that are assigned to them in this Contract or otherwise by the Parties from time to time. The Network Service Provider's Project Manager shall also have the responsibilities set out in Section 3 of the Technical Requirements and Compliance Check attachment.

8.3 **Steering Committee.** Simultaneously with the designation of the Project Managers, as described in Article 8.2, each Party shall nominate at its sole discretion [up to three (3)] senior representatives to a steering committee (the "**Steering Committee**"). The Steering Committee shall meet on a quarterly basis, or more frequently, if so agreed by the Steering Committee itself or by the Parties, and shall be responsible for monitoring the implementation of the Solution and the performance of the Network and the Connectivity Services under this Contract, reviewing the status of any Change Requests and examining issues relating to the development of the Network and the Connectivity Services, including the Development Reviews under Article 9. The Steering Committee shall also have the other responsibilities that are assigned to it in this Contract or otherwise by the Parties from time to time.

8.4 **Regular Reporting.** During the Network Operational Phase, the Network Service Provider shall, on a monthly basis, provide reports to the Eurosystem regarding the performance of the Network and the Connectivity Services as more specifically described in the Specifications. Without prejudice to any reporting requirements defined in the Specifications, the reports shall contain all relevant information regarding the Network and the Connectivity Services, including any problems or Failures reported by the Di.Co.A., the Failure Resolution Times for any Failures reported, and the Service Availability. Upon the Eurosystem's request, but at least once every Contract Year, the Network Service Provider shall provide to the Eurosystem a report including a forecast of the annual volume of traffic and average daily volume of traffic for each remaining Contract Year during the term of this Contract, any changes of the assumptions regarding the annual volume of traffic and the average daily volume of traffic.

8.5 **Ad hoc Reporting.** Without prejudice to its obligations under Article 8.4, the Network Service Provider shall provide to the Eurosystem such other reports or information as the Eurosystem may reasonably request in order to assess the overall performance of the Network and the Connectivity Services or specific incidents which have arisen in connection with the Network or the Connectivity Services. Each such report or information shall be provided by the Network Service Provider within a reasonable time period after the Eurosystem's request taking into consideration the importance and urgency of the subject matter of the report.

Article 9

Development of the Network and the Connectivity Services; Change Management

9.1 **Development Reviews.** Through the Steering Committee, the Parties shall at least once every calendar year review the status of the Network and the Connectivity Services and any future developments of the Network and the Connectivity Services in particular resulting from changes in applicable law, best industry practice or the state of science and technology (the "**Development Reviews**").

9.2 **Change Requests.** Either Party may at any time during the term of this Contract request or propose a modification of the Network or the Connectivity Services (each such modification a "**Change**", and each such request or proposal a "**Change Request**").

The parties agree and acknowledge that the Eurosystem may at any time during the term of this Contract request to the Network Service Provider the provision of the following changes: additional services based on the same message types as those quoted by the concession holder in its economic offer, changes of the protocol primitives and data-center relocation. These changes will be considered as “predefined” changes for the purpose of Article 175 of the Italian Code of Public Contracts.

Any other modification of the Network or the Connectivity Services may be requested or proposed by either Party in accordance with the limits and conditions set out in Article 175 of the Italian Code of Public Contracts. In particular, the Network Service Provider shall make such Change Requests which, in the Network Service Provider's opinion, are necessary or appropriate for the implementation of this Contract, to ensure that, at any time during the term of this Contract, the Network and the Connectivity Services comply with the state of science and technology or in order to generate economic benefits for the Eurosystem or the Di.Co.A. Without limiting the generality of the first sentence of this Article 9.2, the Eurosystem may, in particular, request changes designed to improve the functionality, security and resilience of the ESMIG Services and the security and integrity of the transactions carried out by the Di.Co.A. through ESMIG. The Network Service Provider shall implement any Change in accordance with the timeline agreed by the Parties, it being understood that any Change is to be implemented as soon as reasonably possible.

9.3 **Change Procedure.** Any Change Request shall be submitted and any Change, including the timing of its implementation, shall be agreed by the Parties pursuant to the procedure set forth in this Article 9 and the Technical Requirements. Together with any Change Request submitted by it, the Network Service Provider shall deliver to the Eurosystem a written assessment (the "**Feasibility Assessment**") of:

(a) the technical feasibility of the Change;

(b) the impact of the Change on the Network and the Connectivity Services in terms of operation, use and performance, in particular, on the Service Levels; and

(c) the proposed timing of the implementation of the Change.

Without undue delay after the receipt of a Change Request from the Eurosystem, the Network Service Provider shall deliver to the Eurosystem a Feasibility Assessment (covering the same scope as indicated in lit. a) through c) above) of the Change proposed in such Change Request.

9.4 **Mandatory Changes.** The Network Service Provider shall not be entitled to reject any Change Request which relates to a Change

(a) that is required by applicable law or by a competent government authority;

(b) that was recommended by the Steering Committee as the result of a Development Review or was agreed by the Parties;

(c) the implementation of which is reasonably expected to require less than 40 man-hours or to cost the Network Service Provider less than Euro 5.000 or to otherwise require only minor works or efforts by the Network Service Provider;

(d) that reflects a change in the generally accepted standards in the industry for communications network solutions and network, connectivity and messaging services which the Network Service Provider has implemented in the services it makes generally available to its customers;

(e) that has been requested by more than 60% of the Di.Co.A., which Di.Co.A. together represent more than 60% of the aggregate number of Files or Messages transmitted by using the Connectivity Services during the full twelve (12) calendar months immediately preceding the date on which the Change Request is submitted to the Network Service Provider provided that the Network Service Provider receives adequate compensation for the implementation of such Change under the ESMIG Connectivity Services Agreements (each of the Changes referred to in lit. a) through e) a "**Mandatory Change**");

9.5 **Resources.** The Network Service Provider shall keep adequate resources available during the term of this Contract for the purpose of implementing Changes.

Article 10

Records; Audit Rights; Data Protection

10.1 **Recordkeeping.** Except to the extent prohibited by mandatory applicable law, the Network Service Provider shall retain for a period of minimum six (6) months after the date on which any such information is generated or processed, the information regarding the performance of the Network and the Connectivity Services, in particular the information contained in the transmission logs maintained by the Network Service Provider regarding the Files and Messages exchanged, and for a period of minimum ten (10) years after the date on which such information is generated all security-relevant data regarding the performance of the Network and the Connectivity Services (such information the "**Archival Information**").

10.2 **Delivery of Archival Information.** Except to the extent prohibited by mandatory applicable law, the Network Service Provider shall, upon the Eurosystem's request, make Archival Information available to the Eurosystem, including by providing the Eurosystem with copies of such information.

10.3 **Audits; Access to Information.** During the term of this Contract, the Network Service Provider shall annually prepare an SAS 70 Type II report or a similar report in accordance with an at least equivalent standard (such as ISAE 3402 or the US SSAE 16 standard) and shall provide the Eurosystem (or any person designated by the Eurosystem who is subject to a professional duty of confidentiality) with copies of such reports without undue delay after such reports are prepared by the Network Service Provider. The Network Service Provider shall grant the Eurosystem (or any person designated by it who is subject to a professional duty of confidentiality), upon reasonable advance notice, access to the Network Service Provider's premises and to any Data reasonably required by the Eurosystem to assess whether the Network Service Provider, the Network and the Connectivity Services comply with this Contract, the Specifications and applicable laws. The Network Service Provider shall not be obligated to provide the Eurosystem (or any person designated by it) with access to (i) information regarding any customers of the Network Service Provider other than Di.Co.A., (ii) information regarding any communications network solutions and any network or connectivity services which are provided by the Network Service Provider to such customers or (iii) information which it may not disclose due to mandatory applicable law.

10.4 **Data.** The Network Service Provider acknowledges and agrees that, in the course of the implementation of the Network and the provision of the Connectivity Services it will gain access to personal data as defined in Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, as well as data, information and material regarding the business transactions, financial situation and operations of the market

participants and their customers (together "**Data**"). The Network Service Provider undertakes to solely use Data for the purpose of performing the Connectivity Services, unless otherwise agreed between the Parties.

10.5 **Data Protection.** Each Party shall comply with any laws regarding the collection, storage, transfer or processing of personal data (the "**Data Protection Laws**") which are applicable to it in connection with the performance of its obligations under this Contract, in particular any laws by which Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 and Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 have been transformed into the laws of the EU Member States. The Network Service Provider shall, during the term of this Contract and thereafter for as long as the Network Service Provider continues to have access to or to store any personal data or Confidential Information obtained in connection with the provisions of the ESMIG Services or this Contract, maintain, and comply with, a data protection policy which complies with the Data Protection Laws and the requirements more specifically described in the Business Requirements and which provides for adequate technical and organisational measures regarding the protection of Data (the "**Data Protection Policy**"). The Network Service Provider shall be responsible for the compliance by any of its Subcontractors with the Data Protection Laws applicable to such Subcontractor to the extent such compliance is relevant for the performance of the Network Service Provider's obligations under this Contract.

Article 11

Network Disaster Recovery; Business Continuity and Insurance

11.1 **Security.** The Network Service Provider shall be responsible for the maintenance of security of the Network, the hardware and the software and other technical infrastructure controlled by the Network Service Provider and used for the provision of the Connectivity Services as well as the Files and Messages exchanged by using the Network and the Connectivity Services. For this purpose, the Network Service Provider shall take security measures which comply with best industry practice, but in any event the security measures described in the Technical Requirements. Without limitation to the foregoing, the Network Service Provider shall take all technically feasible and commercially reasonable measures to prevent security threats from adversely affecting the Network or the Services.

11.2 **Responsibility of the Network Service Provider.** The Network Service Provider shall be fully responsible towards the Eurosystem for the operation of the Network and the provision of the Connectivity Services in accordance with this Contract, the Specifications and the ESMIG Connectivity Services Agreements and for any Failure of the Network and the Connectivity Services within the respective boundaries of responsibility. The

Network Service Provider shall have no responsibility regarding the processing or exchange of Files or Messages outside the respective boundaries of responsibility, except to the extent any problem or failure regarding the processing or exchange of Files or Messages which becomes manifest outside the boundaries of responsibility was caused within the boundaries of responsibility.

11.3 **Recovery from a Network Disaster.** The Network Service Provider shall, during the term of this Contract and the term of any ESMIG Connectivity Services Agreement, maintain and comply with a disaster recovery and business continuity plan which complies with best industry practice and the requirements more specifically described in the Specifications, in particular Section 3.6 of the Technical Requirements. The Network Service Provider shall, in response to the occurrence of an event that results in an interruption or suspension of any of the Connectivity Services, including a Force Majeure Event (each such event a "**Network Disaster**") execute its disaster recovery and business continuity plan and shall use commercially reasonable efforts to minimize the disruption of the Connectivity Services and the effects of the Network Disaster on the Network and the Di.Co.A.. In the event of a Network Disaster, the Provider shall treat the Eurosystem and the directly connected market participants no less favourably than any of its other customers, shall follow the procedures set out in Section 3.6 of the Technical Requirements and shall use all reasonable efforts to re-establish, and shall allocate all such resources as are reasonably necessary to re-establish, as soon as reasonably possible, its ability to provide the Connectivity Services to the Di.Co.A.in accordance with this Contract and the ESMIG Connectivity Services Agreements. For the avoidance of doubt, neither the obligation to provide, nor the provision of, disaster recovery or business continuity services shall release the Network Service Provider from its obligation to provide the other Connectivity Services in accordance with this Contract which are not affected by the Network Disaster.

Article 12

Assignment, Transfer and Subcontracting

12.1 **Assignment/Transfer.** The Network Service Provider may not assign or transfer any or all of its rights or obligations hereunder, unless such a transfer occurs as a result of a merger of the Network Service Provider into another entity or any other transaction or event which has a similar effect on the Network Service Provider. In case any such transaction involving the Network Service Provider is contemplated, the Network Service Provider shall give the Eurosystem notice of such transaction reasonably in advance of the transaction becoming effective. The notice shall contain all information required to demonstrate to the Eurosystem that the entity to which the Network Service Provider's rights or obligations would transfer as a result of such transaction fulfils all requirements for participation in the selection procedure for the awarding of the Concession. If the

requirements set out above are not met by the succeeding entity, the Eurosystem may object to the resulting transfer within sixty (60) Business Days from the receipt of the notice; in this case Article 17.2 (e) shall apply. If no objection is raised by the Eurosystem within such period, the resulting transfer shall become fully effective towards the Eurosystem.

12.2 **Subcontracting.** Pursuant to Article 174 of the Italian Code of Public Contracts, the Network Service Provider may, with the Eurosystem's prior written consent, delegate the performance of part (but not all) of its obligations hereunder to third parties (the "**Subcontractors**"), provided that the conditions set out in the Awarding Rules are fulfilled with respect to the Subcontractor.

The Eurosystem shall be entitled to deny its consent if the conditions set out in Article 5 of the Awarding Rules are not fulfilled. If the consent is not denied within twenty days from the delivery by the Network Service Provider of the documents to be delivered pursuant the Awarding rules, the Eurosystem shall be deemed to have granted its consent.

The delegation of the Network Service Provider's obligations to a Subcontractor shall not relieve the Network Service Provider from liability for the performance of such obligations, and any act or omission of a Subcontractor or of any person acting for such Subcontractor shall be deemed to be an act or omission of the Network Service Provider.

12.3 **Continuing Obligations.** The performance of obligations delegated to a Subcontractor may not be further delegated. The Subcontractors shall comply with all laws and collective bargaining agreements applicable to the relevant Subcontractor concerning security, safety at work, insurance, social security and assistance, working conditions and economic treatment. The Network Service Provider shall procure that the Subcontractors comply with such laws and collective bargaining agreements and with the requirements set out in this Article 12.3 and in the Awarding Rules and shall be jointly and severally liable with the Subcontractors for any failure to so comply.

Each contract with a Subcontractor shall provide that the Subcontractor shall assume, and comply with, all obligations regarding traceability of funds referred to in Article 3 of Italian Law no. 136/2010 and subsequent amendments, including the obligations regarding current accounts described in Article 21.7. The Network Service Provider undertakes to inform the Eurosystem and the prefecture-territorial office of the government of the Rome-Province immediately of any non-compliance by a Subcontractor with the requirements regarding traceability of funds.

12.4 **Withdrawal of consent.** Without prejudice to the provision set out in Article 17(2)(f), the Eurosystem shall be entitled to withdraw its consent to the delegation to a Subcontractor of the performance of the Network Service Provider's obligations hereunder at any time if

(a) the Subcontractor no longer fulfils the requirements for participation in the selection procedure for awarding the Concession;

(b) the Network Service Provider or the Subcontractor fail to comply with the requirements and obligations set out in Article 12.3 or in the Awarding Rules.

Article 13

Representations and Warranties, Covenants

13.1 The Eurosystem and the Network Service Provider. Each Party hereby represents and warrants that it has full capacity and authority and all necessary consents to enter into and to perform this Contract and that this Contract is executed by one or more of its duly authorised representatives.

13.2 The Network Service Provider. The Network Service Provider hereby represents and warrants to the Eurosystem that

(a) it has all necessary permits, consents and approvals from government authorities required to enter into this Contract, to design, develop, implement and operate the Network and to provide the Connectivity Services and to perform its other obligations under this Contract;

(b) except to the extent that pursuant to this Contract such hardware or software is to be provided by the Eurosystem or the Di.Co.A., it has all necessary rights and ownership interests, including ownership of, or rights of use or licenses with respect to, Intellectual Property Rights, in the hardware and software to be used in connection with the design, development, implementation and operation of the Network and the provision of the Connectivity Services, in particular, but without limitation, the right to use any Embedded Software;

(c) the Network originally designed, developed and implemented by the Network Service Provider complies with the Specifications and is fit for the purposes intended by the Eurosystem and the Di.Co.A. as they are described in this Contract and the Specifications; and

(d) its professional staff and other resources assigned to the operation of the Network and the provision of the Connectivity Services are sufficiently trained and experienced to perform its obligations under this Contract in accordance with generally accepted industry standards and best industry practice;

(e) no statement made and no information provided by the Network Service Provider during the procedure for its selection as set out in the Awarding Rules or in the Contract Notice, in particular in any documents submitted by it to the Banca d'Italia, or in connection with the awarding of the Concession or the entering into of this Contract was at the time it was made or provided, or is at the date hereof, untrue, incorrect or misleading;

(f) at the time it submitted its offer it fulfilled, and on the date hereof it fulfils, all requirements and prerequisites for the participation in the procedure for its selection, in particular those set out in the Awarding Rules.

13.3 Covenants. The Network Service Provider hereby agrees and covenants that throughout the term of this Contract

(a) it will have and maintain in full force and effect all necessary permits, consents and approvals from government authorities required to enter into this Contract, to design, develop, implement and operate the Network and to provide the Connectivity Services and to perform its other obligations under this Contract;

(b) except to the extent that pursuant to this Contract such hardware or software is to be provided by the Eurosystem or the Di.Co.A., it will have and maintain in full force and effect all necessary rights and ownership interests, including ownership of, or rights of use or licenses with respect to, Intellectual Property Rights, in the hardware and software to be used in connection with the design, development, implementation and operation of the Network and the provision of the Connectivity Services, in particular, but without limitation, the right to use any Embedded Software;

(c) it will procure that the Network and the Connectivity Services (as modified from time to time in accordance with this Contract) comply with the Specifications and are fit for the purposes intended by the Eurosystem and the Di.Co.A. as they are described in this Contract and the Specifications;

(d) it will ensure that its professional staff and other resources assigned to the operation of the Network and the provision of the Connectivity Services are sufficiently trained and experienced to perform its obligations under this Contract in accordance with generally accepted industry standards and best industry practice;

(e) it will continue to fulfil all requirements and prerequisites for the participation in the public procurement procedure for its selection under Italian law, in particular those set out in the Awarding Rules;

(f) it will comply with all applicable laws governing the design, development, implementation and operation of the Network and the provision of the Connectivity Services; and

(g) it will comply with the obligations, requirements and criteria more specifically described in the Business Requirements.

Article 14
Liability

14.1 **Standard of Care.** The Network Service Provider shall perform its obligations with the skill, care and diligence expected of a professional provider of communications network solutions and network, connectivity and messaging services, and in accordance with best industry practice. When performing its obligations under this Contract, each Party shall act in good faith and shall duly consider the rights and interests of the other Party. Each Party shall be obligated to use commercially reasonable efforts to mitigate any Losses incurred by it in connection with this Contract.

14.2 **Liability for Losses.** Each Party shall be liable to the other Party for any Losses incurred by the other Party as a result of the first Party's non-performance of, non-compliance with or breach of its representations and warranties, covenants, undertakings or obligations under this Contract.

Each Party's liability for Losses incurred by the other Party due to the first Party's ordinary negligence during any Contract Year shall be limited to an amount of EUR 2 Million (the "**Liability Cap**").

The Liability Cap shall not apply to a Party's liability (i) for Losses incurred by the other Party due to the first Party's gross negligence or wilful misconduct, (ii) for infringement of third party Intellectual Property Rights under Article 16, (iii) for breaches of representations and warranties under Article 13, (iv) for penalties under Article 14.3 and (v) under Article 14.4.

14.3 **Penalties.** In the events and under the circumstances described below, the Network Service Provider shall pay to the Eurosystem the following penalties

(a) a penalty in the amount of EUR 10.000 for each calendar day (or part thereof) of Delay with respect to any of the Milestones set out in Article 3.1;

(b) for each calendar day (or part thereof) on which a failure by the Network Service Provider, the Network or the Connectivity Services to comply with the criteria or requirements set out in the Technical Requirements affects ESMIG Services

(aa) a penalty in the amount of EUR 1,000 if such failure reduces the reliability of any of the ESMIG Services, but does not impair their operability;

(bb) a penalty in the amount of EUR 5,000 if such failure impairs the operability of any of the ESMIG Services unless such impairment is not material and does not result in any of the ESMIG Services not being available to the Di.Co.A.; and

(cc) a penalty in the amount of EUR 10,000 if such failure materially impairs the operability, or results in any of the ESMIG Services not being available to the Di.Co.A.;

(c) a penalty in the amount of EUR 1,000 for each calendar day (or part thereof) during the first calendar month (or any part thereof) which penalty shall be increased during any subsequent calendar month by an additional EUR 1,000 for each calendar day (or part thereof) (but in no event more than EUR 10,000 for each calendar day) on which

(aa) the Network Service Provider fails to deliver a statement regarding its solvency ratio as more specifically described in Section 1.1 of the Business Requirements;

(bb) the Network Service Provider fails to deliver a legal opinion regarding its data protection policy as more specifically described in Section 1.2 of the Business Requirements;

(cc) the Network Service Provider fails to deliver a copy of its operational risk management policy or a statement from an external auditor as more specifically described in Section 1.3 of the Business Requirements;

(dd) the Network Service Provider fails to deliver a copy of its technology risk management policy or a statement from an external auditor as more specifically described in Section 1.4 of the Business Requirements;

(ee) the Network Service Provider fails to deliver the information regarding the technical solutions, documentation and support available to actual and potential Di.Co.A., or regarding the stages of the connection to the Network and testing opportunities, as more specifically described in Section 2.1 of the Business Requirements;

(ff) the Network Service Provider fails to deliver the annual SAS 70 Type II report or a similar report prepared in accordance with an at least equivalent standard (such as ISAE 3402 or the US SSAE 16 standard) as more specifically described in Section 2.2 of the Business Requirements; and

(gg) the Network Service Provider fails to publish its maximum prices as more specifically described in Section 3 of the Business Requirements;

(d) a penalty in the amount of the indemnification payable to a Di.Co.A. in accordance with Article 7.6 for fees charged to the Di.Co.A. exceeding the maximum prices; and a penalty in the amount of 10% of such indemnification for each month of delay of the payment of such indemnification to the Di.Co.A..

The total amount of the penalties imposed cannot exceed 10 per cent of the value of the Contract. Once this limit is reached, the Eurosystem reserves the right to terminate the contract in accordance with Article 17.2, without prejudice to the right to compensation for additional damages.

The aggregate amount of any penalties accrued hereunder shall be due and payable by the last day of the calendar month immediately following the calendar month in which they have accrued. The penalties payable in accordance with this Article 14.3 shall be cumulative and shall be payable in addition to, and shall not be set off or credited against, any liability of the Network Service Provider hereunder for Losses incurred by the Eurosystem.

14.4 Indemnity. The Eurosystem shall not be liable for any Losses incurred by the Di.Co.A. due to any act or omission of the Network Service Provider. The Network Service Provider shall indemnify and hold harmless the Eurosystem from and against any Losses incurred in connection with any claim asserted against the Eurosystem by a Di.Co.A. or any other third party due to any act or omission of the Network Service Provider.

Article 15
Force Majeure

15.1 **Suspension of Obligations.** Pursuant to Article 107 of the Italian Code of Public Contracts, if a Force Majeure Event occurs, the obligations affected by such Force Majeure Event shall be suspended and the Party affected by such Force Majeure Event shall not be obligated to perform such obligations for the period during which the Party is affected by such Force Majeure Event. The Party affected by the Force Majeure Event shall promptly notify the other Party.

The Party affected by the Force Majeure Event use commercially reasonable efforts to procure that it is able to perform the obligations affected by the Force Majeure event as soon as possible after the occurrence of the Force Majeure Event. A "**Force Majeure Event**" shall include political disturbance, catastrophes in nature, fire, war, epidemics and all other circumstances beyond a Party's reasonable control which prevent the respective Party against its will from performing its obligations under this Contract.

15.2 **Negotiations.** In case a Force Majeure Event occurs, the Network Service Provider and the Eurosystem shall promptly enter into good faith negotiations in order to agree a mutually acceptable solution to the matters arising therefrom.

Article 16
Intellectual Property Rights

16.1 **No Licence to Network Service Provider.** Except as provided in the following sentence, nothing in this Contract shall confer, or be construed to confer, on the Network Service Provider, any licence of, or right of use with respect to, any Intellectual Property Rights in ESMIG or any of the ESMIG Services. To the extent the Network Service Provider can reasonably demonstrate that the implementation or operation of the Network or the provision of the Connectivity Services requires the use by the Network Service Provider of any Intellectual Property Rights in ESMIG or any of the TARGET Services and applications, the Parties shall enter into good faith negotiations about a non-exclusive licence for the Network Service Provider to use the relevant Intellectual Property Rights which license shall be limited to the purpose of implementing or operating the Network or providing the Connectivity Services, as the case may be.

16.2 **Licence.** The Network Service Provider hereby grants the Eurosystem a non-exclusive, royalty-free licence or sub-licence, as the case may be, to use any Intellectual Property rights in any materials, work results or software, including Embedded Software (in each case, including any update, upgrade and new release thereof) required to be used by the

Eurosystem in connection with this Contract, the Network, the Connectivity Services or otherwise for making the ESMIG Services available to the Di.Co.A..

16.3 Infringement of Third Party Intellectual Property Rights. The Network Service Provider shall indemnify and hold harmless the Eurosystem from and against any Losses incurred in connection with any claims of a third party asserted against the Eurosystem that the Network, the Connectivity Services or any part thereof or the use of the Network or the Connectivity Services by the Eurosystem or the Di.Co.A. in accordance with this Contract or the relevant ESMIG Connectivity Services Agreement, as the case may be, infringes the third party's Intellectual Property Rights (each such claim an "**Infringement Claim**") The Eurosystem shall, without undue delay after it becomes aware of such Infringement Claim, notify the Network Service Provider of any Infringement Claim asserted against the Eurosystem in writing. Without undue delay after having been notified of an Infringement Claim, the Network Service Provider shall assume, at its own cost, the defence of such Infringement Claim and shall, to the extent permitted under applicable law, conduct any negotiations and litigation in respect to such Infringement Claim, provided that the Network Service Provider shall not be entitled or authorised to make any declarations or take any actions in the name of the Eurosystem, in particular to agree to the settlement of any Infringement Claim, without the prior written consent of the Eurosystem which consent shall not be unreasonably withheld or delayed. The Eurosystem shall, to the extent reasonably required, assist the Network Service Provider with the conduct of any such negotiations and litigation.

16.4 Remedies for infringement of third party IP Rights. If the Network or the Connectivity Services or any part thereof is held to constitute an infringement of a third party's Intellectual Property Rights or if the use of the Network or the Connectivity Services by the Eurosystem or by the Di.Co.A. in accordance with this Contract or the respective ESMIG Connectivity Services Agreements, as the case may be, is enjoined, the Network Service Provider shall, at its own cost,

(a) obtain for the Eurosystem and the Di.Co.A. the right to continue using the Network and the Connectivity Services, or

(b) modify the Network or the Connectivity Services to ensure that it no longer infringes the third party's Intellectual Property Rights provided, however, that the Network and the Connectivity Services must continue to have the features and functionalities and comply with the technical, operational and Business Requirements more specifically described in this Contract and the Specifications.

Article 17

Term and Termination

17.1 **Term.** This Contract shall become effective as of the date on which this Contract has been duly signed by both Parties (the "**Effective Date**") and shall, unless terminated in accordance with this Contract, have a term ending ten (10) years from the Go-Live Date. The Eurosystem may, in its sole discretion, postpone the Go-Live Date. Any postponement of the Go-Live Date shall be communicated to the Network Service Provider as soon as the Eurosystem is aware of circumstances which require such postponement.

17.2 **Termination.** Without prejudice to any other rights or remedies provided for herein or by applicable law, each of the Eurosystem and the Network Service Provider shall be entitled to terminate this Contract for material breach.

The Eurosystem shall be entitled to terminate this contract pursuant to Articles 108 and 176 of the Italian Code of Public Contracts.

Moreover, the Eurosystem reserves the right to terminate the contract for the purposes of Article 1456 of the Italian Civil Code (express termination clause):

(a) if the total amount of the penalties imposed to the Network Service Provider exceeds 10 per cent of the value of the Contract, in accordance with Article 14.3;

(b) if the Network Service Provider is in breach of any of the representation and warranty, covenants or undertakings set out in Articles 7, 13.1, 13.2, 13.3, 21.7;

(c) if the project for the design, development and implementation of ESMIG fails or is discontinued;

(d) in case of failure of the Compliance Check, as more specifically described in paragraph 2 of Attachment 1.1 ("Technical Requirements and Compliance Check");

(e) if :

(i) the Network Service Provider has infringed the prohibition of the assignment or transfer of rights or obligations under this Contract set out in Article 12.1;

(ii) the Network Service Provider fails to comply with the obligations regarding a transaction pursuant to Article 12.1;

(iii) the Eurosystem has objected to a transaction pursuant to Art. 12.1;

(iv) the Network Service Provider has delegated the performance of its obligations to a Subcontractor without the prior written consent of the Eurosystem;

(v) the Subcontractor has infringed the prohibition, set out in Article 12.3, of further delegating the performance of its obligations;

(f) where the Business Requirements provide for a right of the Eurosystem to terminate this Contract.

In the cases provided for in this Article or if the Network Service Provider does not perform or comply with any of its obligations hereunder or is in breach of any representation and warranty or covenant or undertaking under this Contract the Project manager appointed by the Eurosystem will notify the Responsabile unico del procedimento (Senior officer in charge of the selection procedure) with any non-performance, non-compliance or breach. The Project manager will send a notice to the Network Service Provider, allowing at least 15 days to provide suitable justifications. In case of failure to provide such justifications and on a proposal of the Responsabile unico del procedimento, the Eurosystem will terminate the Contract.

The Eurosystem shall be entitled to terminate this contract if any event or circumstance, including (but not limited to) a Force Majeure Event, which prevents the Network Service Provider from providing the Network or the Connectivity Services in accordance with this Contract persists for a period of more than three (3) months.

The Contract shall terminate automatically if:

(a) the award of the Concession is revoked, withdrawn or declared unlawful, invalid or unenforceable by the Banca d'Italia (the contracting authority), in particular, without limitation, in any of the events described in paragraph 8 of the Awarding Rules;

(b) the Network Service Provider is, for the purposes of any applicable laws, under an insolvency procedure, without prejudice to Article 110 of the Italian Code of Public Contracts.

17.3 Effect of Termination on Concession. The Concession shall expire automatically upon the expiration or termination of this Contract.

17.4 Continuation of Connectivity Services. Unless otherwise agreed by the Parties, the Network Service Provider shall provide the Connectivity Services in accordance with this

Contract until the effective date of a termination of this Contract. Upon the expiration or termination of this Contract, the Network Service Provider shall continue to provide the Connectivity Services and shall use reasonable efforts to ensure an orderly transition of the Services to the Eurosystem or to such other persons or entities designated by the Eurosystem to assume the provision of the Connectivity Services (the "**Successor Network Service Provider**") until such time as the Eurosystem has notified the Network Service Provider of the completion of the transition to the Successor Network Service Provider but in no event longer than two (2) years from the effective date of the termination or the expiration of this Contract (the "**Transition Period**"). During the Transition Period, the Network Service Provider shall, in particular, provide to the Eurosystem or the Successor Network Service Provider any information or documentation reasonably required to render the Connectivity Services.

17.5 **Surviving Provisions.** For the avoidance of doubt, the termination or expiration of this Contract shall not release the Parties from any of their obligations under this Contract which have arisen prior to or in connection with the expiration or termination. Article 10.1 (Recordkeeping), Article 10.5 (Data Protection), Article 16 (Intellectual Property Rights), Article 17.4 (Continuation of Connectivity Services), Article 19 (Confidentiality) and Article 20 (Notices), Article 21 (Miscellaneous), Article 22.1 (Governing Law) and Articles 22.3 (Preliminary Relief) shall survive the termination or expiration of this Contract.

Article 18
Taxes, Duties and Costs

Each Party shall bear all taxes, duties, fees and commissions it has incurred in connection with the negotiation and conclusion of this Contract or will incur in connection with the performance of its respective obligations under this Contract (including, without limitation, costs and fees for permits, licences, etc.).

Article 19
Confidentiality

19.1 **General.** Unless expressly permitted by this Contract, each Party shall treat as confidential and shall not disclose, without prior written consent of the other Party, any Confidential Information.

19.2 **Confidential Information.** For the purposes of this Contract "**Confidential Information**" means any information related to a Party's business operations, including products, services, methods of doing business, research and development activities, know-how, customers, trade secrets, commercial secrets, computer programs or finances and

Data irrespective of the manner in which such information is stored or the manner in which it is disclosed by or on behalf of a Party (the "**Disclosing Party**") to the other Party (the "**Receiving Party**") as well as the terms and conditions of this Contract and the Specifications, any documentation provided in accordance with this Contract and the description of the technical infrastructure, including software and hardware, of the Network.

19.3 **Permitted Disclosure.** The Receiving Party shall be permitted to disclose Confidential Information if and to the extent the Receiving Party can demonstrate that such information:

(a) was already publicly known at the time it was disclosed to the Receiving Party;

(b) became publicly known after the time it was disclosed to the Receiving Party without a breach by the Receiving Party of its obligations hereunder;

(c) was already known to the Receiving Party at the time it was disclosed to the Receiving Party; or

(d) was disclosed to the Receiving Party by a third party that was not under an obligation of confidentiality with respect to such information;

(e) must be disclosed by the Receiving Party due to applicable law or the final and binding order of a competent court or government authority that has jurisdiction over the Receiving Party, including without limitation the European Commission, any Central Bank Supervisory Authority or tax authority;

(f) was disclosed by the Receiving Party to those of its officers, directors, employees, agents, delegates or Subcontractors who need to know such information in order to enable the Receiving Party to perform its obligations hereunder, provided that such persons are made aware of the confidential nature of such information and, in the case of agents, delegates or Subcontractors, such persons have undertaken in writing towards the Disclosing Party to keep such information confidential on terms substantially the same as the confidentiality obligations set forth in this Article 19;

(g) must be disclosed in order to exercise, protect or enforce the rights of the Receiving Party under this Contract before a competent court or government authority;

19.4 **Additional Requirements for Disclosure.** As regards Article 19.3 (e), if the Receiving Party is required to disclose or otherwise make Confidential Information available to a court or a government authority, the Receiving Party shall:

(a) notify the Disclosing Party reasonably in advance of any such disclosure in as detailed a manner as can be reasonably expected in the circumstances;

(b) obtain and make available to the Disclosing Party reasonable substantiated assurance from a reputable law firm as to the lawfulness and enforceability of such disclosure;

(c) cooperate with and provide such reasonable assistance as the Disclosing Party may reasonably request in the circumstances to allow the Disclosing Party to seek any legal remedies it may reasonably deem appropriate and pertinent to protect the Confidential Information against disclosure to the court or other government authority; and

(d) notify the court or other government authority concerned of the confidential nature of the Confidential Information and request it to preserve the confidentiality of the Confidential Information.

19.5 **Press Releases.** The Eurosystem and the Network Service Provider may issue a press release concerning the signing of this Contract, the content of which will be mutually agreed upon between the Parties. The Network Service Provider shall submit to the Eurosystem for approval the wording of any further press release it intends to issue or other public statements it intends to make with respect to this Contract or the provision of the Network or the Connectivity Services under this Contract.

Article 20
Notices

20.1 **Form and language.** Any notice, document or information to be furnished or supplied pursuant to this Contract shall be in writing and in the English language.

20.2 **Means.** Unless provided otherwise in the Specifications, any notice given hereunder shall be delivered personally or dispatched by letter, by e-mail or by facsimile (in case of an e-mail or facsimile transmission, a subsequent confirmation letter is required) and shall be effective upon receipt of the mail or the facsimile transmission.

20.3 **Addresses.** All communications and deliveries of documents hereunder shall be made to the following addresses:

To the Eurosystem:

Banca d'Italia
Servizio Sistema dei Pagamenti
To the attention of Lorenzo Giammò (lorenzo.giammo@bancaditalia.it)
Largo Guido Carli 1
00044 Frascati (RM)
Italia

with a copy to:

Banca d'Italia
Servizio Sistema dei Pagamenti
Divisione Infrastrutture di Mercato dell'Eurosistema
To the attention of Clara Mandolini (clara.mandolini@bancaditalia.it)
Largo Guido Carli 1
00044 Frascati (RM)
Italia

To the Network Service Provider:

S.W.I.F.T SCRL
Attn of Chief Executive Europe, Middle East and Africa
Av Adèle 1
B-1310 La Hulpe
Belgium

with a copy to:

S.W.I.F.T SCRL
Attn of General Counsel
Av Adèle 1
B-1310 La Hulpe
Belgium

The Parties shall promptly notify each other of any change of address for notice.

Article 21

Miscellaneous

21.1 **The Eurosystem.** The Banca d'Italia, as a member of the Eurosystem, has entered into this Contract in its own name and interest and in the name and interest of the other Eurosystem Central Banks. The Eurosystem Central Banks shall be joint and several creditors of the duties, obligations and liabilities of the Network Service Provider under or in connection with this Contract, provided, however, that the Network Service Provider shall, unless expressly agreed otherwise by the Parties, perform its duties and obligations and satisfy its liabilities under or in connection with this Contract only towards the Banca d'Italia.

Unless expressly agreed otherwise by the Parties, the Eurosystem Central Banks shall be joint and several debtors of the duties, obligations and liabilities of the Eurosystem under or in connection with this Contract.

21.2 **Representation in Proceedings.** Each of the Eurosystem Central Banks hereby appoints the Banca d'Italia to represent it, to the extent permitted by applicable law, in any proceedings before a state court arising out of or in connection with this Contract. The Banca d'Italia shall be entitled to make and receive, in the name and on behalf of each of the other Eurosystem Central Banks, any declarations and to take, in the name and on behalf of each of the other Eurosystem Central Banks, any actions which it deems necessary or appropriate in connection with such proceedings and the conduct and termination, including by way of settlement, thereof.

21.3 **Severability.** If any provision of this Contract should be invalid, Article 1419 of the Italian Civil Code will apply. Without prejudice to Article 1339 of the Italian Civil Code, in case of partial nullity, the contractual provision declared invalid shall be replaced with a valid and enforceable provision the economic and legal effect of which approximates as closely as possible that of the invalid provision.

21.4 **Amendments.** Except as otherwise expressly provided for in this Contract, or pursuant to a Change Request, this Contract and its Attachments may only be amended by a written instrument duly executed by authorised representatives of the Parties.

21.5 **Waiver.** The provisions of this Contract may only be waived by a written instrument duly executed by authorised representatives of the Party declaring such waiver. Except where a specific period exercising any right arising under this Contract is provided for herein or under applicable law, no delay on the part of a Party to exercise such right shall constitute, or be construed to constitute, a waiver thereof. Neither any waiver by a Party of any right, power or privilege nor any single or partial exercise of such right, power or privilege shall

preclude any further exercise by such Party thereof or of any other right, power or privilege.

21.6 **Entire agreement.** The Contract Notice, the Awarding Rules, this Contract and the Specifications constitute the entire agreement of the Parties with respect to the subject matter hereof and shall supersede any previous negotiations, proposals, agreements and understandings between the Parties relating to the subject matter of this Contract.

21.7 **Compliance with requirements regarding traceability of funds.** The Network Service Provider shall assume, and comply with, all obligations regarding traceability of funds referred to in Article 3 of Italian Law no. 136/2010 and subsequent amendments. To this end, the Network Service Provider undertakes to communicate to the Eurosystem promptly, and in any case no later than seven days after it is opened, the identifying particulars of the any current account intended to be used by the Network Service Provider in financial transactions relating to the present Contract and the identifying particulars and tax numbers of the persons authorized to perform transactions with respect to such account. In the case the Network Service Provider intends to use one or more current accounts which are already in existence on the date of this Contract, the Network Service Provider undertakes to communicate the data referred to above before the initial use of any such current account in financial transactions relating to the present Contract. The Network Service Provider also undertakes to promptly communicate to the Eurosystem any change in respect of the data transmitted to the Eurosystem pursuant to this Article 21.7.

Article 22

Governing Law and Escalation Procedure

22.1 **Governing law.** This Contract shall be governed by, and construed in accordance with, the laws of the Italian Republic. Any dispute arising under this Contract shall not be subject to arbitration but shall be decided exclusively by the Courts of Rome, Italy.

22.2 **Escalation Procedure.** Without prejudice of the provision under Article 17.2, in the event of a dispute between the Parties arising out of or in connection with this Contract the Parties shall use commercially reasonable efforts to resolve the matter on an amicable basis and in a fair and equitable manner in accordance with the procedure set out in this Article 22.2 (the "**Escalation Procedure**").

(a) Upon notification by one Party to the other Party, the matter shall first be referred to the Project Managers. If the Project Managers fail to resolve the matter within a reasonable period of time after it has been referred to them, but in no event more

than twenty (20) Business Days, they shall refer the matter to the Steering Committee.

(b) The Steering Committee shall use commercially reasonable efforts to resolve the dispute within a reasonable period of time taking into consideration the nature of the dispute, but in no event longer than twenty (20) Business Days after the matter has been referred to the Steering Committee in accordance with Article 22.2 (a).

22.3 Preliminary Relief. Nothing in this Article 22 shall limit, exclude or otherwise impair either Party's right to seek preliminary or injunctive relief before a state court.

THE EUROSYSTEM

Documento firmato da:
MESIANO LAUREANI VINCENZO
25.06.2019 07:53:55 UTC

_____

S.W.I.F.T. SCRL

_____

Pursuant to Article 1341(2) of the Italian Civil Code, the Network Service Provider expressly approves the provisions contained in the following articles:

- Article 2 - Scope of the Contract; Main Obligations of the Parties;
- Article 7.6 - Penalties;
- Article 9 - Development of the Network and the Connectivity Services; Change Management;
- Article 12 - Assignment, Transfer and Subcontracting;
- Article 14 - Liability;
- Article 16 - Intellectual Property Rights;
- Article 17 - Term and Termination;
- Article 19 - Confidentiality;
- Article 22 - Governing law and Escalation Procedure.

S.W.I.F.T. SCRL

_____

Information notice concerning personal data processing

In accordance with the European and national legislation, we hereby inform you that Banca d'Italia (BDI) processes the following personal data of employees of firms that operate in BDI premises:

- name and surname;
- date and place of birth;
- identity document data.

Provision of these data is required for the employees of contractors/subcontractors to gain access to Banca d'Italia premises in accordance with internal security policies.

Data are stored in paper format or processed with IT procedures, with the use of security measures which protect the privacy of the personal data and which prevent unauthorized access to such data by third parties or unauthorized persons. The data will not be communicated or disseminated to third parties.

Personal data will be stored for ten years.

The data may be accessed by the Head of the IT Development Directorate and the Head of the IT Operations Directorate, the official in charge of this procedure and the employees of these Directorates authorized to process data.

Data subjects can exercise their rights with respect to the data controller (Banca d'Italia, Organization Directorate, Via Nazionale 91, 00184 ROME, e-mail org.privacy@bancaditalia.it). These rights include the right to access their personal data and the other rights granted by law, including the right to obtain rectification, integration or erasure of data; the right to anonymize the data or to block the use of any data used in violation of the law; the right to object, on legitimate grounds, to the processing of personal data.

The Data Protection Officer of Banca d'Italia can be contacted at Via Nazionale 91, 00184 ROME or at the e-mail address responsabile.protezione.dati@bancaditalia.it.

Data subjects can lodge a complaint with the Italian Data Protection Authority if they consider that their data are processed in violation of the law.

BANCA D'ITALIA
EUROSISTEMA

DIPARTIMENTO IMMOBILI E APPALTI
SERVIZIO APPALTI (897)
DIVISIONE APPALTI INFORMATICI (004)

ATTACHMENT 1
AWARDING RULES

Open procedure for the concession of Eurosystem Single Market Infrastructure Gateway (ESMIG) Connectivity Services

Code G011/18

PREMISE[1]

Whereas

- The Eurosystem Single Market Infrastructure Gateway (ESMIG) is a technical component delivered as part of the T2-T2S Consolidation project that shall consolidate the access to all market infrastructures that the Eurosystem provides. Via the ESMIG a market participant can use the same technical setup for accessing TARGET2-Securities, TARGET2, TIPS and potentially other services and applications.
- In its meeting on 23/24 April 2018 the Market Infrastructure Board decided that the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d'Italia (hereinafter the '4CB') would make necessary preparations to have up to three network service providers to provide connectivity services to the ESMIG and that the Banca d'Italia would lead the selection procedure.
- In its meeting on 23/24 April 2018 the Market Infrastructure Board decided that the Banca d'Italia would act as the operating arm of the Eurosystem for the selection procedure. It also decided that the Market Infrastructure Board would be responsible for designating the selection panel members since the Eurosystem central banks would be responsible and liable for the selection criteria and for the outcome of the selection panel's decision based on the selection criteria. The Banca d'Italia would be responsible for correctly conducting the selection procedure and its specific liability related to the selection procedure would be separate from the liability assumed by the 4CB under the Level 2-Level 3 agreement.
- The purpose of the selection procedure is to entrust network service providers to provide a set of predefined connectivity services, on the basis of which the ESMIG network service providers design, implement, deliver and operate connectivity solutions intended to securely exchange business information between the market participants connected via them and the Eurosystem market infrastructures via the ESMIG.
- The selection procedure for ESMIG network service providers falls under the scope of Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts and under the Italian Code of Public Contracts (d.lgs. 18 aprile 2016 n. 50, hereinafter the "Code"), which are applicable to the mandated central bank.
- The Banca d'Italia has been appointed by the Governing Council to carry out the selection procedure for the network service providers.
- The Banca d'Italia has accepted the appointment and has confirmed its willingness to act in accordance with the Governing Council's Decision.

The Banca d'Italia has published a Concession Notice for an open procedure pursuant to Art. 60 of the Code to award three ESMIG connectivity services Concessions (hereinafter "the Concessions"). The selection procedure will be managed by means of the Banca

[1] The definitions set forth in the "Concession Contract" (Annex AR.1) shall be applicable to these Awarding Rules.

d'Italia's Electronic tenders Portal ("Portale gare telematiche della Banca d'Italia, hereinafter "the Portal"), in accordance with the general terms and conditions for the use of the Portal ("Condizioni generali di utilizzo del Portale Gare Telematiche della Banca d'Italia", hereinafter "the Conditions") and related instructions ("Istruzioni per l'utilizzo del Portale Gare Telematiche della Banca d'Italia", hereinafter, "the Instructions"), accepted by registered economic operators upon registration to the Portal. All the aforementioned documents are available, in Italian only, at the following URL address: https://gareappalti.bancaditalia.it.

Should the Portal be unavailable or in any case of force majeure, art. 14 of the Conditions will apply. Any responsibility stemming from non-compliance with the Conditions and the Instructions will be borne solely by the candidate. The conditions, requisites and rules for participation to this procedure are established in the Concession Notice, in these Awarding Rules and related attachments, which are an integral part of the Concession Notice.

Economic operators willing to submit an offer for this procedure and not yet registered to the Portal are advised to apply for registration without delay and well in advance of the final term for offer submission since the registration process may take up to 16 working days to complete.

The Responsabile unico del procedimento (Senior officer in charge of the procedure, pursuant to Article 31 of the Code) is Gianfranco Sortino.

1. OBJECT OF THE PROCEDURE

The object of this procedure is the granting of up to three Concessions which will enable the holder (hereinafter also "Network Service Provider" or "NSP") to design, implement, deliver and operate its own connectivity solution intended to securely exchange business information between the market participants connected via them and the Eurosystem market infrastructures through the ESMIG.

The Connectivity Services to be provided by the selected NSP(s) are detailed in the "Concession Contract" (Annex AR.1) and its Attachments annexed to these Awarding Rules. This Annex together with the "Administrative documentation templates" (Annex AR.2) are integral parts of these Awarding Rules.

Each of the selected NSPs may not hold more than one Concession at any given time.

The Concessions will be awarded to up to three candidates offering the lowest maximum prices as specified in par. 2.5 of these Awarding Rules for the set of services listed in the Busta economica (see par 2.5 below).

The estimated value of the three concessions as a whole is € 541.700.065,00.

This estimate is based on:

- the current annual traffic volume for T2 (i.e. 250.000.000 msg SnF; 800.000 msg RT; 100.000 files SnF; 1.000.000 MB via U2A) and T2S (i.e. 2.200.000.000 msg SnF; 8.000.000 msg RT; 1.000.000 files SnF; 3.000.000 MB via U2A) and some assumptions regarding the future traffic volume of TIPS and other services like ECMS;
- the current market prices for T2 and T2S connection services and some assumptions on TIPS connection services prices.

Pursuant to Article 168 of the Code, in order to allow the concessionaires to recoup the investments made in operating the services together with a return on invested capital and also in order to ensure to the newcomers the possibility to access to this market, **the concessions will last ten years**.

The evaluation of the offers will be based on the criteria described in par. 2.5 below.

The Banca d'Italia will sign, in the interest and in the name of the Eurosystem, with each of the selected NSPs a Concession Contract governed by the Italian law as laid down in the Annex AR.1 governing the contractual relationship. The Banca d'Italia and the Eurosystem will not be involved in the contractual relationship between the selected Network Service Providers and their customers.

Following up on the award of the Concession Contracts, it is expected that Eurosystem central banks will conduct procurement procedures, in line with Directive 2014/24/EU[2] and with the applicable national procurement law regimes, with the purpose of awarding contracts for the provision of connectivity services on the basis of the terms contained in the Concession Contracts.

These procurement procedures may be conducted by individual Eurosystem central banks or jointly by two or more Eurosystem central banks.

The Concession and the Concession Contract will have a term of ten (10) years from the Go-Live Date (as defined in the Concession Contract, Art. 1.1).

In case of termination of one or more Concessions after the award but before the expiry of the 10 years term, the contracting authority may, at its sole discretion: not award a replacement concession; or award one or more replacement concessions to the candidate(s) in the selection procedure ranked highest behind those which were awarded a Concession; or launch another selection procedure to award one or more replacement concessions, if the ranking list doesn't allow for the previous option. The above-mentioned replacement Concession shall last for ten (10) years from the successful conclusion of the Compliance Check that shall take place according to the "Timing" provisions set forth in Article 3.1 of the Concession Contract. **The number of Concessions will not exceed three at any given time.**

All activities carried out in the Banca d'Italia's premises will be subject to the provisions of the Italian law concerning safety at work. In particular, workers shall be informed about the so-called "risk of interference", i.e. the risks potentially arising from the work performed in the same period and in the same venue by more than one economic operator. To this end, suitable documentation[3] will be provided to the NSP(s) and – if needed – to the their sub-contractor(s).

National safety laws must be complied with in relation to activities performed in other Central Bank's premises.

[2] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, OJ L 94, 28.3.2014, p. 65–242.

[3] "DUVRI – Documento Unico per la Valutazione dei Rischi di Interferenza".

2. RULES OF PARTICIPATION AND PARTICIPATION REQUIREMENTS

2.1 Economic operators admitted to the procedure

All entities referred to in Art. 45 and 48 of the Code can submit an offer. Candidates must meet, **under penalty of exclusion**, the requirements referred to in Art. 80 and 83 of the Code, along with the technical/professional ability requirement listed below. Requirements must be met from the offer submission date and be kept throughout the selection procedure and the contract execution period.

2.1.1 Technical/professional ability requirement

Three references for the provision of connectivity services and/or data transmission services, each one having a total turnover in the last three years from the offer submission date of at least 1 million euros.

2.2 Additional participation requirements

Under penalty of exclusion, by the offer submission deadline candidates must:

- have a written guarantee and a guarantor commitment issued to them in conformity with par. 2.4 below;
- pay the contribution fee to the Autorità Nazionale Anticorruzione (or ANAC, i.e. the Italian Anticorruption Authority) as explained in par. 2.4 (point 5) below.

The following paragraphs explain how to declare and prove that the participation requirements and conditions are met.

2.3 Offer submission

The offer must be submitted, under penalty of exclusion, via the Portal, using the "RdO – Richiesta di Offerta" (Request for proposal) identified by code rfq_522.

The offer must include:

- a "**Busta amministrativa**" ("Qualification envelope");
- a "**Busta economica**" ("Commercial envelope").

Under penalty of exclusion, the offer must be uploaded to the Portal by the deadline laid down in par. IV.2.2 of the Concession Notice. The offer submission time will be recorded and proved by means of the Portal log files.

The candidate can change and/or complete previously uploaded data before the time-limit for receipt of tenders, as explained in the "Instructions".

The offer submission deadline expires at 16:00:00. Once the time-limit for receipt of tenders expires, the Portal will not allow any change to an already submitted offer and the upload a new offer.

Documents not submitted via the Portal will not be accepted, except as provided for in par. 2.4 with reference to the provisional guarantee and the guarantor commitment.

All the documents must be in English. Any non-English documents must be translated in English; this translation must be certified. This rule will not apply to provisional guarantees and guarantor commitments, for which Italian will be accepted as well.

2.4 Busta amministrativa

The Busta amministrativa must contain the documents hereinafter listed. Candidates are invited to use the downloadable templates available on the Portal, which make an integral and substantial part of these Awarding Rules.

The annexes section ("Area generica allegati") of the Busta amministrativa can be used to upload additional administrative documents requested by these Awarding Rules if the fields in the envelope are insufficient or disabled. Candidates are invited not to submit unrequested documents.

The Busta amministrativa must contain the following documents.

1. A tender application, in conformity with Annex AR.2.1 of these Awarding Rules, digitally signed by a legal representative of the candidate.
2. The European Single Procurement Document(s) (ESPD) referred to in art. 85 of the Code, made in conformity with Annex AR.2.2 of these Awarding Rules, digitally signed by a legal representative of the candidate.
3. The "garanzia provvisoria" (provisional guarantee), issued in conformity with art. 93 of the Code and with the template attached to the Decreto del Ministero dello Sviluppo economico (Ministry for economic development Decree) of 19 January 2018, n. 31 (Annex AR.2.3), amounting to 1% of the concessions' value divided by three (€ 1.805.667,00). The guarantee must be transmitted in conformity with art. 6 of the Conditions.

The amount of the guarantee can be reduced pursuant to art. 93.7 of the Code. To benefit from the reduction(s), the candidate must declare it holds the relevant certification(s) and upload a scanned copy thereof in the Busta amministrativa. In case of temporary associations of economic operators, all economic operators in the association must hold the relevant certification(s).

The amount of the guarantee can be reduced at the conditions explained in the aforementioned art. 93.7 of the Code, to which candidates are invited to refer. The possible reductions and related requirements are summarized hereinafter by way of illustration:

1) by 50% if the candidate holds a certificate of the ISO 9000 series or is a micro, small or medium business;
2) by 30% if the candidate is an Eco-Management and Audit Scheme (EMAS) registered business;
3) as an alternative to number 2), by 20% if the candidate holds an ISO 14001 certificate;
4) by 20% if the candidate holds an EU ecolabel for the services to be provided;
5) by 15% if the candidate holds an ISO 14064-1 or an ISO 14067 certificate;
6) by 30% if the candidate holds a SA8000 certificate or an OHSAS18001 certificate or an ISO 50001 certificate or an UNI 11352 certificate or an ISO 27001 certificate.

The reductions mentioned under numbers 1, 2 (or 3), 4 and 5 can be cumulated. In case of cumulation, the candidate must apply the reductions in sequence, i.e. each reduction must be applied on the amount of the guarantee resulting from the application of the previous reduction(s).

Should the guarantee be issued on paper, the original must be sent to the Banca d'Italia in a sealed parcel bearing the corporate name of the candidate and the caption "Open procedure for the concession of Eurosystem Single Market Infrastructure Gateway (ESMIG) Connectivity Services (Code G011/18) – DO NOT OPEN – NON APRIRE".

The parcel must be **delivered** by the **time limit for receipt of tenders specified in Section IV.2.2 of the Concession Notice** to the following address: **Banca d'Italia, Servizio Appalti, Divisione Appalti informatici, Via Nazionale 91, 00184, Rome (Italy).** It can be:

a) either sent by postal service, in which case it must be sent by registered mail; or

b) hand-delivered directly to the correspondence reception point at the Banca d'Italia, by a person designated for the task or by a courier, on a day which is not a holiday, Monday to Friday, from 8:00 to 16:00 (8:00AM-4:00 PM) Central European Time.

Upon reception, the Banca d'Italia's personnel responsible for correspondence reception will affix a date and time stamp on the parcel as evidence of the date and time of receipt.

The "garanzia provvisoria" must have a duration of at least 270 days (base term) starting from the **time limit for receipt of tenders** and contain an undertaking by the guarantor to extend the duration for an additional 90 days period if the procedure lasts more than 270 days.

The "garanzia provvisoria" will be released:

– for awardees, upon signing of the concession contract;

– for other candidates, upon communication of the award of the concessions, in accordance with art. 93.9 of the Code.

4. A commitment in compliance with art. 103 of the Code, by a bank or financial intermediary or insurance company, to provide, if the candidate is awarded a Concession, a guarantee for non-performance or inexact performance of the Concession Contract (see par. 8 of these Awarding Rules). **The commitment can be included in the same document containing the provisional guarantee and must be submitted in conformity with art. 6 of the Conditions.**

5. Documentation suitable to prove the payment to be executed, **under penalty of exclusion,** of the contribution fee of **€ 500,00** due to the Italian Anticorruption Authority (ANAC). For foreign economic operators the contribution fee can be paid by bank transfer using the following bank account details:

Beneficiary: Autorità Nazionale Anticorruzione
IBAN: IT77O0103003200000004806788
SWIFT (BIC) code : PASCITMMROM
Bank: Monte dei Paschi di Siena
Purpose of the payment: *Taxpayer number or other identification code of the candidate in its country of establishment* - **CIG 77681933A8** .

For more information about the contribution and its payment, candidates can refer to the Authority's website: https://www.anticorruzione.it/portal/public/classic/home/_riscossioni;

6. In case of temporary association of economic operators already established, an authenticated copy of the collective and irrevocable mandate to the lead economic operator.
7. In case of reliance on the capacities of other entities: a) declarations in conformity with art. 89 of the Code; b) the original or authenticated copy of the contract whereby the relied-on entity undertakes the obligation to supply the candidate with the resources it lacks (refer to par. 6 of these Awarding Rules and instructions in the "Busta amministrativa" for details).
8. If the documents are not signed by a legal representative of the candidate, copy of the documentation proving the power of attorney of the signatory.

2.5 Busta economica

The Busta economica must contain, **under penalty of exclusion, the Economic offer, drafted in conformity with the Economic offer form attached to these Awarding Rules (Annex AR.2.4)**.

The Economic offer form must be:

1. **downloaded from the Portal and filled-in**. The Excel file will automatically perform all necessary calculations;
2. **digitally signed, under penalty of exclusion, by a legal representative of the candidate or by a person with suitable powers of attorney** (to be documented as per par. 2.4, point 8 of these Awarding Rules);
3. **uploaded to the "Area generica allegati" (Additional Attachments Area) of the Busta economica.**

The candidate shall copy the Total score, calculated by the Excel file, to Section 2.1.1 of the Busta economica. In case of discrepancy between the total score indicated in the Busta economica and the total score indicated in the Economic offer form, the latter will prevail.

The Area generica allegati of the Busta economica shall also contain a duly signed "**Business Plan**", in which the candidate shall set out:

- the investment needed to implement and the costs of providing and maintaining the connectivity services for each year of the duration of the Concession contract, and
- the gross revenue foreseen on the basis of the prices offered and the volume expected for the connectivity services for each year of the duration of the Concession contract.

The candidate must quote prices for each service indicated in the Economic offer form, except for those marked with "N/A". A zero price quotation or no quotation means that the service is offered for free by the candidate. All prices shall be provided in euros with a maximum precision of 6 decimals.

The candidate must include in the maximum prices offered the costs for data traffic sent

and received from ESMIG (i.e. inbound as well as outbound) and for all other costs related to the service management for ESMIG Services and applications[4]. To avoid any doubt, the maximum prices relate to both the inbound and outbound data traffic. The maximum prices apply for a connection with a basic bandwidth of 10 Mb[5]/s between data centres of the Directly Connected Actors located in the EEA[6] or Switzerland to the ESMIG data centres. All relevant components in the list shall be sized at minimum to allow full utilisation of the basic bandwidth.

The maximum price for the services listed in the Economic offer form shall cover all activities and components that allow a Directly Connected Actor to make use of these services, according to service levels that are equal to those required by the Eurosystem for ESMIG itself, as described in the Concession Contract (Annex AR.1) and its Attachments. If Directly Connected Actors require higher service levels for certain services the selected Network Service Provider is not bound by the maximum price specified in its Economic Offer for these services. The Network Service Provider can also provide additional or different services to the Directly Connected Actors without being bound by any maximum price.

The MAXIMUM TOTAL SCORE accepted is 700.000. Bids whose total score exceeds the maximum total score will be excluded.

The candidates will be ranked on the basis of a score, calculated by applying certain weight factors (specified below) to the maximum prices offered by each candidate for each of the services listed in the Economic Offer form.

The weight factors are the result of an elaboration based on the current traffic volume for T2 and T2S in operation and on the basis of certain assumptions regarding the future TIPS volume.

The selected Network Service Providers are committed to supply during the Term of the Concession all the services included in the Economic Offer form.

Weight factors for each connectivity service for production environment:

Production Service	Weight factor ($W_{Prod\ i}$)
A.1 (Prod)	0,35
A.2 (Prod)	1,45
A.3 (Prod)	0,28
A.4 (Prod)	3,32
B.1 (Prod)	3,46
B.2 (Prod)	1,87

[4] For more details please refer to the Technical Requirements and Compliance Check – Annex AR.1.1.

[5] 1Mb = 1 megabit = 10^6 bits.

[6] The European Economic Area (EEA).

Production Service	Weight factor ($W_{Prod\ i}$)
B.3 (Prod)	2,22
B.4 (Prod)	39,87
C.1 (Prod)	5676938,58
C.2 (Prod)	19910,65
C.3 (Prod)	2883,32
C.4 (Prod)	110,13
C.5 (Prod)	27621,37
C.6 (Prod)	2093,41
C.7 (Prod)	35288,90
D.1 (Prod)	20,77
D.2 (Prod)	0,03
E.1 (Prod)	4,00
E.2 (Prod)	10,00
F.1 (Prod)	71,51

Weight factors for each connectivity service for the test and training environment(s)

Test & training Service	Weight factor ($W_{T\&T\ i}$)
A.2 (T&T)	0,15
A.3 (T&T)	0,03
A.4 (T&T)	0,33
B.2 (T&T)	0,19
B.4 (T&T)	3,99
C.1 (T&T)	567693,86
C.2 (T&T)	1991,06
C.3 (T&T)	288,33
C.4 (T&T)	11,01

Test & training Service	Weight factor ($W_{T\&T\ i}$)
C.5 (T&T)	2762,14
C.6 (T&T)	209,34
C.7 (T&T)	3528,89
D.2 (T&T)	0,01
E.1 (T&T)	0,40
F.1 (T&T)	7,15

Below is the final score calculation formula to be applied by the Selection Panel on the basis of the prices indicated in the offer.

The total score for a j indexed candidate is calculated according to the following formula:

$$T_j = \sum_{i \in \{A1,A2,A3,A4,B1,B2,B3,B4,C1,C2,C3,C4,C5,C6,C7,D1,D2,E1,E2,F1\}} P_{Prod\ i,j} \times W_{Prod\ i} + \sum_{i \in \{A2,A3,A4,B2,B4,C1,C2,C3,C4,C5,C6,C7,D2,E1,F1\}} \left[P_{T\&T\ i,j} \times W_{T\&T\ i}\right]$$

$P_{Prod\ ij}$ is the maximum price offered by the Network Service Provider indexed with j for the service i in the Production environment.

$P_{T\&T\ ij}$ is the maximum price offered by the Network Service Provider indexed with j for the service i in the T&T environment.

$W_{Prod\ i}$ is the weight of the service i in the Production environment.

$W_{T\&T\ i}$ is the weight of the service i in the T&T environment.

The three candidates with the lowest total score T_j will be awarded one concession each.

The maximum price for item C.5 (TIPS A2A message transmission) is limited to € 0,000500 for the production environment to € 0,000250 for the test and training environment. Bids where the prices for these items exceed the respective price cap will be excluded.

The list of maximum prices offered by the selected candidates shall constitute the list of maximum prices according to Art. 7.3 of the Concession Contract.

3. COMMUNICATIONS AND CLARIFICATIONS

Further information and/or clarifications on the content of the Concession Notice, these Awarding Rules, the Concession Contract and their Annexes can be requested to the

Banca d'Italia. Requests, to be made in English, must specify the name of the relevant document (see paragraph 11 "Annexes") and can be transmitted using the messaging function of the Portal. The economic operators not yet registered to the Portal can send their requests to servizio.app.appalti.informatici@bancaditalia.it. The requests must be received at least 15 days before the time limit for receipt of tenders specified in point IV.2.2 of the Concession Notice. All clarifications and any subsequent communications relating to the procedure will be published on the Portal.

4. PARTICIPATION OF TEMPORARY ASSOCIATIONS OF ECONOMIC OPERATORS

Temporary associations of economic operators as indicated in Art. 45 and 48 of the Code or established in accordance with the legislation of the relevant member state[7] may submit offers.

Such groups may be already established or not yet established.

Under penalty of exclusion, an economic operator cannot participate in more than one group of economic operators or take part to this selection procedure both on its own and as a member of a group of economic operators.

If the group of economic operators is already established, the legal representative of the lead economic operator ("mandataria", pursuant to Art. 48 of the Code) must sign the declaration in conformity with Annex AR.2.1 of these Awarding Rules, the Economic Offer and the Business Plan

If the group of economic operators is not yet established, the person(s) empowered to represent each of the economic operators jointly participating must sign the declaration in conformity with Annex AR.2.1 of these Awarding Rules, the Economic Offer and the Business Plan.

Each economic operator in the group must submit a ESPD as laid down in Annex AR.2.2 of these Awarding Rules.

The concessions concern a unique and homogenous service. No grounds for the identification of a "prestazione principale" (main activity) pursuant to art. 48 of the Code therefore exist. As a consequence, only "raggruppamenti temporanei di imprese orizzontali" (horizontal temporary associations of economic operators) pursuant to art. 48 of the Code are admitted.

The lead economic operator's share of contract execution must be greater than any other economic operator's in the group, pursuant to art. 83, para. 8, of the Legislative Decree 50/2016.

With reference to the **requirement laid down in par. 2.1.1 of these Awarding Rules (references)**, in case of temporary associations of economic operators it **must be met by the group as a whole**. **The lead economic operator must provide at least one of the references**.

All the economic operators in a temporary association of economic operators will be jointly liable for the execution of the Concession contract.

[7] See Arts. 48 and 83 of the Code for the regime applicable to Italian groups of economic operators that can submit offers.

5. SUBCONTRACTING

Pursuant to Art. 105 of the Code, the candidate – participating on its own or as member of a temporary association – must indicate in Part. 2, let. D of the ESPD what activities, necessary to execute the Concession Contract, it may subcontract to third parties ("Subcontractors").

The selected NSP(s) will remain the sole responsible to the Banca d'Italia and to the Eurosystem for the service, including the subcontracted services.

Subcontracting will be subject to the following conditions:

- the candidate must indicate in its offer the parts of services that it intends to subcontract;
- the selected NSP(s) must deposit with the Banca d'Italia an authenticated copy of any such subcontract(s) at least twenty days prior to the beginning of the performance of the subcontracted services;
- upon depositing each subcontract, the selected NSP(s) must declare any situation of control (in the meaning of Art. 2359 of the Italian Civil Code) in respect of the subcontractor(s);
- upon depositing each subcontract, the selected NSP must submit a declaration that the subcontractor fulfils the requirements referred to in Art. 80 of the Code;
- the subcontractor(s) must comply with relevant safety at work regulations;
- the selected Network Service Provider(s) must ensure that compliance with these requirements is maintained by all subcontractors for the whole term of the Concession Contract.

All the above obligations will apply throughout the term of the Concession Contract.

If the consent is not denied within twenty days from the delivery by the Network Service Provider of all request documents, the Eurosystem shall be deemed to have granted its consent.

In the event of a failure to present the aforementioned documentation within the term specified above, the subcontracting will not be consented.

The performance of the subcontracted services cannot be further delegated.

The NSP will be jointly liable with all Subcontractor(s) for the latter's performance of all obligations deriving from applicable laws as well as from the collective bargaining in force in the place where the contract is to be performed, concerning: security and safety at the workplace, worker's mandatory insurance, social security and social benefits, working conditions and economic treatment.

In the event that a subcontractor no longer fulfils the above requirements, the consent to subcontract with such subcontractor will be withdrawn.

6. RELIANCE ON CAPACITIES OF OTHER ENTITIES

The candidate can fulfil the technical capacity requirement laid down in par. 2.1.1 of these Awarding Rules by relying in part or in whole on the capacities of other entities, in compliance with Art. 89 of the Code.

Relied-on entities must meet, **under penalty of exclusion of the candidate**, the requirements laid down in art. 80 and 83 of the Code. The relied-on entity must individually submit the self-attested declarations in conformity with the ESPD attached to these Awarding Rules.

The candidate must submit:

a) a declaration attesting its reliance on the technical capacities referred to in par. 2.1.1 of these Awarding Rules, necessary for participating to the procedure, specifying which capacities of the entity it relies on;

b) a declaration signed by the relied-on entity whereby such entity undertakes the obligation to the candidate and to the contracting authority to make available for the entire duration of the Concession Contract the necessary resources that the candidate lacks;

c) the original or authenticated copy of the contract whereby the relied-on entity undertakes the obligation to the candidate to supply the necessary resources. The following elements must, inter alia, emerge from the contract: i) the description of the resources (e.g. staff, equipment, etc.) and requirements that the relied-on entity will make available to the candidate for the entire duration of the Concession; ii) the relied-on entity's economic interest in doing so.

In accordance with Art. 89, par. 7 of the Code it is prohibited, **under penalty of exclusion**, that more than one candidate rely on the same entity or that both the relied-on entity and the economic operator relying on its capacity participate to the selection procedure.

All declarations must be made by the legal representative of the relied-on entity or by a person with specific powers of signature in the name and on behalf of the relied-on entity (demonstrated by the enclosure within the Busta amministrativa of an authenticated copy of the documentation attesting to such power of attorney).

7. AWARDING PROCEDURE

The Concessions will be awarded pursuant to Art. 173 and 95 of the Code, **on the basis of the lowest overall price to be offered to the Directly Connected Actors, calculated in accordance with the rules and the awarding criteria specified in par. 2 above.**

* * *

The awarding procedure will be carried out by a Selection Panel appointed after the deadline for the submission of the offers. The activities of the Selection Panel will be put on record.

The Selection Panel will, inter alia, perform, as necessary, the activities referred to in Art. 97 of the Code concerning abnormally low offers.

The awarding procedure will start at the time and on the day specified in point VI.3 of the Concession Notice in the Banca d'Italia's premises "CDM – Centro Donato Menichella" located in Viale Luigi Einaudi (a side-street of Via di Vermicino) – Frascati (Rome).

The public sessions of the Selection Panel may be attended by one delegate for each economic operator which participates to the procedure. For each public session of the Selection Panel, the name of the delegate must be notified at least two days in advance

using the "Area messaggi" of the Portal, by a legal representative of the economic operator, specifying the powers of representation or proxy conferred on the delegate and attaching a photocopy of an identity document of the legal representative.

Admission of candidates' delegates to the public sessions of the Selection Panel is conditional on compliance with the rules in force at the Banca d'Italia and on presentation of the original identity document of the delegate. Delegates must arrive at least ten minutes in advance of the time at which sessions of the Selection Panel are scheduled to begin.

In the first public session the Selection Panel will verify the presence, regularity and completeness of the documents contained in the Busta amministrativa. The Panel may conduct further checks on the administrative documentation in one or more session(s) not open to the public.

Pursuant to Art. 83 of the Code, the Selection Panel may request the candidate – via the "Area messaggi" of the Portal – to provide clarifications concerning the content of the certificates, documents and declarations submitted. These clarifications must be received, under penalty of exclusion, by the date specified in the request.

All Selection Panel decisions will be formally communicated to the candidates concerned via the Portal.

The company names of the candidates admitted and excluded on the basis of the examination of the administrative documentation will be published in the "Area pubblica" (public section) of the Portal.

In the second public session the Selection Panel will open the commercial envelopes of the admitted candidates, read their total scores and consequently establish the provisional ranking of the candidates. The second public session can be held on the same day of the first public session or the following day or another day which will be communicated to all candidates via the Portal.

If an offer is considered abnormally low, the Selection Panel will request – via the "Area messaggi" of the relevant RDO of the Portal – the candidate to provide adequate explanations pursuant to art. 97 of the Code.

The Selection Panel and the officer in charge of the procedure, as indicated in point II.2.14 of the Concession Notice will examine, in non-public session(s), the explanations submitted by the candidates pursuant to Art. 97 of the Code.

After the aforementioned verifications, the Selection Panel will provisionally rank the candidates in accordance with the award criterion provided for in par. 2 of these Awarding Rules and propose the awards.

The Banca d'Italia will check if the first three candidates meet the requirements set out in the Concession Notice and these Awarding Rules and its Annexes.

In particular, pursuant to art. 85, par. 5 of the Code, the Banca d'Italia will ask awardees to prove, within 10 days of the request, that they meet the requirement laid down in par. 2.1.1 of these Awarding Rules. Should the candidate fail to provide such a proof it **will be excluded**, it will be reported to the ANAC and the provisional guarantee will be executed. The Banca d'Italia may grant an extension of up to 10 days of the aforesaid term if the

candidate proves that it couldn't meet the original 10 day deadline due to exceptional circumstances.

Before the concessions are awarded, the Banca d'Italia will also check that no grounds for exclusion pursuant to art. 80 of the Code exist for the first three candidates in the ranking. To this effect, awardees will be requested to provide self-attested declarations in conformity with Annex AR.2.5 within 10 days of request.

In case of untruthfulness or serious misrepresentation in declarations in lieu of certificate concerning the fulfilment of the requirements for participation in the procedure or in case the fulfilment of the aforementioned requirements is not demonstrated, **the candidate will be excluded**, the award, if already adopted, will be revoked, and the next-in-rank candidate will be verified.

The Banca d'Italia will award the concessions once the body in charge of the legitimacy check of the procedure in the Banca d'Italia has vetted the selection procedure, pursuant to art. 33, para. 1 of the Code.

The award decisions will be published on the Portal and on the ECB website and will be communicated to all candidates via the Portal.

Each award will take effect once all the aforementioned checks on the relevant awardee are completed.

Pursuant to Art. 95, para. 12 of the Code, the Banca d'Italia reserves the right not to award one or more Concessions if the offers received are not deemed adequate or convenient, upon a justified proposal by the Selection Panel.

In any case all the costs incurred to take part to this selection procedure shall be borne solely by the candidates.

8. SIGNING OF CONCESSION CONTRACTS

The signing of the Concession Contracts shall take place at least 35 days after the award notice is sent to the candidates (standstill or grace period).

The Banca d'Italia shall sign the Concession Contracts, in the interest and in the name of the Eurosystem, in conformity with Annex AR.1 of these Awarding Rules.

The signing is subject to the awardee's presentation, within 15 days of receipt of the request, of:

- the documents proving the issuance of a guarantee for the benefit of the Banca d'Italia to be executed, inter alia, in case of non-compliance with Concession Contract obligations, according to the terms and conditions specified in par. 2.4 of these Awarding Rules. The Guarantee ("Garanzia definitiva") must be made in Italian or in English and must be issued in conformity with art. 93 and 103 of the Code and with the template attached to the Decree of the Ministry for economic development ("Ministero dello Sviluppo economico") of 19 January 2018, n. 31, attached to these Awarding Rules (Annex AR.2.3). In particular, it shall be provided by the selected Network Service Provider(s) by means of a bank guarantee or insurance policy before the signing of the Concession Contract, to guarantee, throughout the entire duration of the Concession Contract, the performance of all obligations under the Concession Contract and its Attachments or relating to the

Concession Contract for a value of **€ 18.056.668,00.**The Guarantee must also cover the payment of any penalty that may be applied on the basis of the relevant Concession Contract provisions. The Guarantee shall be executed in the cases and for the amounts indicated in art. 103 of the Code, in these Awarding Rules, in the Concession Contract and its Attachments. The Guarantee will be progressively released in 8 installments each of 10% of the original amount at the end of each year of the Concession Contract execution. The remaining 20% will be released at the end of the Concession Contract period;

- declarations in conformity with Annex AR.2.5, issued by all relevant subjects;
- [only for temporary associations of economic operators not yet established at the time-limit for receipt of tenders], an authenticated copy of the articles of the association.

If the selected Network Service Provider fails to provide the required documentation within the aforesaid term, the award can be revoked and a Concession may be awarded to the next-in-rank of the non-winning candidates.

Upon signature of the Concession Contract, the selected Network Service Provider(s) must demonstrate the power of attorney of the representative who signs the Concession Contract on its behalf, by means of a suitable document authenticated as required by law, if such document has not already been submitted in the course of the procedure.

The results of the procedure shall be published in the same Official Journals, newspapers and websites as the awarding documents.

The award will be revoked and the Concession Contract will be terminated in case of:

- untruthfulness or serious misrepresentation of the declarations in lieu of certificate or if it's proved the participation requirements were never met or if they are lost by the NSP;
- failure to submit the "Garanzia definitiva";
- unsuccessful completion of the network acceptance tests in accordance with the Technical Requirements and Compliance Check – Annex AR.1.1;

the Concession will then be awarded to the next-in-rank of the non-winning candidates.

The award may be revoked and the Concession Contract may be terminated in case of public interest reasons, also stemming from modifications of the factual situation or from a new evaluation by the Eurosystem of the original public interest. In such case, the selected Network Service Providers shall not have any claim against the Eurosystem or the Banca d'Italia except as required by Article 176, para. 4 of the Code.

9. PRIORITY OF DOCUMENTS

In the event of any conflict or inconsistency between relevant provisions of the "Concession Notice", these "Awarding Rules" and the Annexes hereto, the "Concession Notice" shall prevail over any relevant provision of the "Awarding Rules" and the "Awarding Rules" shall prevail over its Annexes.

10. DATA PROTECTION

In accordance with the European and national legislation, please be informed that Banca d'Italia will process the following personal data belonging to the corporate officers of the companies participating in or winning the tender:

- the names and their identity document numbers;
- criminal records, where necessary for verifying that they meet the requirements set out for entering into public contracts.

The data are needed for due diligence purposes and for the management and creation of the contractual relationship arising out of the Contract.

Please note that, in the event that criminal records are obtained, the regulatory sources that authorize the processing of criminal records are the European and national procurement legislation.

Data are stored in paper format or processed with IT procedures, with the use of security measures which protect the privacy of the personal data and which prevent unauthorized access to such data by third parties or unauthorized persons.

Data shall not be disseminated externally. Data may be shared with third parties only as provided by law.

Data will be processed for the time strictly necessary to achieve the purposes for which they have been collected.

The data may be accessed by the Head of the Tenders Directorate and the Head of the IT Planning Directorate and the employees of these Directorates authorized to processing data.

Data subjects can exercise their rights with respect to the data controller (Banca d'Italia, Organization Directorate, Via Nazionale 91, 00184 ROME, e-mail org.privacy@bancaditalia.it). These rights include the right to access their personal data and the other rights granted by law, including the right to obtain rectification, integration or erasure of data; the right to anonymize the data or to block the use of any data used in violation of the law; the right to object, on legitimate grounds, to the processing of personal data.

The Data Protection Officer of Banca d'Italia can be contacted at Via Nazionale 91, 00184 ROME or at the e-mail address responsabile.protezione.dati@bancaditalia.it.

Data subjects can file a complaint with the Italian Data Protection Authority if they consider that their data are processed in violation of the law.

11. ANNEXES

The "Awarding Rules" ([AR]- Awarding Rules) includes the following Annexes:

[AR.1] – Concession Contract

[AR 1.1] – Technical Requirements and Compliance Check

[AR 1.2] – Business Requirements

[AR 1.3] – Hosting Terms and Conditions

[AR.2] – Administrative Documentation and Forms

[AR.2.1] – Tender application

[AR.2.2] – European Single Procurement Document (ESPD)

[AR.2.3] – Decreto del Ministero dello Sviluppo economico of 19 January 2018, n. 31 ("Garanzia provvisoria" and "Garanzia definitiva")

[AR.2.4] – Economic Offer

[AR.2.5] – Declaration in lieu of certificate for antimafia checks (to be provided only by awardees before concession contract signature)

PER DELEGA DEL DIRETTORE GENERALE

Firmato digitalmente da
VINCENZO MESIANO LAUREANI

EUROSYSTEM SINGLE MARKET INFRASTRUCTURE GATEWAY (ESMIG)

TECHNICAL REQUIREMENTS AND COMPLIANCE CHECK

- Attachment 1.1 to the Concession Contract -

TABLE OF CONTENT

1. INTRODUCTION

The Eurosystem operates the financial market infrastructure for the settlement of payments (TARGET2), TARGET Instant Payment Settlement (TIPS) and securities (TARGET2-Securities, or T2S). These platforms form the backbone of the European financial market.

TARGET2 is the real-time gross settlement (RTGS) system. Central banks and commercial banks can submit payment orders in euro to TARGET2, where they are processed and settled in central bank money, i.e. money held in an account with a central bank.

When investors buy and sell securities the security and payment need to change hands – a process called securities settlement. TARGET2-Securities, or T2S, is a safe platform where the exchange can happen simultaneously, i.e. where delivery versus payment is possible.

TIPS is a new market infrastructure service launched in November 2018. It enables payment service providers to offer their customers the possibility to transfer funds in real time and around the clock, every day of the year. This means that thanks to TIPS, individuals and firms are able to transfer money between each other within seconds.

The Eurosystem has launched a project to consolidate TARGET2 and T2S, in terms of both technical and functional aspects. The objective is to meet changing market demands by replacing TARGET2 with a new real-time gross settlement (RTGS) system and optimising liquidity management across all ESMIG. The new consolidated platform will be launched in November 2021.

Another project was launched to implement a common Eurosystem Collateral Management System (ECMS) for managing eligible assets as collateral in credit/liquidity absorbing operations. This single system will replace the current fragmented and decentralised structure composed of 19 local NCBs' collateral management systems. The ECMS will be launched in November 2022.

T2, T2S, TIPS and ECMS are reachable via the Eurosystem Single Market Infrastructure Gateway (ESMIG). The ESMIG is accessed by the Directly Connected Actors (Di.Co.A.) in two modes: "application to application" (A2A) and "user to application" (U2A). The A2A interaction is achieved through two different protocols: Data Exchange Protocol (DEP) and the Message Exchange Processing for TIPS (MEPT).

This document contains the technical requirements that the NSP has to fulfil and the compliance check describing the test cases. Test cases are mapped one to one against the technical requirements.

2. THE COMPLIANCE CHECK WORKFLOW

The criteria for accessing to the compliance check are defined in the following. This section recalls for convenience the two most relevant steps:

- STEP 1 – Project check
- STEP 2 – Running through the test cases

Step 1 is preliminary to the Step 2.

STEP 1 – Project check

In the Technical Solution, the NSP describes the overall architecture by analysing the solution (including technological implementation details from the physical layer to the application layer), the integration among the different components involved in the solution and how the various systems are managed through their respective element managers. The Technical Solution must describe the Connectivity Services and how does the infrastructure looks like. It also must illustrate how all the requirements are matched, i.e. it must correlate the implementation details of the solution to all of the Requirement IDs. The Technical Solution is accepted by the ESMIG OPERATOR only upon successful verification that it meets all the above requirements.

STEP 2 – Running through the test cases

All tests will be conducted on site (i.e. in Banca d'Italia) in cooperation with the NSP. If no Di.Co.A.s are ready in time for the testing phase, they will be emulated by a Di.Co.A. emulator.

Every test case is split into four sections:

1. *Detailed test procedure*: how to perform the test;
2. *Expected result*: what is the outcome of test, i.e. what is the result of the detailed test procedure;
3. *Outcome*: the actual test result; a test can either fail or pass, if it fails then a follow up action is triggered, if it passes then no follow up action is needed and it is possible to proceed straight with the next test;
4. *Formal acceptance*: contains the signatures of the ESMIG Operator testing team staff and the NSP testing team staff performing the test all formally accepting the test result.

Some tests are run in *negative mode*: not only the functionality of the given test condition must be shown, but also additional tests are run to show that in the case that the test condition is not fulfilled, the test result is either a reject or drop.

If a test case identifies a defect and triggers corrective actions, these actions shall be addressed before the end of the user testing phase. Any defect should be remedied or a workaround must have been agreed before the formal acceptance.

Acceptance Test Criteria

Three types of criteria govern the Compliance Check Procedure. The entrance criteria have to be met before the Compliance Check Procedure is started. The acceptance criteria determine the successful completion of the test cases. If the termination criteria are fulfilled, the testing has to be suspended due to major technical issues or immaturity of the solution.

Entrance criteria

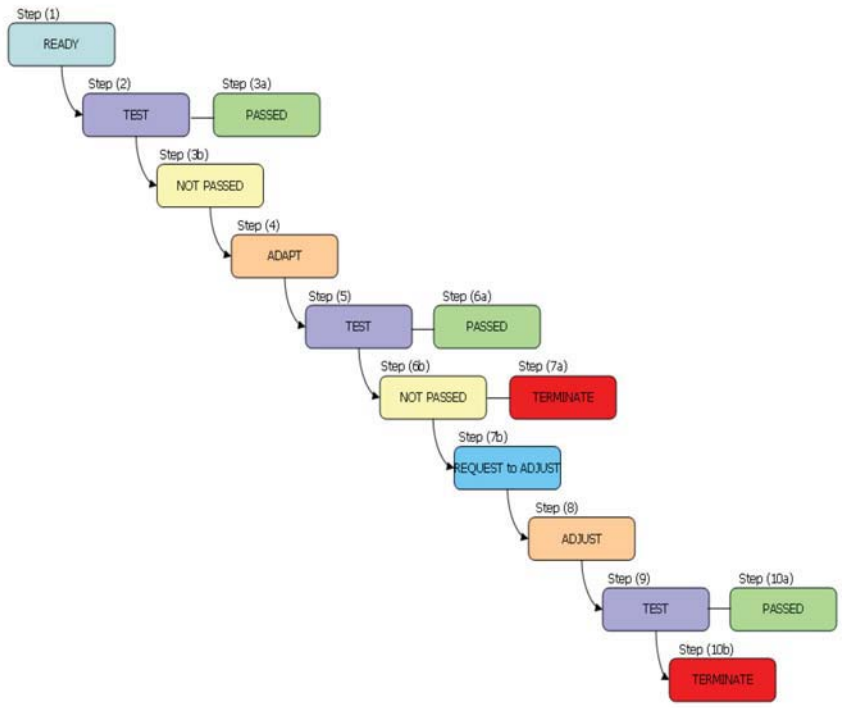
As an entrance criterion, the NSP has passed Step 1 and then communicated to the ESMIG Operator the readiness of its Network for acceptance testing. The NSP has provided to the ESMIG Operator confirmation of the successful completion of the NSP's internal tests. After the ESMIG Operator confirmed the readiness for the Compliance Check Procedure, an acceptance entrance meeting has been held and the ESMIG Operator and the NSP have agreed to start acceptance testing activities.

Acceptance criteria

The acceptance testing phase is completed when all of the following conditions are matched:

- all acceptance test cases have been executed;
- except otherwise agreed with a specific action plan, the NSP has resolved all reported defects;
- all contingency plans and procedures have been successfully tested;
- the NSP's infrastructure has been running without major issues or incidents for at least 7 consecutive calendar days;
- the NSP and the ESMIG Operator have held an acceptance testing exit meeting and agree that the acceptance testing stage has been successfully completed.

The following picture gives a visual representation:



The acceptance flow can be split into 10 different steps: (step 1) ready for acceptance, (step 2) performing the tests, (step 3a) all tests are passed, or (step 3b) some tests are not passed, (step 4) adapt[1], (step 5) tests are repeated, (step 6) some tests are not passed, (step 7a) terminate (i.e. test case is failed), or (step 7b) request to adjust, (step

[1] The "adaptation" starts with listing the deficiency(ies) during the test, then the analysis of the deficiencies by the NSP can lead to a list of remediation to be taken.

8) adjust, (step 9) tests are repeated, (step 10a) all tests are passed, or (step 10b) terminate (i.e. test case is failed).

Termination criteria

If 12 tests have failed, acceptance testing is interrupted for a week. A meeting will be scheduled to check if and what corrective measures can be taken. The staff involved in the acceptance testing shall agree on the measures and a schedule for the next steps.

If the NSP then still fails a repeated set of at least 6 tests, the ESMIG Operator shall be entitled to terminate the Concession Contract.

3. SERVICE LIFECYCLE

3.1 Governance

Project Managers

Requirement ID	ESMIG.30010

The NSP must appoint a Project Manager (PM) who is the responsible central contact person coordinating all required activities and who will communicate with the ESMIG Operator.

The PM has the following duties:

- to maintain the relationship with the ESMIG Operator;
- to coordinate the rollout of the NSP solution;
- to cope with all the issues during the rollout and, when needed, escalate the problem internally within the NSP's organisation;
- to monitor the deadlines of the implementation schedule;
- to prepare a monthly project progress report and to have regular meetings with the ESMIG Operator.

Detailed test procedure:	The NSP' PM is appointed, he/she is the central contact person coordinating all required project activities and central point for coordinating the communication with ESMIG PM. [desk check] Jointly review the relevant documentation provided by the NSP (desk check). List the PM's duties as outlined in the applicable NSP's documentation. Compare the list with the duties outlined above. [desk check]
Expected result:	The NSP has appointed their own PM, the ESMIG Operator is informed about the PMs contact details and the PM is in charge of the duties outlined above.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team _____ date____/____/____

Connectivity service catalogue

Requirement ID	ESMIG.30020

The NSP must develop a catalogue of Connectivity Services as part of the ESMIG overall service catalogue to the ESMIG Operator and the Di.Co.A.s. The content of the Connectivity Services catalogue includes, at least, a description of detailed services and service levels (such as detailing performance, availability and support commitments).

The content of the Connectivity Services catalogue includes the services the NSP offers including:

- Detailed Services,
- Service Levels, performances, availability and support commitments,
- Support for dedicated connectivity solutions,
- Support for backup/Alternative network access solutions,
- Procedures to assure the continuity of service operation.

Detailed test procedure:	Jointly read the Connectivity Service catalogue, verify that it includes a description of detailed services and service levels. The Connectivity Service catalogue contains the topics listed above. [desk check]
Expected result:	The NSP has a Connectivity Service catalogue with all the expected contents.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Operation and Escalation manual

Requirement ID	ESMIG.30030

The NSP must provide the ESMIG Operator with the following documents:

1. **Operations Manual**, which describes the network related components installed in the premises of the ESMIG Operator and contains a complete list of monitored elements and the operational procedures specific to the ESMIG Operator – NSP relation;
2. **Escalation Manual**, which formalises the escalation process in normal and abnormal situations;
3. **User Guides**, which include the detailed technical information needed to install necessary software and hardware infrastructure and make use of the provided services.

It is up to the NSP to consolidate more than a single manual into a single deliverable.

The NSP is the owner of its manuals and is responsible for any updates.

Detailed test procedure:	Jointly read the documentation written by the NSP (the Operations Manual, the Escalation Manual and the User Guides) and check if the contents are as expected. [desk check]
Expected result:	The NSP provides and maintains the Operations Manual, the Escalation Manual and the User Guides. Responsibilities are clearly assigned. To ensure the accuracy of the manuals the ESMIG Operator may submit its observations to NSP and the NSP has to take them on board.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Escalation contacts

Requirement ID	ESMIG.30040

The NSP must maintain the escalation contacts within the Operation Manual.

Detailed test procedure:	The NSP Operational Manual contains the escalation contact and the NSP is committed in updating the contact list. [desk check]
Expected result:	Escalation contacts are up to date.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Service Report and Service Compliance Meeting

Requirement ID	ESMIG.30050

The NSP must report on a monthly basis to the ESMIG Operator the availability of the service connections bandwidth utilization, service incidents, SLAs and open points. The report is discussed and reviewed during a monthly Service Compliance Meeting hosted by the ESMIG Operator.

Detailed test procedure:	Read the monthly report on monitored elements. In case a Service Report is not yet available – because for example the infrastructure has just been setup - then agree on the report mock-up, ie. how the report looks like and what contents are expected to be in the report. [desk check]
Expected result:	The NSP prepares, on a monthly basis, reports on the availability of the monitored communication elements and on the bandwidth utilization of the WAN links.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Service Manager

Requirement ID	ESMIG. 30060

After the go-live, the NSP must appoint a Service Manager (SM) that shall act as unique point of contact for all the Service Compliance related issue.

The SM has the following duties:

- to cope with all the issues during the service lifecycle and, when needed, escalate the problem internally within the NSP's organisation;
- to act as unique point of contact for any request for change submitted by the Eurosystem;
- to verify the status of the Service with periodic meetings and produce the Service Status Report;
- to guarantee the service levels are met.

Detailed test procedure:	Verify on the Operational Manual or any other relevant documentation that the SM duties are clearly described and check whether a SM has been appointed. [desk check]
Expected result:	The NSP has appointed a SM whose roles and responsibilities are clearly identified
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

NSP Technical Solution

Requirement ID	ESMIG.30070

The NSP must provide to ESMIG Operator a comprehensive description of its Technical Solution, encompassing:

- network connectivity (Data centre Connectivity, ESMIG Connectivity, Network Topology, Location of ESMIG Operator data centres, Location of NSP's data centres, Network Access methods, List of Equipment at each ESMIG Operator data centre, Integrity and Confidentiality of Data over the Network, Network Address Translation (NAT), Routing Protocols, Cluster Redundancy Protocol (for example VRRP, FGCP, …), Service Presentation and Demarcation Line, Traffic in the NSP Network for ESMIG, Traffic in the NSP Network for Di.Co.A.);
- secure messaging services covering both A2A (MEPT and DEP) and U2A, NOC, NSP's Network Gateways, GCA, NSP's network Services, A2A Messaging Services, Timestamp service, Scalability and failover in NSP's network, WMQ Connection, Client-server connection, Channel and queue configuration, ESMIG Application Flow, A2A Instant Message, File Store-and-forward, A2A Closed Group of Users Solution, Addressing model, CGU definition, CGU Management, User to Application (U2A), User Authentication, User Authorisation, CGU definition, CGU management, Resiliency, Di.Co.A. Emulator);
- security features (Closed Group of Users (CGU), Key Management, A2A Signature and Non-Repudiation Certificate, U2A authentication, Cryptographic Devices, Processes and Roles);
- operational processes (Customer On boarding, Incident/Problem Management, Change Management, Service Monitoring, Business Continuity Services, Network Connectivity Business Continuity, NSP Business Continuity, Di.Co.A. Business Continuity).

The NSP technical description must include a reference to each requirement defined in this document.

Detailed test procedure:	Analyse the Technical Solution deliverable and make sure all requirements are addressed. [desk check]
Expected result:	The NSP has produced a deliverable describing the Technical Solution, where it is plainly and precisely described how all requirements are going to be met.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Delivery of the NSP Technical Solution

Requirement ID	ESMIG.30080

The NSP must deliver the technical infrastructure and necessary software components as described in the NSP's Technical Solution deliverable. Please notice this applies to ESMIG sites, Di.Co.A. Emulator e NSP data centres.

Detailed test procedure:	Check the part list against the Technical Solution and verify jointly that all HW and SW has been installed and configured. [on field]
Expected result:	Technical infrastructure (HW and SW) components have been delivered by the NSP and are installed in the ESMIG sites, i.e. all equipment and applications have been delivered.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

NSP footprint in the ESMIG Platform

Requirement ID	ESMIG.30090

The NSP must deliver their equipment in the sites of the 4CB, located in two different countries. The 4CB data centres are located in Rome and Frankfurt.

The two sites of a NCB are also named as “region”.

T2 and T2S are deployed in both regions, while TIPS is deployed only in the Italian region.

Detailed test procedure:	The NSP has rolled out the solution in the two data centres in Rome and the other two data centres in Frankfurt. [on field]
Expected result:	The NSP footprint is in line with the Technical Solution.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.2 Change management

Change management

Requirement ID	ESMIG.30100

The NSP must apply a change management process covering all of its components (NSP's Network Gateways and network devices). This process is described in the Operation Manual and it will be compliant with Art. 9 of the Concession Contract.

Detailed test procedure:	NSP has a change management process described in the Operational Manual. [desk check]
Expected result:	The NSP applies a strict change management applicable both to Network Gateways and network devices.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.3 Incident management

Incident Management

Requirement ID	ESMIG.30110

The NSP must have an Incident Management process to detect, notify, escalate and resolve any service related failure.

Detailed test procedure:	Verify the NSP has an operational procedure to handle incidents and failures. Review the section concerning the relevant process handling, and verify the notification and escalation processes. [desk check] Simulate a failure disabling the corresponding Ethernet interface(s) on the demarcation. Verify this event is perceived by the NSP's monitoring, check if it triggers an alarm, see how the alarm is handled, and follow it through the incident management process. [on field]
Expected result:	The NSP has developed an operational procedure to detect, notify, escalate and resolve incidents and failures.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

NSP Support Teams

Requirement ID	ESMIG.30120

The NSP must have Support Teams available 24 hours a day, seven days a week, all year around. The NSP Support Teams operate according to the procedures described in the Operation and Escalation manuals.

Detailed test procedure:	Verify how it is possible to contact the NSP Support Teams. Verify the service level offered by the NSP to ESMIG Operator in the available documentation, , and check the service hours. Verify whether an escalation procedure is contained in the manual. [desk check]
Expected result:	The ESMIG Operator can contact NSP Support Teams 7x24x365. The NSP's Support Teams are aware of the procedure described in the Escalation Manual.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Trouble ticketing management

Requirement ID	ESMIG.30130

The NSP must have a central Trouble Ticketing System (TTS) accessible via Internet.

Detailed test procedure:	An ESMIG Operator logs-in the NSP's TTS via the internet, opens a case for testing purposes, and verifies which input fields are available and the time stamp. [on field]
Expected result:	The NSP's TTS records all actions and time stamps at which a service request/update takes place. TTS is accessible via Internet to both the Di.Co.A.s and the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Incident reports

Requirement ID	ESMIG.30140

The NSP must provide to the ESMIG Operator on a monthly basis a list of all incidents handled during the reporting period. The NSP could produce a report in line with their standard internal procedure.

In case of High Priority Incident, the NSP must produce and deliver an incident report to the ESMIG Operator within 24 hours from the occurrence of the incident.

Detailed test procedure:	Check the format and contents of the NSP's monthly reports. Look for the following information: case creation date/time, case closure date/time, impacted Di.Co.A.s, severity of the incident and incident description and reason for closure. NSP provides further details about parameters and values contained in the report upon request. [desk check]
Expected result:	The NSP provides a monthly report containing all the information described in the technical requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Security Incident Handling

Requirement ID	ESMIG.30150

The NSP must report immediately any security incident to the ESMIG Operator.

Detailed test procedure:	Verify that the NSP has an operational procedure to report any security incident to the ESMIG Operator. Verify whether this procedure regulates how to contact the ESMIG Operator and how to manage the information sharing. [desk check]
Expected result:	The NSP has an operational procedure to report any security incident to the ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.4 Problem management

Problem management

Requirement ID	ESMIG.30160

The NSP must have a Problem Management process to detect and resolve the root cause of incidents.

Major problems must be periodically addressed with the ESMIG Operator during the Service Compliance Meeting.

Detailed test procedure:	Verify that the NSP has a process to detect and resolve the root cause of incidents. Verify whether this process includes exhaustive reporting of Major problem that will be addressed in the Compliance Meeting with the ESMIG Operator. [desk check]
Expected result:	The NSP has a process to detect and resolve the root cause of incidents.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.5 Event Management (Monitoring)

Monitoring of NSP infrastructure

Requirement ID	ESMIG.30170

The NSP must proactively monitor all the components of the deployed infrastructure.

Detailed test procedure:	Part I: The Technical Solution document contains a list of the NSP's components. Jointly assess how the NSP monitors the infrastructure (i.e. provides evidence of the monitoring operational procedures). [desk check] Part II: Simulate a failure and check the relevant events are reported on the NSP's monitoring facility, i.e. all failure events are visible on the monitoring facility and an alarm is triggered. Restore to normal operation and verify that the event is cleared. The test is expected to cover at least the following scenario: 1. Simulate a WAN failure and check the relevant indication on the monitoring facility. Restore to normal operation. 2. Simulate a Network Gateway failure and check the relevant indication on the monitoring facility. Restore to normal operation. 3. Simulate an Ethernet interface failure on the demarcation (§ LAN interface specifications) and check the relevant indication on the monitoring facility. Restore to normal operation. [on field]
Expected result:	The NSP gives evidence that all his components are monitored by the NSP.
Outcome:	Please describe the test result: [] PASSED [] FAILED

	If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Monitoring NSP's Network Gateways and network devices through SNMP v.3

Requirement ID	ESMIG.30180

NSP’s components (Network Gateways and network devices) must send SNMP v.3 traps to the ESMIG network monitoring platform. The list of events is bilaterally agreed.

Detailed test procedure:	Ensure a list of relevant events has been bilaterally agreed. Trigger one of such events (for example multiple failure of login attempts or device failure) and verify a SNMP trap is sent from NSP to the ESMIG Operator. [on field]
Expected result:	The NSP triggers an automated SNMP alert in case of occurrence of a monitored event.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.6 IT Service Continuity Management

Support to ESMIG Business Continuity

Requirement ID	ESMIG.30190

The NSP Technical Solution must support the ESMIG Business Continuity ensuring no impact affects the Di.Co.A. technical configuration: in case of ESMIG site recovery, regional recovery or periodic rotations no change is requested to Di.Co.As..

Detailed test procedure:	Part I: Simulate a Business Continuity scenario, i.e. a site isolation of the active site. Simulate a site A failure (disable the interface(s) on the ESMIG DMZ switch where the NSP demarcation is connected), check if the Di.Co.A. Emulator is able to access the ESMIG seamlessly (without any impact or change to the configuration). Restore to normal operation. Part II: Simulate a Business Continuity scenario, i.e. a regional isolation of the active region. Simulate a site A and B failure (disable the interfaces on the ESMIG DMZ switch where the NSP demarcation is connected), check if the Di.Co.A. Emulator is able to access the ESMIG seamlessly (without any impact or change to the configuration). Restore to normal operation. [on field]
Expected result:	The NSP supports both Business Continuity scenarios (site isolation and regional isolation) without any user intervention or impact on Di.Co.A..
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

T2 Business Continuity time objectives

Requirement ID	ESMIG.30200

The NSP supports the T2 Business Continuity with the following time objectives:

- in case of intra-region recovery, between primary and secondary Site in the same region, upon request of the ESMIG Operator, the NSP switches the traffic between the sites in less than 15 minutes;
- in case of inter-region recovery between two Regions (on request of the ESMIG Operator) and/or on periodic rotation occurrence (almost every six months), the NSP shall switch the traffic between the Regions in less than 30 minutes.

Detailed test procedure:	Part I (intra-region recovery): Test the business continuity scenario (intra-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery. Part II (inter-region recovery): Test the business continuity scenario (inter-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery. [on field]
Expected result:	The NSP supports T2 Business Continuity scenarios (site isolation and regional isolation) within the expected time limits.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

T2S Business Continuity time objectives

Requirement ID	ESMIG.30210

The NSP supports the T2S Business Continuity with the following time objectives:

- in case of intra-region recovery, between primary and secondary Site in the same region, upon request of the ESMIG Operator, the NSP switches the traffic between the sites in less than 15 minutes;
- in case of inter-region recovery between two Regions (on request of the ESMIG Operator) and/or on periodic rotation occurrence (almost every six months), the NSP shall switch the traffic between the Regions in less than 30 minutes.

Detailed test procedure:	Part I (intra-region recovery): Test the business continuity scenario (intra-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery. Part II (inter-region recovery): Test the business continuity scenario (inter-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery. [on field]
Expected result:	The NSP supports T2S Business Continuity scenarios (site isolation and regional isolation) within the expected time limits.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

TIPS Business Continuity time objectives

Requirement ID	ESMIG.30220

The NSP supports the TIPS Business Continuity with the following time objectives:

- in case of intra-region recovery, between primary and secondary Site in the same region, upon request of the ESMIG Operator, the NSP switches the traffic between the sites in less than 15 minutes;
- should the second Region be implemented:
  - in case of inter-region recovery (on request of the ESMIG Operator) and/or on periodic rotation occurrence (almost every six months), the NSP shall switch the traffic between the Regions in less than 30 minutes.

Detailed test procedure:	Part I (intra-region recovery): Test the business continuity scenario (intra-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery. Part II (inter-region recovery): The inter-region scenario is currently not envisaged but it was mentioned to assure that NSP will be able to implement it in the future if requested. [on field]
Expected result:	The NSP supports TIPS Business Continuity scenarios (site isolation and, if implemented, regional isolation) within the expected time limits.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

NSP Business Continuity time objectives

Requirement ID	ESMIG. 30230

The NSP shall have in place a solution for the business continuity based on two sites with different risk profiles. A third backup site shall be available to restart from an empty state in the extreme unlikely event of the loss of the primary sites, i.e. cold restart.

The NSP shall manage its disaster recovery solution, which affects the ESMIG connectivity Services, with the following time objectives:

- in case of loss of one of the primary sites the NSP switches the traffic in less than 15 minutes with no data loss;
- in case of loss of both the primary sites the NSP shall activate the backup site in less than 45 minutes in zeroed state. The NSP shall define the procedures with the Direct Connected Actors and the ESMIG Operator to recover the lost traffic.

Detailed test procedure:	Part I (loss of one primary site): Test the business continuity scenario (loss of one primary site) and take note of how long it takes to recover the full service operation: disable the service on one of the primary sites and clock the time elapsed for service recovery. Part II (loss of both primary sites): Test the business continuity scenario (loss of both the primary sites) and take note of how long it takes to recover the operation: disable the service on both the primary sites and clock the time elapsed for service recovery (with empty state). [on field]
Expected result:	The NSP supports Business Continuity scenarios within the expected time limits.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

No single point of failure

Requirement ID	ESMIG.30240

The NSP Technical Solution (and the corresponding roll-out) must avoid any single point of failure (SPOF), i.e. any software or hardware component must be redundant.

Detailed test procedure:	Inspect the Technical Solution and verify whether the technical infrastructure is designed with full redundancy. Prove there is no single point of failure. [desk check] Inspect the implementation rolled-out and check whether it is in line with the technical requirements. Identify deficiencies (if any) and agree on corrective measures to be taken. [on field]
Expected result:	The NSP designs and implements the solution avoiding any single point of failure (SPoF). Additional software and hardware components are redundant.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

DNS functionalities for Business Continuity

Requirement ID	ESMIG.30250

The NSP connects to the ESMIG Domain Name System (DNS) to obtain automatically the current location of the services and URL for A2A and U2A. The ESMIG communicates to the NSP one IP address for each site where a DNS server system - able to provide IP address information to the NSP - will be activated.

It is also possible to agree with the ESMIG alternative non DNS based solutions. In such a case, also a specific detailed test procedure has to be bilaterally agreed.

Detailed test procedure:	Part I – in case there is a DNS Identify the ESMIG DNS servers. ESMIG has communicated to the NSP four IP addresses (one per site) where a DNS server is activated. The NSP uses this information to "route" A2A and U2A to the active ESMIG Site. Check that the DNS disclose to the NSP the IP addresses of the ESMIG Site for the A2A and U2A application services (i.e. both sites in case of active / active). The NSP is able to "route" A2A and U2A requests to the ESMIG. Part II – in case there is no DNS Review the alternative solution as described in the Technical Solution document; examine the alternative solution comparing it to the implementation. Jointly define a testing approach and execute the test [on field]
Expected result:	The NSP interfaces the ESMIG DNS in order to obtain the current location of the services (and URL) for A2A and U2A services.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.7 Release and Deployment Management

NSP Release management process

Requirement ID	ESMIG.30260

The NSP must have a release and deployment management process ensuring no impacts occur on the service, through a rolling approach. Major releases must be announced to the ESMIG Operator at least 6 months before the deployment. Minor releases must be announced to ESMIG Operator at least 4 weeks before the deployment.

Detailed test procedure:	Verify the NSP has a release and deployment management process including the corresponding procedures. The process (and procedures) should provide a rolling approach to release and deployment. Verify whether this process (and procedures) includes the definition of Major and Minor releases and associate the timing mentioned in the requirement. [desk check]
Expected result:	The NSP has a release and deployment management process that is compliant with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Capacity during site/regional failure

Requirement ID	ESMIG.30270

The NSP must ensure that the capacity of all components provided in each ESMIG site are able to handle the whole messaging volumes; i.e. in case of site/regional failure, then the surviving sites must handle the whole traffic without impacting the service level.

Detailed test procedure:	During the whole test (both part I and part II) A2A message traffic is coming simultaneously from the Di.Co.A. Emulator to the ESMIG and from the ESMIG to the Di.Co.A.. Part I: The NSP disables the Ethernet interface(s) at ESMIG site A that are part of the demarcation between the NSP and ESMIG (cfr. ESMIG.30280). The whole traffic is then handled by the remaining link connected to the ESMIG site B. When test outcome is recorded please restore the initial condition. Part II: The NSP disables the Ethernet interface(s) at ESMIG site B that are part of the demarcation line between the NSP and ESMIG (cfr. ESMIG.30280). The whole traffic is handled by the remaining link connected to the ESMIG site A. [on field]
Expected result:	The NSP has to ensure that the link bandwidth to each single ESMIG site (A or B) is able to handle the whole traffic and in case of site failure the link to the remaining ESMIG site is expected to handle the whole traffic.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

3.8 Service Level Management

The boundaries of responsibility (logical demarcation)

Requirement ID	ESMIG.30280

The NSP must define two logical demarcation lines. The demarcation lines define the boundaries of the responsibilities either between the NSP and the ESMIG or between the NSP and the Di.Co.A..

The demarcation line between the NSP's perimetral network device and the ESMIG must be the Ethernet interfaces defined in ESMIG.40040.

The demarcation line between the NSP and the Di.Co.A. is bilaterally agreed by the Parties.

Detailed test procedure:	Verify in the NSP contractual framework template that the boundary of responsibilities between NSP and the Di.Co.A. and between the NSP and the ESMIG are clearly identified. [desk check]
Expected result:	A clear boundary of responsibilities has been defined and agreed. All responsibilities have been clearly identified.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

DEP A2A real-time message delivery time

Requirement ID	ESMIG.30290

The NSP delivers a real-time message from the Sender to the Receiver in less than 2s for the 95% of the messages and 100% in less than 40s. The acknowledgment of the delivery sent back to the sender is not included in the delivery time.

Detailed test procedure:	Send real-time messages from the Di.Co.A. emulator to the Platform at a constant rate – close to the 90% of the overall agreed maximum allowed rate (measured in messages/sec) – for at least 16 hours and record the delivery time for each of the messages. Record the overall number of messages, record the number of messages delivered in less than 2s, record the number of messages which took longer than that to be delivered. Calculate the percentage of the "lazy" ones and make sure they are less than 5%. [on field] Verify that no messages are delivered in more than 40 s.
Expected result:	Sending a message from the Di.Co.A. emulator to the ESMIG takes no longer than 2s and only 5% of the overall number of messages take longer and no messages are delivered after 40s.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

DEP A2A store-and-forward message delivery time

Requirement ID	ESMIG.30300

The NSP delivers a store-and-forward message from the Sender to the Receiver in less than 10s for the 95% of the messages and 100% in less than 60s (and referred to the incoming traffic only, i.e. from the Di.Co.A. to the ESMIG Platform). The acknowledgment of the delivery sent back to the sender is not included in the delivery time.

Detailed test procedure:	Send store–and-forward messages from the Di.Co.A. emulator to the Platform at a constant rate – close to the 90% of the overall maximum allowed rate (measured in messages/sec) – for at least 16 hours and record the delivery time for each of the messages. Record the overall number of messages, record the number of messages delivered in less than 10s, record the number of messages which took longer than that to be delivered. Calculate the percentage of the "lazy" ones and make sure they are less than 5%.. Verify that no messages are delivered in more than 60s. [on field]
Expected result:	Sending a message from the Di.Co.A. emulator to the ESMIG takes no longer than 10s and only 5% of the overall number of messages take longer and no messages are delivered after 60s.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

MEPT A2A instant message delivery time

Requirement ID	ESMIG.30310

The NSP delivers an instant message from the Sender to the Receiver in less than 250ms for the 95% of the messages and 100% in less than 1s. The acknowledgment of the delivery sent back to the sender is not included in the delivery time.

Detailed test procedure:	Send instant messages from the Di.Co.A. emulator to the Platform at a constant rate – close to the 90% of the overall maximum allowed rate (measured in messages/sec) – for at least 16 hours and record the delivery time for each of the messages. Record the overall number of messages, record the number of messages delivered in less than 250ms, record the number of messages which took longer than that to deliver. Calculate the percentage of the "lazy" ones and make sure they are less than 5%. Verify that no messages are delivered in more than 1s. [on field].
Expected result:	Sending a message from the Di.Co.A. emulator to the ESMIG takes no longer than 250 ms and only 5% of the overall number of messages take longer and no messages are delivered after 1s.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____

	NSP testing team_____date____/____/____

Connection availability

Requirement ID	ESMIG.30320

The Connection Availability measures the availability of the connection of the Di.Co.A. to the ESMIG independently of the type of messaging services used.
The Connection Availability is the percentage of time that the connection for the Di.Co.A. is considered to be operational. It is calculated using the following formula.

$$Connection\ availability = 100 - \frac{TotalOutageTime}{TotaleServiceTime} \cdot 100$$

Where:

1. TotalOutageTime is the sum of the product of each OutageTime (in minutes in the reporting period) and the number of affected DiCoAs; if the outage impacts the connection with the ESMIG, all the Di.Co.A. are considered to be affected by the outage;
2. Total Service Time is the product of the total number of the Di.Co.A. and the Service time in minutes in the reporting period as defined above.

The connection availability shall not be less than 99,999 calculated on a monthly basis.

Detailed test procedure:	Inspect the documentation provided by the NSP [desk check], then collect at least one month of Connection Availability data and calculate the Availability.
Expected result:	The NSP describes how Connection Availability is measured and this availability is in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A Service availability

Requirement ID	ESMIG.30330

The A2A Service Availability is the percentage of the time that the A2A services are available to the Di.Co.A.s to send and receive messages (with no impact on performances). It is calculated with the following formula:

$$ServiceAvalability = \left(\frac{ServiceTime - OutageTime}{ServiceTime} \right) \cdot 100$$

Where:

- Outage time is the sum of the outage time of each NSP connected Di.Co.A. (in minutes) in the reporting period;
- Service Time is the sum of the expected availability time of each NSP connected Di.Co.A. (in minutes) in the reporting period.

The Service Availability is not less than 99,98% calculated on a monthly basis. The NSP describes in detail how the above measurements of the outage times are calculated.

Detailed test procedure:	Inspect the documentation provided by the NSP [desk check], then collect at least one month of A2A Service Availability data and calculate the A2A Service Availability. [desk check]
Expected result:	The NSP describes how Service Availability is measured and this availability is in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

U2A Service availability

Requirement ID	ESMIG.30340

The U2A Service Availability is the percentage of the time that the U2A services are available to the Di.Co.A.s to access the ESMIG Platform web resources. It is calculated with the following formula:

$$ServiceAvalability = \left(\frac{ServiceTime - OutageTime}{ServiceTime} \right) \cdot 100$$

Where:

- Outage time is the sum of the outage time of each NSP connected Di.Co.A. (in minutes) in the reporting period;
- Service Time is the sum of the expected availability time of each NSP connected Di.Co.A. (in minutes) in the reporting period.

The U2A Service Availability must be not less than 99,98%, calculated on a monthly basis. The NSP describes in detail how the above measurements of the outage times are calculated.

Detailed test procedure:	Inspect the documentation provided by the NSP [desk check], then collect at least one month of U2A Service Availability data and calculate the U2A Service Availability. [desk check]
Expected result:	The NSP describes how Service Availability is measured and this availability is in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Fault classification

Requirement ID	ESMIG.30350

The NSP must classify faults at least according to the following classes:

HIGH - Fault causes outage time affecting Service Availability or a system component is unable to perform critical tasks. Examples:

- ESMIG is unable to access the service using anyone of the available accesses
- A single ESMIG site is unable to access the service
- WAN service parameters are strongly degraded.

MEDIUM - Fault results in serious disruptions, limitations or restrictions in the operating infrastructure. Examples:

- ESMIG WAN component is faulty or a link has failed.
- ESMIG access is degraded (intermittent or slow)
- A2A or U2A service parameters are partially degraded.

LOW - Fault results in moderate/limited impact in the operating infrastructure. The ESMIG is able to exchange traffic, problems occur on redundant devices or supporting functions (monitoring access, management interfaces, ticketing system…). Examples:

- Fault has only slight impact on operations
- Request for information submitted by ESMIG Operator.

Detailed test procedure:	The fault classification described in the NSP Operational Manual envisages at least three classes: High, Medium, Low. [desk check]
Expected result:	The description of the fault classes is in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Fault metrics

Requirement ID	ESMIG.30360

The NSP must measure the fault clearance process according to three metrics, as defined as follows:

- Status Notification Interval (SNI): The ESMIG Operator is informed about fault status and the fault clearance progress at recurring intervals;
- Maximum Time To Intervene (MxTTI): maximum time elapsing between the acceptance of a trouble ticket and the start of the fault clearing process;
- Maximum Time To Repair (MxTTR): maximum time between the acceptance of a trouble ticket and the end of the fault clearing process. (MxTTR is temporarily suspended by the following events: 1. ESMIG is not available to support or provision access to the faulty components, or 2. ESMIG refuses to allow contractor personnel to enter the site, or force majeure (a circumstance due to an external, unpredictable event unrelated to computer operations and when that circumstance could not have been either foreseen or prevented with all due reasonable care).

Detailed test procedure:	The fault metrics described in the NSP Operational Manual envisages at least three metrics: SNI, MxTTI, MxTTR. [desk check]
Expected result:	The description of the fault metrics is in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Fault clearance

Requirement ID	ESMIG.30370

The NSP must guarantee a fault clearance of the incidents affecting services provided by the NSP to the ESMIG within the times defined in the following table, depending on the criticality of the identified fault. In order to establish its priority, the criticality of each fault episode may be classified as high, medium or low (or equivalent Priority levels, mapped on the NSP trouble ticketing system).

The definition of the related levels is the following:

	Service level (SL)		
	High	medium	low
MxTTI [hours]	0.5	4	8
MxTTR [hours]	4	8	16
SNI [hours]	1	2	4

Detailed test procedure:	The NSP's Operational Manual reports the agreed service levels for MxTTI, MxTTR and SNI. [desk check]
Expected result:	The NSP contractual framework includes the agreed service levels.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

4. NETWORK

WAN links – connected sites

Requirement ID	ESMIG.40010

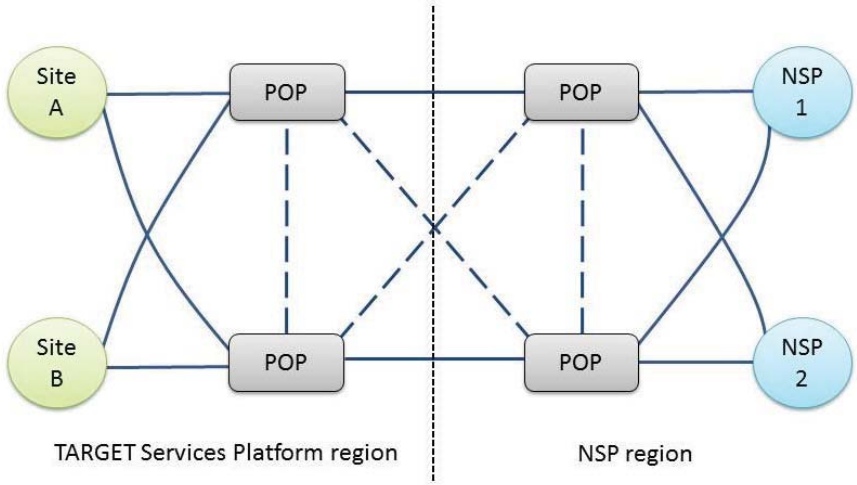
Each ESMIG site must be connected – using WAN links – to at least two NSP sites. [A WAN link is defined as the local loop from ESMIG site to the local metro area PoP + backbone $_{Carrier}$ + metro area from the metro area PoP to the local NSP site].

The NSP can serve the ESMIG sites using one or more carriers.

The NSP can reuse existing WAN links.

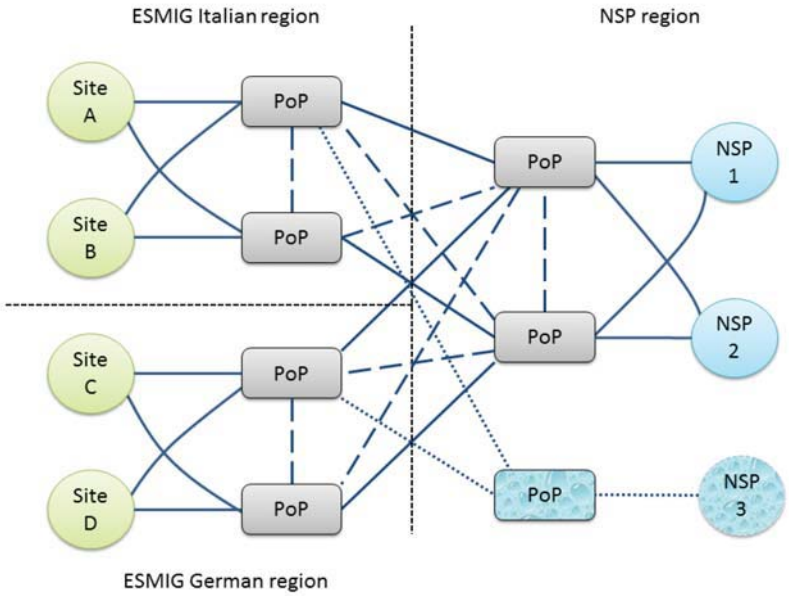
The NSP can be a carrier.

The network topology might for example look like this:



Sites C and D follow the same pattern.

Including the NSP cold site it would then look like the following:


ESMIG Italian region
NSP region
Site A
Site B
Site C
Site D
PoP
PoP
PoP
PoP
PoP
PoP
NSP 1
NSP 2
NSP 3
ESMIG German region

Detailed test procedure:	The NSP details the WAN connectivity: in the ESMIG region (addresses of the metro area PoPs, paths from the ESMIG sites to the local metro area PoPs, ...), in the NSP region (addresses of the metro area PoPs, paths from the NSP Sites to the metro area PoPs, ...) and backbone connectivity from the PoPs in the ESMIG region to the PoPs in NSP region. The NSP describes how the cold site is connected. The NSP describes if the ESMIG sites are served by one or more carriers (information purposes only). The NSP should declare if WAN links reuse any pre-existing infrastructure and if yes which one. [desk check]
Expected result:	Sites are connected using WAN links in line with the requirement description.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WAN links – local loop and metro specifications

Requirement ID	ESMIG.40020

Local loops are the links from each NSP's carrier POPs (Point of Presence) to the ESMIG site. The NSP must have at least two POPs in the metro area (where the ESMIG data centres are located). Each ESMIG sites must have at least two local loops, one connected to the first NSP's POP and another one connected to the second NSP's POP (providing both redundancy and path diversification in the metro area).

Detailed test procedure:	The NSP describes the connectivity from the ESMIG sites to the NSP's PoP in the same metro area and highlights how redundancy and path diversification is achieved in the metro area. The NSP also describes the connectivity from the NSP Sites to his own PoPs in the same metro area and highlights how redundancy and path diversification is achieved in the metro area. [desk check]
Expected result:	Local loop in the metro area are in line with the requirement description.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WAN links – backbone specifications

Requirement ID	ESMIG.40030

The backbone links between the PoPs in the ESMIG data centre metro area and PoPs in the NSP's data centre metro area must provide both redundancy and paths diversification.

Detailed test procedure:	The NSP describes the connectivity through the backbone (i.e. from the PoPs in the ESMIG metro area to the PoPs in the NSP's metro area) and highlights how redundancy and path diversification is achieved in the backbone itself. [desk check]
Expected result:	Backbone is in line with the requirement description.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

LAN interface specifications (physical demarcation)

Requirement ID	ESMIG.40040

The NSP must connect to ESMIG sites either using 1 Gigabit Ethernet ports or 10 Gigabit Ethernet ports. Ethernet local link port interface speed and specifications can be proposed by the NSP, but the ESMIG reserves the right to mandate to the NSP the adoption of a specific LAN interface standard.

The NSP is allowed to connect to the ESMIG using up to two Ethernet interfaces per site per footprint. The NSP is allowed to have a more than a single footprint (i.e. a footprint for T2, another one for T2S and one for TIPS, etc.), each footprint can then have up to two Ethernet interfaces.

Detailed test procedure:	Visually inspect the NSP's physical demarcation in the ESMIG sites and verify if it has either a 1 GbE or 10 GbE. The interface media type has been bilaterally agreed between the ESMIG and the NSP. [on field]
Expected result:	LAN interface specifications are in line with the requirement description.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Internet Protocol (IP) type (IPv4 and IPv6) and IP addressing schema

Requirement ID	ESMIG.40050

The NSP must deliver the connectivity to the ESMIG sites either using Internet Protocol (IP) version 4 (IPv4) or Version 6 (IPv6); no other layer three protocols are allowed between the ESMIG and the Di.Co.A..

The NSP must use an IP addressing schema agreed with the ESMIG; this IP addressing schema can either be a private address allocation in terms of RFC1918 or a public IP address range registered by the NSP.

Once the boundary subnets – between the NSP and the ESMIG – have been agreed, the NSP agrees with the ESMIG on how to split the IP addresses within the subnet and how to map them to the specific services.

Detailed test procedure:	Jointly inspect the documentation describing the Network, including network diagrams and verify either IPv4 addresses or IPv6 addresses are transported on the service boundaries. [desk check]
Expected result:	IPv4 and IPv6 are the two only allowed protocols on the boundary between the NSP and the ESMIG Platform. The IP addressing schema are in line with the requirement description.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Static Routing

Requirement ID	ESMIG.40060

The NSP must use only static routes in the boundary between the NSP itself and the ESMIG; ie. no dynamic routing protocols are allowed.

Detailed test procedure:	Check network equipment configuration and verify there is no dynamic routing protocol between the NSP and the ESMIG. [on field]
Expected result:	Only static routing has been implemented between the NSP itself and the ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5. SECURITY

5.1 Information security policies

ISO 27001:2013 certification

Requirement ID	ESMIG.50010

The NSP must have an ISO 27001:2013 (Information technology — Security techniques — Code of practice for information security controls) certification.

Detailed test procedure:	Verify the NSP's conformity to the ISO27001:2013 standard. [deck check]
Expected result:	NSP is compliant with the ISO27001:2013 standard and is able to formally demonstrate this compliancy.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

PCSG - Requirements and Controls

Requirement ID	ESMIG.50020

The NSP must have in place a guidance document - aimed to the Di.Co.A.s - describing its security services regarding connectivity Participants Connectivity Security Guidance (PCSG), where the "Participants" are the Di.Co.A.s. The PCSG shall define requirements and controls towards the NSP's Di.Co.A.s that ideally aim to cover the following areas:

- Protection and segregation of the Di.Co.A's infrastructure used to connect to the NSP, (hereafter the "NSP connected local infrastructure") from the enterprise IT environment.
- Network security of the traffic flow to and within the NSP connected local infrastructure.
- Security testing of the NSP connected local infrastructure testing also access from the enterprise network.
- Vulnerability and Patch Management of the NSP connected local infrastructure.
- Physical Security of the NSP connected local infrastructure.
- HR screening such as background and credit checks as well as other industry standard anti-fraud measures for users of the NSP connected local infrastructure.
- Plans, procedures and responsibilities for Incident Response with demonstrated readiness.
- Information sharing for security incidents and near misses with industry members and ecosystem participants.
- Credential security of the NSP connected local infrastructure taking into account multifactor authentication where needed and protection of privileged identities as well as proper user management, account and password practices.
- System and applications security including adoption of antimalware and endpoint security, hardening of systems and applications, control of software and use of software integrity mechanisms.
- Detection of security incidents and fraudulent transactions from the NSP connected local infrastructure (system, application, middleware, other).
- Security training and awareness for all users with access to the NSP connected local infrastructure.
- Perform risk assessments for the NSP connected local infrastructure taking into account any relevant 3rd parties.

Detailed test procedure:	The NSP has a PCSG aimed to the Di.Co.A.s that covers all the areas described in the requirement. [deck check]
Expected result:	NSP has provided a PCSG and is able to formally demonstrate this to the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

PCSG - NSP's management commitment to guide and evolve the PCSG

Requirement ID	ESMIG.50030

The Board of the NSP must strongly commit to keep the Di.Co.A.s' connectivity security guidance (PCSG) fit-for-purpose in order to assist its Di.Co.A.s to secure the IT environment through which it connects to the NSP infrastructure and network.

The NSP must commit to ensure that the PCSG evolves with the threat landscape and shall - at least annually - review the PCSG and assess whether further requirements and controls shall be included in the PCSG to help ensuring the security of its network infrastructure, the infrastructure of its Di.Co.A.s as well as the infrastructure of the entire ecosystem.

The Eurosystem may in the future require an alignment of PCSGs if significant divergences are identified.

Detailed test procedure:	It is possible to prove the NSP's board commitment to the implementation and annual review of the PCSG. [deck check]
Expected result:	NSP's Board is committed to guide the evolution of the PCSG and is able to formally demonstrate this to the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

PCSG - compliance checking process and self-attestation

Requirement ID	ESMIG.50040

The NSP must have a process in place which requires its Di.Co.A.s to regularly self-certify or attest, at least annually, that they are in line with the PCSG. The Di.Co.A.s shall be required to present action plans to ensure, within 12 months after self-certification or attestation that it complies with those elements of the guidance against which it has reported as being not compliant.

The NSP should ideally have measures in place, possibly within the contractual relation with its Di.Co.A.s, to ensure that Di.Co.A.s comply with the PCSG such as for example:

- The transfer of liability for potential security breaches that may be attributed to the non-compliance to one or several controls in the PCSG;
- The possibility to disconnect a Di.Co.A.s from the network in case of systematic non-compliance with the PCSG.

The NSP shall also commit to provide aggregated results of the compliance checks to the ESMIG service providing central banks which may share these results with the community of central banks participating in the ESMIG.

Detailed test procedure:	It is possible to prove the compliance checking process and annual self-attestation. [deck check]
Expected result:	NSP's has a compliance checking process including a yearly self-attestation exercise and is able to formally demonstrate this to the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.2 Organization of information security

Security Cooperation

Requirement ID	ESMIG.50050

The NSP must cooperate with the ESMIG Operator Computer Emergency Response Team (CERT) in order to share Cyber Threat Intelligence (CTI) and IOC (Indicator of Compromise) and security relevant information (alerts, bulletins,…).

Detailed test procedure:	Verify that the NSP CERT and ESMIG Operator CERT have identified their respective contact points, are willing to cooperate and communication channels have been agreed. [desk check]
Expected result:	Cooperation between NSP CERT and ESMIG Operator CERT has been established.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.3 Access control

Logically segregated groups of users and Closed Group of Users (CGU)

Requirement ID	ESMIG.50060

The NSP must allow creation, management and removal of logically segregated groups of Di.Co.A.s through Closed Group of Users (CGU). The NSP must have different CGUs for the production environment and for the test environments, for each ESMIG application.

The subscription to a group of users, and any subsequent modification to such subscription, must be arranged through an electronic workflow on the Internet. All the electronic forms must be authorised by the relevant National Central Bank and/or CSD. The activation date for the subscriptions must be set at latest within two weeks following the form's approval by the ESMIG Operator; the new subscription must be scheduled and activated ensuring the availability of the service (e.g. adopting the "rolling update" approach). Upon request from the ESMIG Operator, the NSP must withdraw from the CGU a Di.Co.A. within one hour.

Detailed test procedure:	Subscribe some Di.Co.A.s (using the Di.Co.A. emulator) to a test CGU already created by the NSP. Check any new Di.Co.A. is able to operate. Request to remove a Di.Co.A. assigned to the CGU. Check the removed Di.Co.A. is not able to operate anymore. While performing these actions verify the Internet electronic workflow for Di.Co.A. creation/deletion. [on field]
Expected result:	The NSP allows the creation and removal of logically segregated groups of users, manages all the user groups, and is able to segregate production environment from each test environment. The NSP shall demonstrate that the process to remove a user within an hour has been documented. User and group creation are in line with the process described in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

ESMIG's access control

Requirement ID	ESMIG.50070

The NSP must ensure that only authenticated parties are able to access the ESMIG.

Detailed test procedure:	Verify that the A2A and U2A traffic between the NSP and the ESMIG is allowed only to authenticated parties. [on field]
Expected result:	Only authenticated parties are able to access the ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Unique identification of users (A2A and U2A)

Requirement ID	ESMIG.50080

The NSP must identify the Di.Co.A. and the ESMIG in a unique way (every time a new session is being set up). The NSP must guarantee the identification of A2A users and U2A users via digital certificates.

Detailed test procedure:	Verify that the NSP uniquely identifies Di.Co.A. (use the Di.Co.A. emulator) via digital certificates, then verify that the NSP uniquely identifies ESMIG via digital certificates. [on field]
Expected result:	NSP uniquely identifies both the Di.Co.A. and the ESMIG using digital certificates.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Authentication in A2A

Requirement ID	ESMIG.50090

The NSP must authenticate the Di.Co.A. and the ESMIG (every time they open a new session). The NSP must base this authentication mechanism on the availability of digital keys stored in a Hardware Security Module (HSM) accessible by the NSP's Network Gateways.

Detailed test procedure:	The possibility to open a new session on the NSP's Network Gateway mandates the presence of a valid digital certificate. Part I: A new session is opened from a Di.Co.A. (using the Di.Co.A. emulator) with no certificate or invalid certificate (i.e. suspended certificate or expired certificate), then verify the NSP's Network Gateway rejects the session. Part II: A new session is opened from a Di.Co.A. (using the Di.Co.A. emulator) with a valid certificate, then verify the NSP's Network Gateway accepts the session. [on field]
Expected result:	Every time a new session is opened the NSP authorizes both the Di.Co.A. and the ESMIG (through the A2A NSP's Network Gateway) using digital keys stored in a HSM. NSP successfully completes the message partners authentication, digital certificates are checked, same keys are used for authentication and digital signatures.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Authentication in U2A mode – Smartcard/USB token

Requirement ID	ESMIG.50100

The NSP must provide either Smart Cards or USB tokens for storing all digital keys used for U2A. These devices must be compliant with FIPS 140-2 Level 3 or Common Criteria EAL4+.

Smart Card readers or USB tokens must comply at least with the following specifications:

- USB interface with A-type connector;
- power supply through the same USB interface;
- ISO 7816 Class A, B and C (5V, 3V and 1,8V) smart card support;
- short circuit protection;
- compatible with ISO 7816-1,2,3,4 specifications. T=0 and T=1 protocols;
- PC/SC for Microsoft driver;
- Microsoft Windows Hardware Quality Labs (WHQL) compliance;
- Operating Systems: Windows, Linux and Mac OS X.

Detailed test procedure:	The specifications of the smart card readers are verified and checked. Check if smart card/USB token are compliant either with FIPS 140 - L3 or Common Criteria EAL4+ and complies with the specifications described above. [desk check]
Expected result:	The smart card /USB token provided by the NSP comply with FIPS 140 - L3 or Common Criteria EAL4+.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Authentication in U2A mode – Remote HSM

Requirement ID	ESMIG.50110

The NSP must provide an authentication mechanism based on remote HSM for storing all digital keys used for U2A. These devices must be compliant with FIPS 140-2 Level 3. The Di.Co.A. can either use the "Authentication in U2A mode – Smartcard/USB token" (ESMIG.50100) or this "Authentication in U2A mode – Remote HSM" (ESMIG.50110). This authentication is two factor based (because of the user's knowledge of the PIN). The NSP must check validity of the digital certificate

Detailed test procedure:	The NSP demonstrate that the remote HSM solution is FIPS 140-2 L3 compliant. [desk check] The NSP has generated the client certificates for the Di.Co.A.s. Access to the ESMIG in U2A mode using the remote HSM as a part of 2FA mechanism. [on field]
Expected result:	The NSP's remote HSM solution is FIPS 140-2 L3 compliant. The authentication to the ESMIG is successful using the remote HSM.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.4 Cryptography

Public Key Infrastructure and Certificate Extensions

Requirement ID	ESMIG.50120

The NSP must deliver a Public Key be Infrastructure ("PKI") that shall comply with X.509 version 3 standard for the digital certificates. The NSP's PKI must produce certificates for both A2A and U2A.

A2A certificates used for digital signature must have the Non-Repudiation bit set in the "Key usage" extension.

U2A certificates used for digital signature and authentication must have the Non-Repudiation and the "DigitalSignature" bit set in the "Key usage" extension. Two separate certificates for digital signature and authentication can be used, in this case only the certificate not used for NRO must have the "DigitalSignature" flag set.

Detailed test procedure:	Check that the NSP has in place a Certification Authority. Check certificates signed by the NSP's Public Key Infrastructure (PKI) are compliant to version X.509 ver.3. Examine certificates to check which extensions NSP uses. Verify NSP all requested extensions are actually used. [on field]
Expected result:	NSP's PKI Infrastructure provides a Certification Authority. Certificate extensions in use are documented.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Decentralised management of users

Requirement ID	ESMIG.50130

The NSP must allow local security administrators of its Di.Co.A. and the ESMIG to manage the end users' identity and credentials required to access the ESMIG (such as end user provisioning, service provisioning).

Detailed test procedure:	The local security administrator creates a new user and assigns credentials, ESMIG' security administrator approves access privilege granting access to the ESMIG. [on field]
Expected result:	Local security administrators manage users' identity and credentials required to access ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Cypher suite and usage of up-to-date algorithms (hashing and encryption)

Requirement ID	ESMIG.50140

The NSP must use only strong and not deprecated encryption algorithms and digest (hash) algorithms:

- AES-256 is the minimum required algorithm for encryption (with a minimum length of 256 bit for symmetric encryption keys and 2048 bit for asymmetric encryption keys).
- SHA-256 is the minimum required algorithm for digest computation.

The usage of alternative algorithms can be bilaterally agreed between the NSP and the Platform.

Detailed test procedure:	List which algorithms are used and where. [desk check]
Expected result:	The NSP uses only strong and not deprecated algorithms.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Administration of cryptographic keys

Requirement ID	ESMIG.50150

The NSP must ensure the following administration functions for symmetric and asymmetric (private only) cryptographic keys.

- *Generation*: The NSP must ensure secure generation of keys.
- *Distribution*: The NSP must ensure secure (i.e. encrypted) electronic distribution of the keys.
- *Renewal*: The NSP must ensure the renewal of the keys and must ensure that keys renewal does not interfere with its own services.
- *Storage*: The NSP must ensure that keys are stored securely (e.g. on the HSM).
- *Revocation*: The NSP must ensure immediate revocation of the key/certificate when compromised.

Detailed test procedure:	Verify together with the NSP the procedure used to generate, distribute, renew, store and revoke symmetric/asymmetric cryptographic keys. [desk check] Generate and distribute the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Renew the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Store the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Revoke the asymmetric crypto keys, then try to use it and verify it fails. [on field]
Expected result:	The NSP ensures the foreseen administration functions (generation, distribution, renewal, storage and revocation of the keys).
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

NSP's Network Gateways Certificate independence

Requirement ID	ESMIG.50160

The certificates issued by the PKI must be used without any constraint to the physical location of the NSP's Network Gateways active site. The certificates used by the Di.Co.A. must be valid on all ESMIG sites, i.e. during a ESMIG site recovery (or in case of loss of a ESMIG site) the sessions from the Di.Co.A. to the Platform remain valid on the surviving site. Vice versa the certificates used by the ESMIG must be valid on all Di.Co.A. sites, i.e. during a Di.Co.A. site recovery (or in case of loss of a Di.Co.A. site) the sessions from the ESMIG to the Di.Co.A. remain valid on the surviving site.

Detailed test procedure:	Use Di.Co.A. emulator for this test. Part I: Isolate site B (disabling the Ethernet interfaces on the 4CBNet switch), have the Di.Co.A. to send successfully messages to the Network Gateways in site A. Restore site B and isolate site A, have the Di.Co.A. to send successfully messages to the Network Gateways in site B. No changes of certificate on the Di.Co.A. are expected. Part II: Isolate Di.Co.A. site 2 (disabling the Ethernet interfaces on the 4CBNet switch), have the ESMIG to send successfully messages to the Network Gateways in site 1. Restore site 2 and isolate site 1, have the ESMIG to send successfully messages to the Network Gateways in site 2. No changes of certificate on the ESMIG are expected. [on field]
Expected result:	Independently of where the ESMIG is running (either site A or site B), the Di.Co.A. can successfully connect to the ESMIG; i.e. all certificates are signed by the same CA.

Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Certificate Revocation List (CRL)

Requirement ID	ESMIG.50170

The NSP must provide to the ESMIG Operator the CRL in the HTTP or LDAP or OCSP formats. The ESMIG will select with the NSP the most appropriate protocol for the intended scope.

Detailed test procedure:	Query the NSP's CRL using at least one of the supported protocols (HTTP, LDAP, OCSP). [on field]
Expected result:	It is possible to read the CRL using at least one of the following protocols: HTTP, LDAP and OCSP.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Certification Authority, Certificate Policy (CP) and Certificate Practices Statement (CPS)

Requirement ID	ESMIG.50180

The NSP must deliver Certification Authority (CA) functions to the Di.Co.A. and to the ESMIG. The functions provided by the CA must support the generation, management, storage, deployment, revocation and signature of public key certificates. The NSP's CA functions are described in the Certificate Policy (CP) and operated in accordance with the Certificate Practices Statement (CPS). The contents of the CP and CPS are described in RFC 3647 "Internet X.509 Public Key Infrastructure, Policy and Certification Practices Framework". The NSP must deliver to the ESMIG Operator both deliverables (CP and CPS).

Detailed test procedure:	1. A Di.Co.A. generates a certificate using the NSP's CA. The Di.Co.A. is able to manage the certificate life cycle (store, deploy and eventually revoke certificates). ESMIG Operator performs the same tests. In case no Di.Co.A. is available during the testing phase, then please run the test only with the ESMIG Operator and using the Di.Co.A. emulator. [on field] 2. Compare the life cycle with CP and CPS. [desk check] 3. Jointly analyse the NSP's CP and CPS, in the analysis give a focus on NSP responsibilities and certificates usage, enrolment, issuance, revocation, and liability, then make sure all NSP's CA functions are covered within operational procedures. [desk check] 4. List the CA functions the NSP performs. Jointly inspect the CPS. Make sure all listed functions are covered within operational procedures. [desk check]
Expected result:	The NSP delivers Certification Authority (CA) functions to Di.Co.A. and the ESMIG, i.e. generation, management, storage, deployment, and revocation of public key

	certificates. The NSP delivers the CP and CPS to ESMIG. The CA functions are compliant with the CP and operate in accordance with the CPS. The NSP provides CA functions to ESMIG Operator and Di.Co.A., and ensures the above mentioned functions within the CP and CPS context.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

MEPT Hardware Security Modules

Requirement ID	ESMIG.50190

The NSP must provide tamper-proof HSM for storing all digital keys used for A2A. The HSM(s) must be compliant at minimum with FIPS 140-2 Level 3 or Common Criteria EAL 4+. The NSP's Network Gateway must be equipped with tamper-proof HSM(s).

Detailed test procedure:	1. Check if the HSM(s) are installed in the ESMIG sites; [on field] 2. Check if the HSM(s) are FIPS 140-2 L3 compliant or Common Criteria EAL 4+; [desk check] 3. Check if all A2A keys used (both on the ESMIG and the Di.Co.A.) are stored in the HSM(s); the HSM contains a key pair for every certificate, during the test list the available certificates. [on field]
Expected result:	The NSP have installed FIPS 140-2 Level 3 or Common Criteria EAL 4+ compliant HSM in the ESMIG sites. HSM(s) contain(s) the digital keys used for A2A.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

MEPT Responsibilities for management of cryptographic keys

Requirement ID	ESMIG.50200

The management of cryptographic keys (assigned to ESMIG) must remain under the sole responsibility of the ESMIG Operator, which must be the only Institution having key management duties to its key storage devices delivered by the NSP.

Detailed test procedure:	Verify that the ESMIG Operator is able to manage crypto keys in the HSM; then verify whether the NSP is able to logically access the HSM (for example in order to perform a SW upgrade of the device), but is not authorized to manage the key material in the HSM itself. Logical access is permitted to the NSP only for administrative and operational purposes. [on field]
Expected result:	The management of cryptographic keys is under the sole responsibility of the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.5 Operations security

Protection from malware

Requirement ID	ESMIG.50210

The NSP must implement detection, prevention and recovery controls to protect against malware. Anti-malware software must be deployed on NSP's Network Gateways and be updated daily. Anti-malware scans are conducted on the NSP's Network Gateways Operating System and on the files transmitted through the infrastructure.

Detailed test procedure:	List the anti-malware software installed on the NSP Network Gateway. Verify the software is updated daily. Check anti-malware scans are conducted on the Operating System and on the transmitted files. Identify what actions are triggered when a malware is detected.
Expected result:	Anti-malware software is in place accordingly to the requirement. The NSP detects malware and promptly alerts the ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

ESMIG Operator

Event logging

Requirement ID	ESMIG.50220

The NSP must enable logging functionality on all its components (both NSP's Network Gateway and network devices). Event logs record user activities (i.e. audit logs), exceptions, faults and information security events. Event logs should include the fields listed in ISO/IEC 27002:2013 § 12.4.1.

Detailed test procedure:	Part I Check that all network devices are logging all events described in the ISO control. Part II Identify which logging servers are configured and verify they are actually receiving the expected logs. [on field]
Expected result:	All provided NSP's components have a logging functionality enabled in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Protection of log information (anti-tampering)

Requirement ID	ESMIG.50230

The NSP must ensure and control the integrity of all ESMIG related logs. All logs produced by the NSP devices must be maintained on a Security Information and Event Management (SIEM). The SIEM must have anti-tampering measures (ISO/IEC 27002:2013 § 12.4.2 “Protection of log information”), i.e. it must ensure that logs cannot be manipulated. Logs are transmitted from the device to the SIEM using an encrypted channel.

Detailed test procedure:	List all NSP devices, list all audit logs produced, prove the compliancy with the ISO 27002:2013 control 12.4.2 “Protection of log information” and give evidence of the anti-tampering measures in place. Verify integrity can be ensured for all audit logs. [on field]
Expected result:	The NSP ensures and controls the integrity of NSP related equipment audit logs; audit logs integrity is ensured and the NSP is able to determine when integrity is compromised.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Control of operational software and software integrity

Requirement ID	ESMIG.50240

The NSP must ensure the integrity of software installed both on NSP's Network Gateway and network devices. Software integrity checks provide a detective control against unexpected modification to operational software. Software integrity checks on NSP Network Gateway are conducted upon start-up and additionally at least once per day; while network devices only on start-up. Integrity check of downloaded software is conducted via verification of the checksum at the time of its deployment. Software integrity should cover middleware (e.g. MQ) configuration files. The NSP must automatically detect every modification to its own software and immediately alert the ESMIG Operator.

Detailed test procedure:	List the software installed on the NSP Network Gateway and network devices. Verify how the operational software is protected to detect unexpected modification. Identify what actions are triggered when a validation fails. [on field]
Expected result:	Control of software integrity is in place accordingly to the requirement. The NSP detects validation failures and promptly alerts the ESMIG Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Time synchronisation

Requirement ID	ESMIG.50250

The NSP must synchronise the date and time of all its Network Gateway and Network devices either with the same date and time source adopted by the ESMIG or by using a Stratum 2 (or 3) time source, approved by the ESMIG Operator. The Network Time Protocol (NTP) synchronisation interval is at least every one minute. In terms of time zone and time format, the official time of the ESMIG is the ECB time (i.e. the local time at the seat of the ECB); the NSP must provide time information using Coordinated Universal Time (UTC) format.

Detailed test procedure:	Considering the reference terminology described in Request for Comments 5905 "Network Time Protocol Version 4: Protocol and Algorithms Specification" verify that all the NSP devices adopt a NTP synchronized with a single time source. Check the compliance of the time source with the ones approved by the ESMIG Operator. Check the synchronisation interval, the time format and the Stratum level. [on field]
Expected result:	NSP's devices date and time are NTP synchronised with a time source in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Technical vulnerability management of NSP's Network Gateway and network devices

Requirement ID	ESMIG.50260

The NSP must have a process of Vulnerability Patch Management (VPM) where responsibilities are clearly defined; this process must include monitoring, prioritization, remediation and reporting. The NSP must ensure quick updates of all its NSP's Network Gateway and network devices; security patches must be installed according to the following table:

CVSS Score	**Vulnerability Rating**	**Rollout schedule**	
		Target	**Maximum**
0 – 2	Negligible	With the next release of the service / component.	Within 1 year
2.1 – 4.5	Low		
4.6 – 7.0	Medium		
7.1 – 10	High	48 hours (for configuration related vulnerabilities)	Within 1 month.
		2 weeks (after release of the patch)	Within 3 months (after release of the patch)

Table 1: CVSS scoring and prioritization scheme

Detailed test procedure:	Part I Verify the NSP has a VPM procedure taking into account the Vulnerability Rating. [desk check] Part II List the versions of all SW installed on the NSP's Network Gateway and network devices, verify the CVSS Scoring associated to the vulnerabilities present in the installed SW (if any), focus on scoring higher or equal than 7.1, and demonstrate the Rollout schedule has been respected. [on field]
Expected result:	The VPM is in line with the requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.6 Communications security

A2A Segregation of data

Requirement ID	ESMIG.50270

The NSP must ensure each Di.Co.A. is able to access only its own data (incoming and outgoing A2A traffic).

Detailed test procedure:	1. a Di.Co.A. (use the Di.Co.A. emulator) can access in A2A his own relevant data; 2. a Di.Co.A. (use the Di.Co.A. emulator) cannot access in A2A data relevant to other Di.Co.A.s; [on field]
Expected result:	The NSP ensures Di.Co.A. can access only their own A2A incoming and outgoing traffic.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

U2A Segregation of data

Requirement ID	ESMIG.50280

The NSP must ensure that each Di.Co.A. must be able to access only its own data (incoming and outgoing U2A traffic).

Detailed test procedure:	1. a Di.Co.A. can access in U2A his own relevant data; 2. a Di.Co.A. cannot access in U2A data relevant to other Di.Co.A.s. [on field]
Expected result:	The NSP ensures Di.Co.A. can access only their own U2A incoming and outgoing traffic.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A Integrity of traffic

Requirement ID	ESMIG.50290

The NSP must ensure the integrity of all A2A traffic exchanged between its Di.Co.A. and the ESMIG. Integrity of A2A traffic is ensured using a Local Authentication (LAU) mechanism. The NSP must perform an integrity check of each message forwarded through its network, i.e. an hash must be calculated and verified at both the sending and receiving side.

Detailed test procedure:	Verify that the NSP performs an integrity check on each message entering/leaving its network; an hash must be calculated at both the sending and receiving side. [desk check]
Expected result:	The NSP ensures the integrity of all traffic from the Di.Co.A. to the ESMIG and back.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Segregation of traffic

Requirement ID	ESMIG.50300

The NSP must ensure segregation of data traffic between different CGU. Di.Co.A.s belonging to different CGUs cannot exchange data with each other. Di.Co.A.s belonging to test CGU shall not be able to send or receive messages from the production environment and vice versa.

Detailed test procedure:	Send a message to a user belonging to a different CGU. Repeat test for a file. Both attempts are expected to fail. Using a test user account, send messages to the production environment. Repeat test for a file. Both attempts are expected to fail. Using a production user account, send messages to the test environment. Repeat test for a file. Both attempts are expected to fail. [on field]
Expected result:	The NSP ensures segregation of data traffic between different groups of users and segregation of environments (production vs. test) within the same user.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Confidentiality and integrity of data in transit across the public soil

Requirement ID	ESMIG.50310

The NSP must take appropriate measures to protect all data in transit between ESMIG sites and the NSP's sites and between the NSP sites and the Di.Co.A.'s sites. An example of an "appropriate measure" is an IPSec VPN tunnel. All traffic must be encrypted and authenticated.

Detailed test procedure:	Part I: Verify that all data leaving the NSP to the ESMIG, and vice versa, is cryptographically protected (encrypted and authenticated). Part II: Verify that all data leaving the Di.Co.A. (using the Di.Co.A. emulator) to the NSP, and vice versa, is cryptographically protected (encrypted and authenticated). [on field]
Expected result:	All traffic – between the ESMIG and the NSP and between the NSP and the Di.Co.A. – is encrypted and authenticated, confidentiality and integrity of data in transit across the public soil is ensured.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

MEPT Non Repudiation in A2A

Requirement ID	ESMIG.50320

The NSP must manage the non-repudiation of emission on A2A messages. The NSP's Network Gateways of the sender must sign - on behalf of the Di.Co.A. - using the appropriate private key stored in the HSM. The signature must include the (digest of) message payload provided by the sending application. The signature data shall be delivered to the receiver together with the A2A message. The NSP's Network Gateways of the receiver must check the validity of the certificate and verify the signature (using the public key certificate of the sender).

Detailed test procedure:	Send a message from a Di.Co.A. (using the Di.Co.A. emulator) and check that the business payload is signed by the Network Gateway on the sender. The signature includes the (digest of) message payload and is delivered to the receiver together with the "instant" message. Verify that the Network Gateway of the receiver: 1. checks the validity of the signing certificate (for example include its ID in the CRL and verify that the Gateways rejects the message) 2. verifies the signature. [on field]
Expected result:	The non-repudiation mechanism is in place (signing is in line with the requirement described above).
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Non Repudiation support in A2A

Requirement ID	ESMIG.50330

The NSP must provide a non-repudiation support service to verify the signature of a message (this service could be requested by the Di.Co.A. in case of dispute or claim). In order to perform the signature validation, the Di.Co.A. should provide the signature and all signature-related information (including the A2A message to be validated) to the NSP. The NSP must be able to retrieve the certificate and the certificate status at the time of the signature. The verification report should containing at least the following information: User DN, User Status, the certificate information (certificate Serial Number, Issue Date, Expiry Date) and a verification summary.

The non-repudiation service must be available up to three months after the traffic exchange took place. The NSPs could choose their favourite modality to deliver this service (email, electronic workflow, ...).

Detailed test procedure:	A non-repudiation support service is made available by the NSP. Select an A2A message at least one week old. The message and all the associated necessary information is given to the NSP, who then verifies the validity of the signature and reports back the outcome of the verification. [on field]
Expected result:	The NSP performs the signature verification of the message and produces a report with an outcome of the validity assessment.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Digital Signature management

Requirement ID	ESMIG.50340

The NSP must ensure the sender of a message uses the certificate provided by the NSP to digitally sign the message. The receiver of the message must be able to check the validity of the signature by using the associated certificate (public key) of the sender.

Detailed test procedure:	Part I: The sender (ESMIG) digitally signs a message; the receiver (Di.Co.A. emulator) of the message is able to check the validity of the signature through the NSP. Part II: The sender (Di.Co.A. emulator) digitally signs a message; the receiver (ESMIG) of the message is able to check the validity of the signature through the NSP. [on field]
Expected result:	The digital signature is created with the certificate provided to the sender by the NSP and the receiver of the message is able to check the validity of this signature.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

5.7 Supplier relationship

Information security in supplier relationships

Requirement ID	ESMIG.50350

The NSP must propagate the relevant information security requirements also to his own suppliers; the subset of "relevant requirements" is contained in this Technical Requirement document, chapter 5, proposed by the NSP and validated by the ESMIG Operator. All relevant information security requirements must be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components to the NSP.

Detailed test procedure:	List the requirements contained in the Technical Requirement document (chapter 5), the NSP proposes the subset of information security requirements applicable to his own suppliers, the list is validated by the ESMIG Operator (which is empowered on what stays in the list and what not). The NSP demonstrate if and how these requirements are propagated to his own suppliers. [desk check]
Expected result:	Relevant information security requirements are propagated from the NSP to his own suppliers.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Supplier service delivery management

Requirement ID	ESMIG.50360

The NSP must regularly monitor and review supplier service delivery. Changes to the provision of services by suppliers, procedures and controls, must be managed in line with the previous requirement about “Information security in supplier relationships”.

Detailed test procedure:	The NSP demonstrates if and how is regularly monitoring and reviewing the supplier service delivery. [desk check]
Expected result:	Information security in supplier relationships is managed in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

6. MESSAGING SERVICES

The "application to application" (A2A) and "user to application" (U2A) modes

Requirement ID	ESMIG.60010

The NSP must offer the A2A and the U2A modes to the ESMIG and to the Di.Co.A..

Detailed test procedure:	Inspect the NSP Technical Solution describing the A2A mode, then go through the NSP Technical Solution describing the U2A mode. [desk check]
Expected result:	The NSP offers both A2A and U2A services to ESMIG and to its Di.Co.A..
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

6.1 A2A Common requirements

A2A multi-protocol support

Requirement ID	ESMIG.60020

The NSP must offer to the Di.Co.A. connectivity services using A2A DEP and MEPT protocols to exchange messages and files with all Market Infrastructure Service and Application via the ESMIG.

The NSP must support the message/file exchange based on the following addressing elements:

- Sender Address, to identify the sending network entity, according to the network addressing scheme (e.g. X500, URI);
- Receiver Address, to identify the receiving network entity, according to the network addressing scheme (e.g. X500, URI);
- Combination of Service and Environment names, to identify the business environment and the closed group of users (e.g. ESMIG Test #1, ESMIG Test #2, ESMIG Prod)
- Type of Message Flow, to identify different message typologies (e.g. Message2)

Detailed test procedure:	Send a DEP message/file from a Di.Co.A. (using the Di.Co.A. emulator). Collect the message at the receiving interface at the ESMIG and inspect the message itself. The four following addressing elements should be present: Sender Address, Receiver Address, Service and Environment names and Type of Message Flow. Repeat the test with a MEPT message[on field]
Expected result:	NSP routes the messages based on the four addressing elements mentioned above.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A NSP routing independency

Requirement ID	ESMIG.60030

The NSP must provide a location independent routing. The ESMIG is unaware of the physical location of the Di.Co.A. and viceversa. If the Di.Co.A. configuration changes, for example due to disaster recovery procedures, no changes are required to the ESMIG .

Detailed test procedure:	Part I: Assuming the Di.Co.A. has at least two sites, send a message to the ESMIG from a test Di.Co.A. (using the Di.Co.A. emulator to simulate "site 1"). Then, recover the Di.Co.A. on another site (using the Di.Co.A. emulator to simulate "site 2") and send another message. Check that both messages are received by the ESMIG while no configuration change has been performed. Part II: Send a message to the Di.Co.A. (using the Di.Co.A.emulator) from the ESMIG (site A). Then, recover the ESMIG on another site (site B) and send another message. Check that both messages are received by the Di.Co.A. (using the Di.Co.A. emulator) while no configuration change has been performed. [on field]
Expected result:	The ESMIG is unaware of the physical location of the Di.Co.A..
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A NSP flooding control

Requirement ID	ESMIG.60040

The NSP must implement an anti-flooding (throttling) mechanism to ensure that no single Di.Co.A. can affect the availability of the solution at ESMIG side.

Detailed test procedure:	Send from a Di.Co.A. (using the Di.Co.A. emulator) a set of messages with a rate higher than the threshold set by the NSP. The NSP should drop the messages above the predefined threshold rate. For example, before starting the test set a very low threshold (ie. 5 msg/sec), then try to send messages at a higher rate; the messages above threshold should be dropped. [on field]
Expected result:	The NSP has a throttling mechanism in place.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A message size management

Requirement ID	ESMIG.60050

The NSP rejects as soon as possible any message that is not in the allowed size range indicated for the specific protocol (DEP or MEPT). The NSP rejects the operation by sending back to the originator a negative acknowledgement message with the explanation of the error (e.g. "Message size out of allowed range.").

Detailed test procedure:	Generate from a Di.Co.A. (using the Di.Co.A. emulator) an oversized message and verify that the NSP rejects it and sends back to the Di.Co.A. Di.Co.A. a negative acknowledgement message. The ESMIG does not receive the initial oversized message. [on field]
Expected result:	The NSP rejects any message that is not in the allowed size range. The originator receives a negative acknowledgement message. The NSP rejects the oversized message as close as possible to the source.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A user authentication

Requirement ID	ESMIG.60060

The NSP must provide to the Di.Co.A. the required certificates to access the A2A messaging services. The private keys of the PKI certificates must be secured by means of FIPS 140-2 Level 3 HSM – compliant equipment.

Detailed test procedure:	The NSP delivered the certificates to the Di.Co.A.. Verify certificates' private keys are secured by means of FIPS 140-2 Level 3 HSM, and the protocols, including key length, are in line with the most up-to-date security recommendation (e.g. NIST 800-57). [on field]
Expected result:	The devices and the certificates provided by the NSP to the Di.Co.A. are in line with the requirement.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A closed group of user authorization

Requirement ID	ESMIG.60070

The NSP checks the authorization of the Di.Co.A. to access the ESMIG based on enforced rules at NSP level, supporting segregation of traffic flows between participants.

Detailed test procedure:	Part I: Send a message to the ESMIG from an authorized Di.Co.A. (using the Di.Co.A. emulator), then send another message from another Di.Co.A. (using the Di.Co.A. emulator) not present in the CGU. First one should pass, while the second one should fail. Part II: Add the second Di.Co.A. to the CGU and send messages from the ESMIG to both the Di.Co.A.. Check that each message is delivered only to the intended addressee. [on field]
Expected result:	The NSP checks that the Di.Co.A. belongs to the Closed Group of Users and guarantees the traffic segregation among different users.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ product version

Requirement ID	ESMIG.60080

The NSP must connect to the ESMIG sites using the IBM Message Queuing ("WMQ") transport protocol. The NSP uses a WMQ product version compliant with the WMQ version adopted by ESMIG.

Detailed test procedure:	Check the WMQ product version on all NSP's Network Gateways. Check the WMQ version on all ESMIG systems, ensure a bilateral compatibility. [on field]
Expected result:	The NSP adopts an WMQ product version compliant with the WMQ version adopted by the ESMIG. WMQ versions are either the same or compliant between each other.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ channels

Requirement ID	ESMIG.60090

The NSP must support the use of multiple channels to connect to the ESMIG WMQ infrastructure.

The NSP and the ESMIG shall jointly agree the channels set up for different flows.

Detailed test procedure:	Count the number of WMQ channels available for messages and for files store-and-forward. Verify NSP is able to manage all available WMQ channels simultaneously. [desk check + on field]
Expected result:	Each kind of flow – both messages and files store-and-forward - has at least one WMQ channel. The number of channels is bilaterally agreed.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ channels TLS connection

Requirement ID	ESMIG.60100

WMQ channel connections must be secured by using the TLS protocol and digital certificates exchanged between the ESMIG and the NSP. Digital certificates for the WMQ channels TLS connection are provided by the ESMIG Services Operator to the NSP.

Detailed test procedure:	Check that WMQ channels are secured with TLS certificates. Make sure that the TLS certificates are signed by a ESMIG Operator's compliant CA. [desk check + on field]
Expected result:	WMQ channels are secured with TLS certificates provided by the ESMIG Services Operator.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ channels type

Requirement ID	ESMIG.60110

The NSP must connect to the ESMIG WMQ infrastructure using client-server mode (channels SVRCONN located at the ESMIG sites). The name of the channels follows the ESMIG naming convention.

Detailed test procedure:	Check if the NSP connects to ESMIG WMQ in client-server mode (channels SVRCONN located at the ESMIG sites). The name of the channels should follow the ESMIG naming convention. [desk check + on field]
Expected result:	The NSP connects to ESMIG WMQ infrastructure using client-server mode and the channels name is compliant with the agreed naming convention.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ message queues

Requirement ID	ESMIG.60120

The NSP must manage a set of queues for each specific flow in the transport protocol. The name of queues shall follow the ESMIG naming convention. The NSP and the ESMIG shall jointly agree the WMQ configuration details.

Detailed test procedure:	Verify the WMQ message queues managed by the NSP are in line with ESMIG naming convention and the NSP is able to get and put messages on all the defined queues. [on field]
Expected result:	On each defined WMQ message queue NSP is able to manage the messages (reading from outgoing queues and writing to incoming queues) .
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ messages management - load balancing

Requirement ID	ESMIG.60130

The NSP must manage the load balancing across WMQ traffic queues (also belonging to different WMQ instances) for incoming messages/files (sent by Di.Co.A.) with a load balancing mechanism based on a random choice (e.g. round robin mechanism) across the queues dedicated to each kind of flow.

For outgoing messages the NSP must manage all WMQ traffic queues (also belonging to different WMQ instances) foreseen for this kind of flow.

Detailed test procedure:	The NSP gateway performs load balancing on traffic queues for incoming messages (sent by the Di.Co.A. using the Di.Co.A. emulator). Simulate incoming message traffic while monitoring the queues to verify the load balancing mechanisms. Simulate outgoing message traffic while monitoring the queues to verify that all messages are processed by the NSP. [desk check + on field]
Expected result:	There is a messages load balancing mechanism across WMQ queues for incoming messages. All outgoing messages are processed.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ message description section – CCSID

Requirement ID	ESMIG.60140

The NSP handles the WMQ message description section field CCSID based on the one used by ESMIG (character set name: UTF-8, CCSID: 1208).

Detailed test procedure:	Inspect the message description section field CCSID 1208. Take note of field value. [on field]
Expected result:	WMQ message description section field CCSID 1208 is populated with a significant and meaningful value.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WMQ additional headers

Requirement ID	ESMIG.60150

The NSP must support additional WMQ standard header RFH2 and JMS.

Detailed test procedure:	Check the additional header structure RFH2 and JMS in the WMQ messages. [on field]
Expected result:	NSP supports the additional header structure RFH2 and JMS in WMQ.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Di.Co.A. Emulator Access Point

Requirement ID	ESMIG.60160

The NSP must provide to the ESMIG a “Di.Co.A. Emulator access point” to perform testing/monitoring (continuous and/or specific after any change implementation).

The Di.Co.A. Emulator access point includes:

- a connectivity infrastructure at one of the ESMIG sites. The connectivity infrastructure is of the same type as the one provided to the Di.Co.A.;
- a minimal set of software components to manage simple message exchange, i.e. to trigger message sending and to support message receiving, emulating the basic configuration of a Di.Co.A..

The ESMIG Operator is able to use the Di.Co.A. Emulator software without the need of any prior notice to the NSP. It must be possible to have more than a single Emulator, to support the various Business Services and Application (e.g. T2, T2S, TIPS, ECMS) message exchange.

Detailed test procedure:	Verify that through the Di.Co.A. Emulator access point it is possible to manage simple message exchanges between the ESMIG and the emulated Di.Co.A.
Expected result:	The ESMIG Operator is able to use the Di.Co.A. Emulator access point without the need of any prior notice to the NSP.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

6.2 A2A DEP

Application to Application (A2A) mode

Requirement ID	ESMIG.60170

The NSP must support exchange of messages in A2A mode via "store-and-forward" and “real time” . The NSP must support exchange of files in A2A mode via "store-and-forward" and “real time”. For the real-time mode, although incoming/outgoing messages and files exchange are part of the DEP protocol, for the time being usage of real-time mode is limited to incoming messages only.

Detailed test procedure:	Part I: Send messages (A2A mode) via the “real time” transfer mode. Part II: Send messages (A2A mode) via the “store-and-forward” transfer mode. Part III: Send files (A2A mode) via the “store-and-forward” transfer mode. Part IV: Send files (A2A mode) via the “real time” transfer mode. Verify that all messages and files has been received.
Expected result:	The NSP exchange A2A messages via the "real time" transfer and "store-and-forward" mode; the NSP exchange A2A files in the "real time" transfer and "store-and-forward" mode.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Backup of messages and files

Requirement ID	ESMIG.60180

The NSP must create back-up copies of store-and-forward information exchanged (both messages and files) and must store them for a period of six months. A restore action using one back-up copy provided by the NSP will be tested by the ESMIG at least once a year.

Detailed test procedure:	Verify how the NSP intends to back up messages and files and how to retrieve them. [desk check] Select a message one week older and perform the restore procedure. Repeat the test for a file. [on field] [Please notice it is not practical to test six months retention period.]
Expected result:	The NSP is able to back up and restore messages and files.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Real-time timeout management

Requirement ID	ESMIG.60190

The NSP must manage the timeout for real-time message exchange. This timeout has a value of 60 seconds. The timeout will occur if the exchange of the message will not be completed in the timeout timeframe duration.

Detailed test procedure:	Position the receiver as not being able to receive messages. Send messages to the receiver. Verify a time out after 60 seconds.
Expected result:	The timeout occurs if the receiver is not available to receive the message in the timeout timeframe duration.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Usage for messages and files

Requirement ID	ESMIG.60200

The NSP must manage message/files exchanged with the ESMIG in the following format:

- The Exchange Header section contains all "service information" needed for the transport layer, exchanged between the NSP and the ESMIG to manage messages and files flows;
- The Exchange Payload for business layer (BusinessEnvelope + document or document set) section. This section contains "business information". It shall reach the receiver in an unchanged form, consequently the NSP shall not modify this section. The NSP shall not execute any checks on that content unless explicitly requested by a bilateral agreement between the NSP and the Di.Co.A.. The business layer does not fall into the scope of this document.

Detailed test procedure:	Jointly analyse the contents of the EH and EP and verify they are in line with the Technical Requirements. Identify defects, each defects shall be recorded in an action plan.
Expected result:	The NSP manages messages/files exchanges accordingly to the requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A message size limitations

Requirement ID	ESMIG.60210

The NSP must offer its A2A mode in compliance with the size limitations described in the Table 2 below. The Table 2 specifies the allowed size range for messages and files, without taking into account the communication protocols overheads.

	MINIMUM LENGTH	MAXIMUM LENGTH
Message channel	1	32 KB (KB=2^{10})
File channel	1	32 MB (MB=2^{20})

Table 2 – Size limit of messages and files

Detailed test procedure:	Send messages with business payload size equal and less than 32 KB. Send files with size equal and less than 32MB. Verify the messages are successfully delivered. Then send messages with business payload size larger than 32 KB. Send files with size larger than 32MB. Verify the messages are not delivered.
Expected result:	The NSP offers A2A services in compliance with the size limitations described in the Technical Requirement document. It is possible to send messages up to 32 KB and files up to 32MB.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A message delivery approach

Requirement ID	ESMIG.60220

The NSP shall deliver messages and files once and only once. In case of error or doubt conditions, a retry mechanism is implemented for store-and-forward traffic, but additional mechanisms to avoid message duplication are in place.

Detailed test procedure:	Send the same message twice. Verify the message in store-and-forward mode is delivered with a retryin case of error in the delivery (for example when the MQ is not accessible). Send the same file twice; verify the file in store-and-forward is delivered with a retry in case of error in the delivery (for example when the MQ is not accessible).
Expected result:	Duplicated messages do not reach the platform. Duplicated files do not reach the platform.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Message against file priority

Requirement ID	ESMIG.60230

The NSP must avoid that massive exchange of files negatively affects messages delivery.

Detailed test procedure:	Send a bulk quantity of files and simultaneously send a bulk quantity of messages. To avoid message queuing starvation in case of bulk file transfers in the Network, the NSP has installed a queuing / prioritising function.
Expected result:	The NSP avoids that massive exchange of files negatively affects the messages delivery.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Message and files retrieval

Requirement ID	ESMIG.60240

The NSP must be able to provide a resending functionality for store-and-forward traffic to the Di.Co.A. and ESMIG. During a predefined period of time (up to five calendar days or two business days), it will be possible for the Di.Co.A. or ESMIG operator to request the NSP to retrieve sent and/or received Store-and-forward traffic for relevant technical address/es.

Detailed test procedure:	Request to the NSP resending of the store-and-forward traffic to the Di.Co.A. emulator the traffic related to a specific timeframe. Request to the NSP resending of the store-and-forward traffic to the ESMIG the traffic related to a specific timeframe.
Expected result:	Verify the Di.Co.A. emulator and the ESMIG receive the store-and-forward traffic related to the specified timeframe.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

Unbalanced workload traffic management for T2S

Requirement ID	ESMIG.60250

A huge amount (unbalanced) workload Di.Co.A., can overload the queues shared with the others. As all the communication path between Di.Co.A. – NSP and T2S is based on queuing messages, the possible unbalanced workload of a specific Di.Co.A. could affect the transmission performance of the others (the messages are transported over the same shared resources - channels and queues).

For this reason, T2S offers the possibility to the NSP, under specific traffic volume conditions and only for CSDs and subject to specific agreement with ESMIG operator, to differentiate the path (channels) of the unbalanced workload traffic, in order to improve manageability.

Detailed test procedure:	Using an unbalanced channel send a bulk quantity of files/messages and simultaneously send a message/file using standard channel. To avoid message queuing starvation between unbalanced and standard channel.
Expected result:	The NSP avoids that massive exchange of messages/files via unbalanced channel negatively affects the messages/files sent via standard channel.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

6.2.1 A2A WebSphere MQ Requirements.

To manage A2A services, the NSP must connect to the WebSphere MQ ("**WMQ**") architecture of ESMIG. The NSP shall comply with the following requirements.

WebSphere MQ channels

Requirement ID	ESMIG.60260

The NSP must connect to at least one ESMIG WMQ channel for each kind of flows:

- Messages real-time
- Files real-time
- Messages store-and-forward
- Files store-and-forward

Detailed test procedure:	1. count the number of WMQ channels available for messages real-time; 2. count the number of WMQ channels available for files real-time; 3. count the number of WMQ channels available for messages store-and- forward; 4. count the number of WMQ channels available for files store-and-forward.
Expected result:	Each kind of flow (1. Messages real-time, 2. Files real-time, 3. Messages store-and-forward, 4. Files store-and-forward) has at least one WMQ channel.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WebSphere MQ message description section – MsgType

Requirement ID	ESMIG.60270

The NSP must manage the WMQ messages having the following MsgType: request, reply, report, datagram.

Detailed test procedure:	Inspect the MsgType in the WMQ messages. Check request, reply, report, and datagram.
Expected result:	The NSP manages the WMQ messages having the following MsgType: request, reply, report, and datagram.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WebSphere MQ message description section – Format

Requirement ID	ESMIG.60280

The NSP must manage the WMQ messages having the following format. The payload data of WMQ messages shall be handled as binary data during transfer. Therefore, the according format header field shall have the value NONE.

Detailed test procedure:	Check the String Format in the WMQ messages.
Expected result:	The NSP manages the WMQ messages having the String Format.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WebSphere MQ message structure

Requirement ID	ESMIG.60290

The NSP shall manage the exchange of message/file based on a WMQ message. A WMQ message is composed by a "Message Description" part (MQMD) and by a "Message Text" part.

The following WMQ message standard MQMD header fields shall be managed by the NSP and ESMIG when a message/file is exchanged:

DATA SECTION	DESCRIPTION
WMQ Message Description	No particular header (e.g. RFH2) are foreseen. • **MQMD.MsgType**: report/datagram values are allowed; • **MQMD.Format**: e.g. MQFMT_NONE; • **MQMD.MsgId** and **CorrelationId**; • **MQMD.Encoding**; • **MQMD**.**ApplIdentity**; • **MQMD**.**Feedback;** • **MQMD.CodedCharacterSetId**; • **MQMD.Report** option: set to the value MQRO_PAN, MQRO_NAN or MQRO_NONE; • **MQMD.Expiry**: this field will be used only for Real-Time Request traffic setting the value equal to the Real-Time time-out timeframe (e.g. 60 seconds). In this way it is possible to avoid the unnecessary management of already expired messages.
WMQ Message Text	• **Exchange Header** section: contains all "service information" needed for the transport layer, exchanged between the Di.Co.A. and the ESMIG to manage message and file flows; • **Business Envelope** for business layer: contains the Business Application Header or the File Application Header with document (or document set) section. • **Digital Signature** contains the signature at DEP level (signature at business level is, if present, inside the Business Envelope)

Detailed test procedure:	A WMQ message is composed by a "Message Description" part (MQMD) and by a "Message Text" part. Supported WMQ message are: MQMD.MsgType, MQMD.Format, MQMD.Enconding, MQMD.CodeCharacterSetId, MQMD.Report option, MQMD.Expiry. Messages are generated for each of the above types and the correct transport and delivery of the messages is verified.
Expected result:	The NSP manages the message / file exchange based on a WMQ message.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

WebSphere MQ general rules

Requirement ID	ESMIG.60300

The general rules summarized in the following table should be applied to WMQ messages. All other fields that are not specifically mentioned here should preserve their default values as defined in the WMQ API or as set as the defaults for the applied WMQ platform.

FIELD IN MQMD	GENERAL RULES	EXCEPTIONS AND FURTHER EXPLAINATIONS
StrucId	MQMD_STRUC_ID	
Version	MQMD_VERSION_1	MQMD_VERSION_2:·Version 2 of MQMD may be used. However, features that need MQMD version 2 are not supported (i.e. grouping or segmentation).
Report	MQRO_NONE	For Request and Response (and DeliveryNotification) DEP primitives (Datagram MsgType), it must be equal to 0; for Technical Ack (Report MsgType), it must be equal to MQRO_PAN (for Positive Technical Ack) or to MQRO_NAN (for Negative Technical Ack).
MsgType	MQMT_DATAGRAM	The message type of all Request and Response (and DeliveryNotification) DEP primitives will be MQMT_DATAGRAM. - For Technical Ack it will be MQMT_REPORT
Expiry	MQEI_UNLIMITED	The Expiry of Real-Time Request messages should be set to the equivalent of 60 seconds (i.e. the numerical value of 600).
Feedback		.Meaningful only for Report MsgType: must be equal to 0 for PAN (Positive Technical Ack), 1000 for NAN (Negative Technical Ack) and 2000 for Pseudo-NAN
Encoding		
CodedCharSetId		
Format	MQFMT_NONE.	
Priority	Default value	WMQ ESMIG queues are defined with default delivery mode in ESMIG as FIFO and the default priority set to 5. Message priority is not honoured unless there is a specific agreement with the connected counterparties. Priority can be set but will not be honoured by ESMIG in case of missing pre-agreement.
Persistence	Default value	WMQ queues in ESMIG are defined with default persistence set to YES. The messages inherit the queue definition. Requirements for deactivation of persistence need to be agreed with ESMIG.
MsgId		

FIELD IN MQMD	GENERAL RULES	EXCEPTIONS AND FURTHER EXPLAINATIONS
CorrelId		In Technical Ack, it must be set to the MQMD.MsgId value of the original Request/Response/Deliverynotification the Technical Ack refers to. In Response, it must be set to the MQMD.MsgId of the original Request the Response refers to.
BackoutCount	0	
ReplyToQ	Blanks	The fields ReplyToQ should never be set and never be checked for answers. All messages will be directed to the message queues that match the nature of that message (i.e. qualified by Real-Time or Store-and-Forward, file or message; data or Ack).
ReplyToQMgr	Blanks	ReplyToQmgr should never be set and never be checked for answers. All messages will be directed to the Queue Manager configured in the communication path.
UserIdentifier		
AccountingToken		
ApplIdentityData	Set to the system identification of the sending application (the counterparty's gateway hostname or the ESMIG hostname).	
PutApplType		
PutApplName		
PutDate	Date when message is sent	
PutTime	Time when message is sent	
ApplOriginData	Blanks	
GroupId		
MsgSeqNumber		
Offset		
MsgFlags		
OriginalLength		

Detailed test procedure:	Send a message and a file from the Di.Co.A. emulator to the ESMIG. Verify incoming MQMD fields are compliant for incoming message and file with the general rules reported in the previous table.
Expected result:	The NSP manages the message / file exchange using the MQMD field in the proper way.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

6.2.2 Protocol Description

A2A primitives

Requirement ID	ESMIG.60310

The NSP must manage the following primitives to exchange messages with the ESMIG:

- Request: The ESMIG uses this message type to send a message/file to a Di.Co.A. and vice versa. This kind of primitive shall be used in both real-time and store-and-forward mode;
- Response: The ESMIG uses this message type to answer to a previously received request. This kind of primitive is used only in real-time mode;
- TechnicalAck: this acknowledgement is provided for each data exchange between the communication counterparties (Di.Co.A. and ESMIG) for the confirmation of the completion of the data exchange. This kind of primitive shall be used both in real-time mode and in store-and-forward mode;
- DeliveryNotification: The NSP's gateway sends a message to inform the ESMIG about the successful/unsuccessful delivery of the original sent message/file. This kind of primitive is used only in store-and-forward mode;
- EnableSnFTraffic: The ESMIG sends to the NSP's gateway the request to enable the exchanging store-and-forward traffic;
- DisableSnFTraffic: The ESMIG sends to the NSP's gateway the request to disable the exchanging store-and-forward traffic;
- QuerySnFTraffic: The ESMIG sends to the NSP's gateway the request to query the status of store-and-forward traffic;
- EnableRTTraffic: The ESMIG sends to the NSP's gateway the request to enable the exchanging real-time traffic;
- DisableRTTraffic: The ESMIG sends to the NSP's gateway the request to disable the exchanging real-time traffic;
- QueryRTTraffic: The ESMIG sends to the NSP's gateway the request to query the status of real-time traffic;
- CloseTrafficChannels: The ESMIG sends to the NSP's gateway the request to inform the NSP about the start the Maintenance Window;
- OpenTrafficChannels: The ESMIG sends to the NSP's gateway the request to inform the NSP about the end of the Maintenance Window;
- QueryTrafficChannels: The ESMIG sends to the NSP's gateway the request to query the status of the Maintenance Window as known by the NSP Gateway.

Detailed test procedure:	The above mentioned primitive are tested using the following technical requirements: ESMIG.60440 ESMIG.60450 ESMIG.60390 ESMIG.60460 ESMIG.60470 ESMIG.60480
Expected result:	Verify all the listed technical requirements are successfully passed.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team_____date____/____/____ NSP testing team_____date____/____/____

A2A Primitives management

Requirement ID	ESMIG.60320

The NSP must manage the primitives to exchange messages/files with the ESMIG.

All these primitives are composed by an "Exchange Header" part and by a "Business Envelope" part.

The function of the Exchange Header (or Technical Envelope) is to provide the information needed to route the object (message or file) to the correct destination and to identify and describe the object type.

Hereafter is reported an example of a DEP protocol message:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
   xmlns:dep="http://www.ecb.eu/dep-2.0"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
   <dep:ExchangeHeader>
      <dep:Version>2.0</dep:Version>
      <dep:Sender>cn=appl1,o=prod</dep:Sender>
      <dep:Receiver>cn=cust1,o=nsp-name1</dep:Receiver>
      <dep:TechnicalServiceId>service1.nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
<dep:MessageId>MSGRT.NSPname1.20110101000000.000001</dep:MessageId>
      <dep:SendTimestamp>2018-01-01T00:00:00</dep:SendTimestamp>
      <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
      <dep:ExchangeStatus>OK</dep:ExchangeStatus>
   </dep:ExchangeHeader>
   <dep:BusinessEnvelope>
      <dep:BusinessApplicationHeader>
         <!-- business application header goes here -->
      </dep:BusinessApplicationHeader>
      <dep:BusinessMessage>
         <!-- business message goes here -->
      </dep:BusinessMessage>
   </dep:BusinessEnvelope>
</dep:Request>
```

The "Exchange Header" part shall be managed by the NSP's gateway in order to exchange data with ESMIG.

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:Version *<mandatory tag>*	Version of Data Exchange Protocol. **Enumeration** with fixed value "**2.0**"	<dep:Version> 2.0 </dep:Version>

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:Sender *<mandatory tag>*	Identification for the Technical Sender that sends the message. **Restriction** is set on base type "**string [100]**".	<dep:Sender> cn=appl1, o=prod </dep:Sender>
dep:Receiver *<mandatory tag>*	Identification for the Technical Receiver that receives the message. **Restriction** is set on base type "**string [100]**".	<dep:Receiver> cn=cust1, o=nsp-name1 </dep:Receiver>
dep:TechnicalServiceID *<mandatory tag>*	Name of the technical service used to send messages and files, made up by the Service, the DEP counterpart name, the message pattern and the environment of reference. Specifying a message pattern, it's possible to manage a message or a file as a payload of the DEP message. **Message pattern** means the following: • MSGRT: **Real Time Message**; • MSGSNF: **Store & Forward Message**; • FILERT: **Real Time File**; • FILESNF: **Store & Forward File**. **Restriction** is set on base type "**string [60]**", with expression in the format: <Service>+"."+<NSPName>+ "." + <msg-pattern> + "." + <environment> where <msg-pattern> is one of: MSGRT MSGSNF FILERT FILESNF and <environment> is one of: INTEG,IAC,EAC,UTEST, PROD (additional environment can be added)	<dep:TechnicalServiceId> Service1.nsp-name1.MSGRT.PROD </dep:TechnicalServiceId>

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:RequestType *<mandatory tag>*	Type of request, to classify message content. When there are different request types in the same BusinessEnvelope (multi-message), a multirequest value shall be used as RequestType **Restriction** is set on base type "**string [100]**".	<dep:RequestType> MultiRequest </dep: RequestType >
dep:CommunicationID *<minOccurs="0">*	Unique message identifier assigned by the ESMIG counterpart (at DEP transport level)l **Restriction** is set on base type "**string [100]**".	<dep:CommunicationId> nsp-name1.gtw134567. 20100908185555.123456 </dep:CommunicationId>
dep:ESMIGMessageId *<minOccurs="0">*	Unique message identifier generated by ESMIG **Restriction** is set on base type "**string [100]**".	<dep:ESMIGMessageId> MSGRT.NSPname1.20110101000000.000001 </dep:ESMIGMessageId>
dep:ActorMessageId *<minOccurs="0">*	Unique message identifier generated at Di.Co.A. site **Restriction** is set on base type "**string [100]**".	<dep:ActorMessageId> ActorGateway1.20100908175531.123456 </dep:ActorMessageId>
dep:EntryTimestamp *<minOccurs="0">*	Timestamp of the NSP's gateway reception based on UTC time with the following rule: ▪ the Zulu character shall be present ▪ fractional seconds are optional (maximum 3 digits) ▪ the representation of midnight is 00:00:00Z **Restriction** is set on base type "**dateTime**".	<dep:EntryTimestamp> 2011-01-01T00:00:00Z </dep:EntryTimestamp>

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:SendTimestamp *<mandatory tag>*	Timestamp of the sending of message, based on UTC time with the following rule: ▪ the Zulu character shall be present ▪ fractional seconds are optional (maximum 3 digits) ▪ the representation of midnight is 00:00:00Z **Restriction** is set on base type "**dateTime**".	<dep:SendTimestamp> 2011-01-01T00:00:00Z </dep:SendTimestamp>
dep:ReceiveTimestamp *<minOccurs="0">*	Timestamp of the receiving of message, based on UTC time with the following rule: ▪ the Zulu character shall be present ▪ fractional seconds are optional (maximum 3 digits) ▪ the representation of midnight is 00:00:00Z **Restriction** is set on base type "**dateTime**".	<dep:ReceiveTimestamp> 2011-01-01T00:00:01Z </dep:ReceiveTimestamp>
dep:PDMHistory *<minOccurs="0">*	Only for **Store-and-Forward**, Timestamp's list of the attempts of the delivery of the message, based on UTC time. This list contains a sequence of SendTimestamp entries. It also contains for each timestamp an optional AdditionalInfo. This is a **complex type** tag based on a sequence of maximum occurrences, each one containing two elements: • **TimeStamp**, a mandatory tag with base type **dateTime;** • **AdditionalInfo**, an optional tag with **restriction** set on base type "**string [100]**".	<dep:PDMHistory> <dep:TimeStamp> 2011-01-01T00:00:00Z </dep:TimeStamp> <dep:TimeStamp> 2011-02-14T00:10:01Z </dep:TimeStamp> <dep:AdditionalInfo> Annotation on 2th timestamp entry </dep:AdditionalInfo> </dep:PDMHistory>

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:DeliveryNotification *<minOccurs="0">*	Delivery notification management; this field has to be set only in the case of **Store-and-Forward mode**. The following values are foreseen: • "**YES**": the delivery notification is requested always • "**FAIL**": the delivery notification is requested only in case of failure • "**NO**": the delivery notification is not requested **Restriction** is set on base type "**string**".	<dep:DeliveryNotification> FAIL </dep:DeliveryNotification>
dep: NonRepudiationExchange *<mandatory tag>*	Flag that indicates if the non-repudiation is requested or not **Enumeration** with possible values: **YES** or **NO**.	<dep:NonRepudiationExchange> NO </dep:NonRepudiationExchange>
dep:Compression *<mandatory tag>*	Flag that indicates the algorithm used to compress the payload or "NONE" (if compression is not used) **Enumeration** with possible values "**NONE**" or "**ZIP**". The used compression format is ZIP implemented by DEFLATE algorithm into the ZLIB java libraries, moreover Base64 encoding need to be applied.	<dep:Compression> ZIP </dep:Compression>

TAG NAME	TAG DESCRIPTION / ALLOWED VALUES	EXAMPLE
dep:ExchangeStatus *<minOccurs="0">*	Status of the exchange: "OK" for successful exchange "KO" for failure This element must be present in DEP technical ack messages and in Response messages of R-T (message and file) exchange. **Enumeration** with possible values: • "**OK**" in the case of successful exchange • "**KO**" in case of failure	<dep:ExchangeStatus> OK </dep:ExchangeStatus>
dep:ErrorDescription *<minOccurs="0">*	Description of the error occurred during the exchanging process (tag has to be set only if tag dep:ExchangeStatus has value "KO") This is a **complex type** tag based on two elements: • **ErrorCode**, a mandatory tag with base type **string** and a validation pattern "**DEP[0-9]{3}E**". • **AdditionalInfo**, an optional tag with **restriction** set on base type "**string [2000]**".	<dep:ErrorDescription> <dep:ErrorCode> DEP040E </dep:ErrorCode> <dep:AdditionalInfo> Message expired. Receiver has not been connected for 14 days. </dep:AdditionalInfo> </dep:ErrorDescription>
dep:MessageDigest *<minOccurs="0">*	Used only in Technical Ack primitive when the NonRepudiationExchange flag has been set to YES. The digest has to be calculated based on the received DEP Exchange Header and Business Envelope using the same canonicalization and digest methods/algorithms described in requirement ESMIG60450. **Restriction** is set on base type "**string [1024]**".	

Table 3 – Exchange Header

Detailed test procedure:	Send and receive a message and a file using both real-time and store-and-forward exchange and verify all the mentioned tags are correctly used.
Expected result:	The NSP is able to manage DEP Exchange Header tags accordingly to the rules reported in Table 3.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

NSP inbound routing

Requirement ID	ESMIG.60330

The NSP must manage traffic routing related to the business services, each of them made of one or more components, see table below. Components can be specific (dedicated to a business service) or common (shared among different business services).

The NSP must be able, if requested, to route inbound traffic to different MQ queues, using the DEP tag named TechnicalServiceID ("service" field in particular).

The NSP must be able to add/remove component and/or business service if requested.

The following table is a sample describing the relationship between business service, component and TechnicalServiceID.

BUSINESS SERVICE	COMPONENT	TECHNICALSERVICEID (SERVICE FIELD)
T2S	T2S	T2S
T2S	CRDM	T2SCRDM
T2S	…..	T2S….
T2	RTGS	T2RTGS
T2	CLM	T2CLM
T2	CRDM	T2CRDM
T2	……	T2…..
ECMS	ECMS	ECMS

Detailed test procedure:	Send messages and files from the Di.Co.A. emulator to address different TechnicalServiceID.
Expected result:	Verify on ESMIG that based on the different TechnicalServiceID the NSP is able to perform routing of inbound traffic to the correct MQ queue.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Exchange Header management and validation

Requirement ID	ESMIG.60340

The "Exchange Header" shall include all necessary information for the sending and the managing of the data by the NSP and by the counterpart.

The NSP's gateway shall validate the "Exchange Header" of the message/file in order to check that all the required fields are present, in the right format (such as date, Boolean,) and filled in with the appropriate values indicated in the "allowed values" column of the "Exchange Header".

The NSP shall validate the “Exchange Header” for the message/file received from ESMIG and for the message/file that the NSP sends to the ESMIG.

The validation of the Exchange Header shall be based on the the XML Schema Definition (XSD) reported in “Annex 1 - DEP XSD”

Detailed test procedure:	Send from the Di.Co.A. emulator to ESMIG messages and files in real-time and store-and-forward. Send from the ESMIG to Di.Co.A. emulator messages and files in real-time and store-and-forward.
Expected result:	The NSP is able to manage for inbound (building Exchange Header) and outbound (verifying Exchange Header) traffic the Exchange Header based on the provided schema (Annex 2 – DEP XSD).
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____

	NSP testing team _____ date ____/____/____

Compression flag and compression algorithm management

Requirement ID	ESMIG.60350

The NSP must forward the "Compression" fields of the Exchange Header to the receiver. This field will specify the algorithm used to compress the business payload contained in the message. If the payload is not compressed, the compression field will contain the value NONE.

If compression is used the compression format is ZIP implemented by DEFLATE algorithm into the ZLIB java libraries, moreover Base64 encoding need to be applied. The compression field will contain in this case the value ZIP, size of business data after the uncompress operation cannot be more than 99MB.

Detailed test procedure:	Inspect the "Compression" and "Compression algorithm" fields of the technical envelope on one end and inspect the same envelope on the other end, make sure the contents of the two fields are still the same. Verify that uncompressed size of business data is not more than 99MB.
Expected result:	The NSP forwards the "Compression" and "Compression algorithm" fields of the technical envelope to the receiver.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____

	_____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Non-repudiation Exchange flag management

Requirement ID	ESMIG.60360

The NSP must manage the non-repudiation flag on exchanging of incoming and outgoing messages/files. In the following is described the process that the ESMIG and the NSP shall manage in case of non-repudiation.

If the non-repudiation is requested for a message / file:

- the sending part (e.g. ESMIG) shall sign the DEP Request or Response and insert the electronic signature into the Signature element;
- the receiving part (e.g. the NSP) shall verify the validity of the signature and send back an error message (NAN Technical ack) if the check fails (i.e. Code DEP301E), otherwise, the receiving part shall create a PAN Technical Ack;
- the receiving part shall sign the Technical Ack and insert the electronic signature into the Signature element;
- the sending part shall check the validity of the signature added to the Technical Ack and store the message.

The MessageDigest field shall be populated for each Technical ack with the DigestValue of the Reference (URI="") found in the Signature of the DEP Request or Response message acknowledged. In case the DigestValue cannot be found, the MessageDigest of the NAN technical ack contains the value "NOREF".

Signature management is based on the XML Advanced Electronic Signature (XAdES) standard for signature of DEP message/file exchange. In particular, the DEP adopts the BES (Basic Electronic Signature) signature format as defined in version 1.4.2 of the ETSI specification (ETSI TS 101 903 V1.4.2 of 2010-12). For the use within DEP messages, no additional signed properties should be included in the signature.

Additionally, signatures shall follow the manifest signature format of the W3C XML Signature Syntax and Processing recommendation (http://www.w3.org/TR/xmldsig-core/, section 2.3).

The signature shall contain:

- one Reference in the SignedInfo to the KeyInfo element. The KeyInfo must include a ds:X509Data element containing the certificate used to create the signature (not all the certification chain must be included);
- one Reference in the SignedInfo that points to the Manifest;
- a Manifest structure in its Object container. The Manifest itself will contain References as follows:
    - for Technical Ack:
        1. a Reference with empty URI covering the Technical Ack itself containing its DigestValue;
        2. one Reference with absent URI covering the content[2] of the BusinessEnvelope of the message or file for which the technical ack was generated containing its DigestValue, only for Technical Acks related to Request/Response; this Reference is not present in TechnicalAck related to DeliveryNotification.
    - for Request/Response (and DeliveryNotification):
        1. a Reference with empty URI covering the Request/Response (or DeliveryNotification) itself containing its DigestValue.

The algorithms used are:

- For the SignedInfo
    - CanonicalizationMethod must be http://www.w3.org/2001/10/xml-exc-c14n# (omitting XML comments)
    - SignatureMethod must be http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- For Reference
    - Digest algorithm must be http://www.w3.org/2001/04/xmlenc#sha256
    - Transform algorithm must be must be http://www.w3.org/2001/10/xml-exc-c14n# (omitting XML comments)
    - For Reference with empty URI must have an additional Transform algorithm http://www.w3.org/2000/09/xmldsig#enveloped-signature

[2] The content of the BusinessEnvelope could be defined using the following XPath expression:

```
std:string queryXPath =  pathToBusinessEnvelope + "/descendant::*/. | " +
// child nodes
                         pathToBusinessEnvelope + "/descendant::*/@* | " +
// attributes of child nodes
                         pathToBusinessEnvelope + "/descendant::*/namespace::* | " +
// namespaces of child nodes
                         pathToBusinessEnvelope + "/descendant::text()";
// text elements
```

The following sample shows the contents of a Technical Aack signature:

```
<ds:Signature ">
 <ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#"/>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
  <ds:Reference URI="# _b7a1a00e-e449-48ae-9d50-e0f48fc010f2">
   <ds:Transforms>
    <ds:Transform Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#"/>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
   <ds:DigestValue>...</ds:DigestValue>
  </ds:Reference>
  <ds:Reference Type="http://www.w3.org/2000/09/xmldsig#Manifest" URI="#_70f715b4-0330-4895-abb9-
6de4843e78b3">
   <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
   <ds:DigestValue>...</ds:DigestValue>
  </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue>...</ds:SignatureValue>
 <ds:KeyInfo Id="_b7a1a00e-e449-48ae-9d50-e0f48fc010f2">
  <ds:X509Data>
   <ds:X509Certificate>...</ds:X509Certificate>
  </ds:X509Data>
 </ds:KeyInfo>
 <ds:Object xmlns="http://www.w3.org/2000/09/xmldsig#">
  <ds:Manifest Id=" _70f715b4-0330-4895-abb9-6de4843e78b3">
   <ds:Reference URI="">
    <ds:Transforms>
     <ds:Transform Algorithm=http://www.w3.org/2000/09/xmldsig#enveloped-signature/>
     <ds:Transform Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>...</ds:DigestValue>
   </ds:Reference>
   <ds:Reference>
    <ds:Transforms>
     <ds:Transform Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>...</ds:DigestValue>
   </ds:Reference>
  </ds:Manifest>
 </ds:Object>
</ds:Signature>
```

Detailed test procedure:	Inspect the content of the Technical Ack in case of the original message is sent by ESMIG with the "dep:NonRepudiation" field set to YES. The Technical Ack must be signed by the NSP gateway as well as the original message must be signed by the ESMIG.
Expected result:	The NSP manage correctly the non-repudiation flag of the technical envelope.

Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message and file unique identification

Requirement ID	ESMIG.60370

The NSP must identify all messages and files with a unique identifier according to the format indicated in the "Exchange Header" description section. The NSP shall insert this unique identifier in the envelope (field NSP Communication ID) of all messages and file exchanged. This unique identifier will be used to prove the handover of the message/file between ESMIG and the NSP. The same identifier shall be used in the data exchange with the Di.Co.A..

Detailed test procedure:	Inspect the field NSP Communication ID in the technical envelope, field value is the same both in the path from ESMIG to NSP and from NSP to Di.Co.A..
Expected result:	The NSP identifies all messages and files with a unique identifier according to the format indicated in the "technical envelope" description section.

Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Message patterns

Requirement ID	ESMIG.60380

The NSP must manage the exchange of messages and files with the ESMIG in accordance with the following workflows.

Messages and files can be exchanged in real-time or in store-and-forward mode.
The NSP shall manage the following message/file patterns:

- Real-time outgoing
- Real-time incoming
- Store-and-forward outgoing
- Store-and-forward incoming

In all these message/file patterns is foreseen a "Technical Acknowledgement" ("**Tech-Ack**" or "**Technical Ack**") message between the NSP's gateway and the ESMIG to confirm the reception of the message/file.

Detailed test procedure:	1. Send message and file in Real-time outgoing pattern; 2. send message and file in Real-time incoming pattern;

	3. send message and file in Store-and-forward outgoing pattern; 4. send message and file in Store-and-forward incoming pattern. Verify that Technical Acknowledgements are received.
Expected result:	The NSP manages message / file exchanges in accordance with the workflows described in the Technical Requirements .
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Technical Acknowledgment management

Requirement ID	ESMIG.60390

A Technical Ack is provided for each exchange between the ESMIG and the NSP for the confirmation of the completion of the exchange.

The NSP shall manage the Technical Acknowledgement as described in the following. The Technical Ack is a WebSphere MQ report message of type PAN (Positive Application Notification) or NAN (Negative Application Notification). This report shall be sent back from the receiving WebSphere MQ application (the ESMIG middleware or the NSP's

gateway function) when the message is taken in charge (e.g. the message is stored or managed). The structure of the "Technical Ack" is the following:

1. In the MQMD.Feedback field of the MQ Message Descriptor the value 0 (zero) in case of PAN or a positive numeric value in case of NAN shall be returned;
2. In the "Application Identity Data" of the MQMD, the system identification of the receiving application (the NSP's gateway hostname or the ESMIG hostname) shall be returned.
3. In the "Correlation Id" field of the MQMD section the "Message Id" value of the original message shall be returned.
4. In the "Message Text" part of the MQ message, the "Exchange Header" of the original message, updated as foreseen in the following message patterns description in the case of a PAN shall be reported. In case of NAN the field "dep:ErrorDescription" must be filled with an error message as described in the requirement ESMIG.60400.
5. In case of store-and-forward sent to the ESMIG the NSP shall forward the full content of the “Message Text” part of the MQ message to the Di.Co.A. in the delivery notification.

The Technical Ack shall be returned to the sender (ESMIG or NSP) within a time-frame of an initial value of 10 minutes (this value could be changed in a flexible way at a later time). For the real-time mode no particular actions are required if this time is exceeded because of the already foreseen time-out mechanism management. For the store-and-forward incoming message flow if the time-frame for the Technical Ack is exceeded, the NSP shall re-send the message including in the ExchangeHeader section the “dep:PDMHistory” element with the delivery time of the previous attempt(s) in the following format:

```
<dep:PDMHistory>
    <dep:TimeStamp>2018-11-12T14:53:52Z</dep:TimeStamp>
    <dep:TimeStamp>2018-11-12T15:03:55Z</dep:TimeStamp>
    <dep:TimeStamp>2018-11-12T15:13:56Z</dep:TimeStamp>
</dep:PDMHistory>
```

As described in requirement ESMIG.60450, after 10 unsuccessful attempts the NSP shall send back to the original sender a “Delivery Notification Failure” and shall suspend the

sending of the store-and-forward messages/files to the ESMIG. An alarm shall be triggered in order to allow to the NSP staff to inform the ESMIG Service Desk that a problem occurred in the store-and-forward channel.

Detailed test procedure:	Verify the structure of the Technical Acknowledgement structure contains: 1. MQMD.Feedback, 2. "Application Identity Data", 3. "Correlation Id", 4. "Message Text" as described in the Technical Requirements.
Expected result:	The NSP manages the Technical Acknowledgement, which can be either Positive Application Notification (PAN) or Negative Application Notification (NAN).
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Negative Technical Acknowledgment – Error description fields

Requirement ID	ESMIG.60400

The NSP and ESMIG must manage the negative message acknowledgement in all cases of error. In this case a NAN must be returned to the originator of the message. The "dep:ExchangeStatus" field must be set to the value "KO" and the "dep:ErrorDescription" field must be set accordingly to the following table:

CATEGORIZATION	CODE	ERROR DESCRIPTION FIELD VALUE	DESCRIPTION
Protocol errors [**DEP1xxE**]	**DEP100E**	Message or file size is not in the allowed size range	Received communication size is bigger then the maximum size allowed for the communication service used
	DEP101E	Field xxxx missing	The field reported in the error text is required for the communication exchange workflow (see DEP protocol description for further information)
	DEP102E	Communicationid/ESMIGMessageId/ActorMessageId not unique	The ID provided in the Request is not unique
	DEP104E	maximum number of retries attempt reached	For the Snf communication service the message has been received 10 times with ''PDMHistory''.
	DEP105E	Timeout occurred	For the RT communication service the timeout condition occurred before receiving the response to the original request (timeout is normally set to 60 seconds)
	DEP106E	Unmatched response	For the RT communication service, the response is received and there are no Request matching (via MQMD.MsgId).

CATEGORIZATION	CODE	ERROR DESCRIPTION FIELD VALUE	DESCRIPTION
Addressing errors [**DEP2xxE**]	**DEP200E**	Wrong sender/receiver or not configured	The DEP sender or receiver fields refer to DN that are not configured at NSP or ESMIG level.
	DEP201E	TechnicalServiceId not correct	The information reported in the TechnicalServiceId is not correct. It could be related to wrong logical environment addressed
	DEP202E	Message in wrong queue	The communication was put into a queue not compatible with the selected messaging service (e.g. the TechnicalServiceId refers to MSGRT service while the communication was put into an MQ queue dedicated to the FILESNF messaging service) or the VA-NSP part of the TechnicalServiceId is unknown
Non-repudiation errors [**DEP3xxE**]	**DEP300E**	NonRepudiationExchange field not set in store-and-forward exchange	The received communication was sent via SNF service but the NonRepudiationExchange field is not set accordingly
	DEP301E	Signature validation failure	The certificate or the signature present in the DEP ExchangeHeader is not valid
Validation errors [**DEP4xxE**]	**DEP400E**	Error during MQMD validation	MQMD content is not compliant with the DEP specification or it is corrupted

CATEGORIZATION	CODE	ERROR DESCRIPTION FIELD VALUE	DESCRIPTION
	DEP401E	XML not well formed	The ExchangeHeader validation fails. It is not compliant with the DEP protocol XSD or the xml is corrupted
Compression errors [**DEP5xxE**]	**DEP500E**	ESMIG does not process decompressed communication which size exceeds 99 MB	The communication after the decompression process is bigger than 99 MB
	DEP501E	The Di.Co.A. sending the inbound A2A communication has not used a compression algorithm supported by ESMIG	An error occurred during the decompression of the communication. The file is corrupted or an algorithm not supported by ESMIG was used to compress it
Generic errors [**DEP9xxE**]	**DEP999E**	Error occurred. Message/File exchange aborted	For all the errors not listed in the available error codes

Table 4 – Error messages

The text presented in the "ERROR DESCRIPTION" column above represents the value to be used for field "AdditionalInfo" in block ErrorDescription". However, each implementation may add, if available and without any obligation, additional free text **after** the “standard” message foreseen in the above table to provide any useful information to further clarify the error condition detected. In any case, DEP counterparties should not process the additional text, setting aside the logging for problem determination support.

Detailed test procedure:	Inspect "dep:ExchangeStatus" and "dep:ErrorDescription" field in case a NAN must be returned to the message originator. Flag differences if the result differs from the expected result. Trigger corrective actions.
Expected result:	In this case a NAN must be returned to the message originator. The "dep:ExchangeStatus" field must be set to the value "KO" and the "dep:ErrorDescription" field must be

	set in accordance with the table in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Pseudo-NAN

Requirement ID	ESMIG.60410

The Pseudo NAN is sent back to the sender in the event of format errors that prevent the correct handling of the DEP protocol.

It is used in the following error conditions:

Validation errors DEP4xxE

- DEP400E Error during MQMD validation
- DEP401E XML not well formed

If the WMQ message being checked does not comply with the expected rules, it is considered a “poisonous” or “garbage” message. If the “garbage” message has been read from a WMQ queue related to Request/Response/DeliveryNotification, a Pseudo-NAN is generated and sent onto the WMQ queue related to Technical Ack. If the “garbage” message has been read from a WMQ queue related to Technical Ack, no Pseudo-NAN is generated.

The MQMD.FEEDBACK field shall be filled with 2000. This information helps the receiver of the NAN to understand that the message refers to a Pseudo NAN so as to apply the correct validation procedure.

Then the message shall be filled with the following information:

• The meaningful fields are:

- ReceiveTimestamp: contains the arrival timestamp of the ''incorrect'' message;
- TechnicalServiceID : possibly built by extracting information from the MQ queue where the message was obtained from;
- SendTimestamp: copied from the ReceiveTimestamp.

• The following fields shall be filled with predefined values as in the example:

- Error description: contains the validation error which occurred;
- NonRepudiationExchange: is always set to NO;
- Compression: is always set to NONE.

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:TechnicalAck
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>2.0</dep:Version>
    <dep:Sender>NOREF</dep:Sender>
    <dep:Receiver>NOREF</dep:Receiver>
    <dep:TechnicalServiceId> service1.nsp-name1.MSGRT.PROD  </dep:TechnicalServiceId>
    <dep:RequestType>NOREF</dep:RequestType>
    <deè:CommunicationId>NOREF</dep:CommunicationId>
    <dep:ESMIGActorMessageId>NOREF</dep:ESMIGActorMessageId>
    <dep:SendTimestamp>2019-01-01T12:00:05Z</dep:SendTimestamp>
    <dep:ReceiveTimestamp>2012-01-01T12:00:05Z</dep:ReceiveTimestamp>
    <dep:NonRepudiationExchange>NO</dep:NonRepudiationExchange>
    <dep:Compression>NONE</dep:Compression>
    <dep:ExchangeStatus>KO</dep:ExchangeStatus>
    <dep:ErrorDescription>
      <dep:ErrorCode>DEP401E</dep:ErrorCode>
      <dep:AdditionalInfo>XML not well formed</dep:AdditionalInfo>
    </dep:ErrorDescription>
  </dep:ExchangeHeader>
</dep:TechnicalAck>
```

Detailed test procedure:	Send from the ESMIG to the NSP an invalid Request (real-time and store-and-forward) and verify that the Pseudo-NAN is sent back from the NSP to the ESMIG.
Expected result:	The NSP is able to generate a Pseudo-NAN.

Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2.3 Real-time Outgoing

Real-time outgoing management

Requirement ID	ESMIG.60420

The NSP must manage the real-time outgoing message pattern as detailed below.

The scenario to be considered is one when the ESMIG sends a message/file in real-time mode to a counterpart. This message pattern is shown in the following figure:

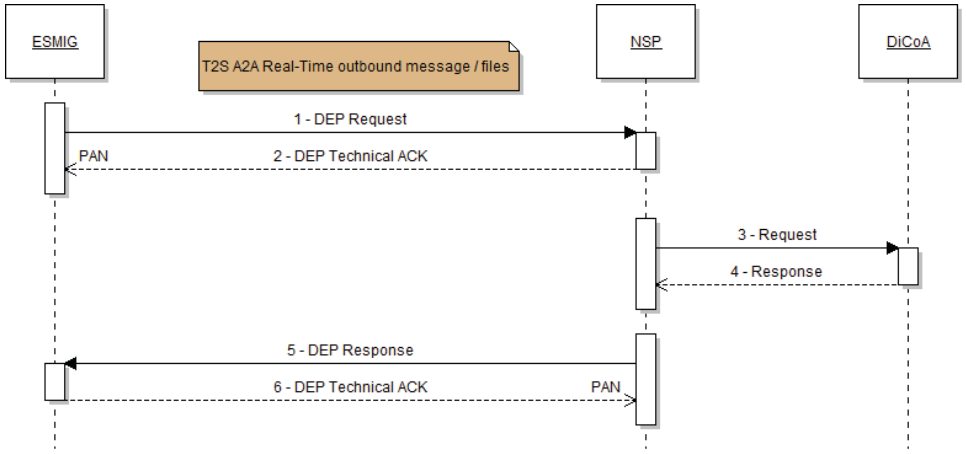


Figure 4 – Real-time outgoing flow

When the ESMIG needs to send a message in real-time mode to a Di.Co.A. it will go through the following steps.

STEP NUMBER	STEP DESCRIPTION
1)	The ESMIG sends a "Request" primitive to the NSP's gateway. The "ESMIGMessageId" field has to be generated by the ESMIG (this identifier shall be unique at ESMIG level).
2)	The NSP's gateway receives the message/file and performs the validation check of the "Exchange Header" part and checks of the size of the message/file. If the validation process fails, then the NSP's gateway sends back to ESMIG a "NAN Technical Ack" setting the error description field with the reason of the failure and the flow is completed. Otherwise, the NSP's gateway saves the message, assigns a unique identification to it, stores this value in the "dep:CommunicationID" field of the "Exchange Header", saves the current timestamp in the "dep:EntryTimestamp" field and sends back to ESMIG a "PAN Technical Ack".
3)	The NSP then sends the message to the Di.Co.A.. If there is an error in the transmission to the final receiver (for instance the receiver is not connected) or the transmission is not completed in the "timeout" timeframe, then the NSP's gateway sends back to the ESMIG a Response message with the "dep:ExchangeStatus" set to "KO" and the "dep:ErrorDescription" field set with the reason of the error occurred and the flow is completed. The business part of the response message in case of error will be not included in the message.
4)	The receiver sends back the response to the NSP's gateway setting in the message header a unique identification of the response generated at receiver site.
5)	The NSP's gateway checks the size of the message coming from the receiver. If the size is outside of the allowed range the message is rejected and an error message is returned to the receiver: in this case a response message is sent to the ESMIG with the "dep:ErrorDescription" field set to "ERROR occurred – Message/File exchange aborted" value. In the case of a successful result of the check the NSP sends the "Response" to the ESMIG setting in the "Exchange Header": • the same "dep:CommunicationID" and "dep:EntryTimestamp" fields used for the original "Request" ; • the field "dep:ActorMessageId" with the unique identification generated at client site; • the field "dep:SendTimestamp" with the time of the sending time (cfr. point 4)
6)	The ESMIG performs the "Exchange Header" validation and sends back to the NSP's gateway a PAN or NAN "Technical Ack".

A set of possible messages for this pattern is reported below as an example.

Message sent by ESMIG to the NSP's gateway at the step no. 1:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
```

```
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=appl1,o=prod</dep:Sender>
  <dep:Receiver>cn=cust1,o=nsp-name1</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
  <dep:ESMIGMessageId>MSGRT.NSPname1.20110101000000.000003</dep:ESMIGMessageId>
  <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
  <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
  <dep:Compression>NONE</dep:Compression>
 </dep:ExchangeHeader>
 <dep:BusinessEnvelope>
  <dep:BusinessApplicationHeader>
   <!-- business application header goes here -->
  </dep:BusinessApplicationHeader>
  <dep:BusinessMessage>
   <!-- business message goes here -->
  </dep:BusinessMessage>
 </dep:BusinessEnvelope>
</dep:Request>
```

Technical Ack (data part) sent by the NSP's gateway to the ESMIG at the step no. 2:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:TechnicalAck
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=appl1,o=prod</dep:Sender>
  <dep:Receiver>cn=cust1,o=nsp-name1</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
  <dep:CommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:CommunicationId>
  <dep:ESMIGMessageId>MSGRT.NSPname1.20110101000000.000003</dep:ESMIGMessageId>
  <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
  <dep:SendTimestamp>2011-01-01T00:00:01</dep:SendTimestamp>
  <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
   <dep:Compression>NONE</dep:Compression>
  <dep:ExchangeStatus>OK</dep:ExchangeStatus>
 </dep:ExchangeHeader>
</dep:TechnicalAck>
```

Response sent by NSP's gateway to ESMIG at the step no. 5

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Response
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=cust1,o=nsp-name1</dep:Sender>
  <dep:Receiver>cn=appl1,o=prod</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
  <dep:CommunicationId> service1.nsp-
name1.gtw134567.20100908185555.123456</dep:CommunicationId>
<dep:ActorMessageId>ActorGateway1.20100908175531.123456</dep:ActorMessageId>
  <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
  <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
  <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
  <dep:Compression>NONE</dep:Compression>
 </dep:ExchangeHeader>
 <dep:BusinessEnvelope>
  <dep:BusinessApplicationHeader>
   <!-- business application header goes here -->
  </dep:BusinessApplicationHeader>
```

```
   <dep:BusinessMessage>
     <!-- business message goes here -->
   </dep:BusinessMessage>
  </dep:BusinessEnvelope>
</dep:Response>
```

Detailed test procedure:	Send a message from ESMIG to Di.Co.A. in real-time mode. Follow the sequence of steps described in the Technical Requirements. Inspect the message sent by the ESMIG to the NSP's gateway at the step #1. Inspect the Technical Acknowledgment sent by the NSP to the ESMIG at the step #2. Inspect the response sent by the NSP to the ESMIG at the step #5. Repeat the test in negative mode. Repeat the same test for a file.
Expected result:	The NSP manages the real-time outgoing message pattern as detailed in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2.4 Real-time Incoming

Real-time incoming management

Requirement ID	ESMIG.60430

The NSP must manage the real-time incoming message pattern as detailed below.

An incoming real-time message is when the ESMIG receives a message/file in real-time mode from a Di.Co.A.. This message pattern is shown in the following figure.

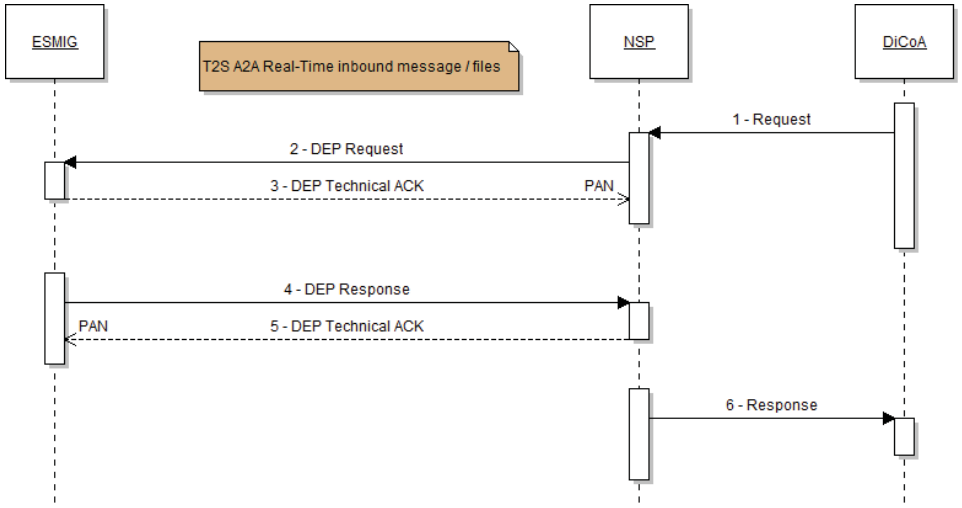


Figure 5 – Real-time incoming flow

When the ESMIG receives a message/file in real-time mode from NSP's gateway it will go through the following steps.

STEP NUMBER	STEP DESCRIPTION
1)	The Di.Co.A. sends a real-time message/file to the NSP's gateway. If the size of the message/file is outside of the allowed range the NSP's gateway must reject the exchange with an error message sent to Di.Co.A.
2)	The NSP's gateway sends a "Request" primitive to the ESMIG. The "CommunicationId" envelope field has to be generated by the NSP (this identifier shall be unique at NSP level). The ActorMessageId has to be set to the unique message identification generated at Di.Co.A. site.

3)	The ESMIG receives the message/file and performs the validation check of the "Exchange Header" and checks the size of the message/file. After the validation of the envelope, the ESMIG sends back to the NSP's gateway a PAN or NAN "Technical Ack" setting the “dep:ReceiveTimestamp” with the receiving time (MQMD.putime field of the WMQ message). If a NAN is returned the flow is completed and the NSP has to inform the counterpart about the failure. If the ESMIG doesn't answer with a response in the timeout timeframe, the NSP shall send a "timeout" information to the sender.
4)	The ESMIG sends the "Response" message to the NSP's gateway, setting in the "Exchange Header" the "dep:ESMIGMessageId" to a unique identifier and keeping all other fields as received in the request.
5)	The NSP's gateway receives the "Response" and performs the validation check of the "Exchange Header" part and of the size. If the validation process fails, or the size of the response is not in the allowed range, then the NSP's gateway send back to the ESMIG a "NAN Technical Ack" setting in appropriate way the "dep:ExchangeStatus" and "dep:ErrorDescription" fields. The NSP informs the Di.Co.A. about the failure with a response error messages. The flow is completed.
6)	The NSP's gateway sends the "Response" to the counterpart including the information of the ESMIGMessageId fields generated at the ESMIG site (cfr step no.4)

The following messages describes, as an example, a set of possible messages for this pattern.

"Request" message received by ESMIG step no. 2

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=cust1,o=nsp-name1</dep:Sender>
  <dep:Receiver>cn=appl1,o=prod</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
  <dep:CommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:CommunicationId>
  <dep:ActorMessageId> 2011-11-01T00:00:25.18476.903847Z</dep:T2SActorMessageId>
  <dep:EntryTimestamp>2011-01-01T00:04:00</dep:EntryTimestamp>
  <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
   <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
  <dep:Compression>NONE</dep:Compression>
 </dep:ExchangeHeader>
 <dep:BusinessEnvelope>
  <dep:BusinessApplicationHeader>
   <!-- business application header goes here -->
  </dep:BusinessApplicationHeader>
  <dep:BusinessMessage>
   <!-- business message goes here -->
  </dep:BusinessMessage>
 </dep:BusinessEnvelope>
</dep:Request>
```

Detailed test procedure:	The ESMIG receives a message in real-time mode from a Di.Co.A.. It goes through the six steps described in the

	Technical Requirements. Inspect message at step #2. Repeat the test in negative mode. Repeat same test for a file.
Expected result:	The NSP manages the real-time incoming message pattern as detailed in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2.5 Store-and-Forward Outgoing

Store-and-forward outgoing management

Requirement ID	ESMIG.60440

The NSP must manage the store-and-forward outgoing message pattern as detailed below.

An outgoing store-and-forward message is when the ESMIG sends a message/file in store-and-forward mode to a Di.Co.A.. This message pattern is shown in the following figure:

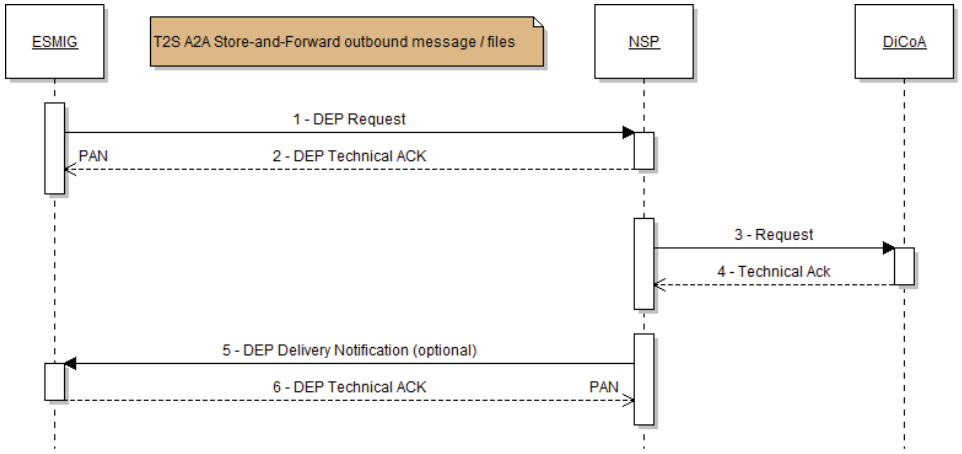


Figure 6 – Store-and-forward outgoing flow

When the ESMIG needs to send a message in store-and-forward mode to its clients, it will take the following steps.

STEP NUMBER	STEP DESCRIPTION
1)	The ESMIG sends a "Request" primitive to the NSP's gateway. The "ESMIGMessageId" envelope field is generated by the ESMIG (this identifier shall be unique at ESMIG level).
2)	The NSP's gateway receives the message/file and performs the validation check of the "Exchange Header" part and the validation of the size of the message/file. If the validation process fails, the NSP's gateway sends back to the ESMIG a "NAN Technical Ack" setting in the "dep:ExchangeStatus" and "dep:ErrorDescription" fields appropriately and the flow is completed. If the validation check is passed, the NSP's gateway sends back to ESMIG a "PAN Technical Ack" setting the "dep:CommunicationId" and the "dep:EntryTimestamp" fields of the Exchange Header.
3)	If the receiving Di.Co.A. is available for store-and-forward traffic, the NSP's gateway shall send the message/file to it.
4)	The receiving Di.Co.A. sends back to the NSP's gateway a "Technical Ack" (if and in the form agreed between the NSP and the Di.Co.A.).
5)	If the delivery of message/file has failed for 10 times when the receiver is available, or the Di.Co.A. is unavailable for store-and-forward traffic for 14 calendar days, the NSP's gateway sends back to the ESMIG a "DeliveryNotif" message with the same "Communication id" of the original request and with the information of the error occurred on the delivery. If in the original request the "dep:DeliveryNotification" field was set to "YES", the NSP shall send a "DeliveryNotifaction" message also in successful condition. When the "DeliveryNotification" is received by the ESMIG, it sends a Technical Ack back to the NSP and the flow is completed.

The following messages describe, as an example, a set of possible messages for this pattern.

"Request" message sent by the ESMIG at step no.1

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=appl1,o=prod</dep:Sender>
  <dep:Receiver>cn=cust1,o=nsp-name1</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
<dep:ESMIGMessageId> MSGSNF.NSPname1.20110101000000.000005</dep:ESMIGMessageId>
  <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
 <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
  <dep:Compression>NONE</dep:Compression>
 </dep:ExchangeHeader>
 <dep:BusinessEnvelope>
  <dep:BusinessApplicationHeader>
   <!-- business application header goes here -->
  </dep:BusinessApplicationHeader>
  <dep:BusinessMessage>
   <!-- business message goes here -->
  </dep:BusinessMessage>
 </dep:BusinessEnvelope>
</dep:Request>
```

Data part of the Technical Ack received by the ESMIG at step no. 2

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:TechnicalAck
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
  <dep:Sender>cn=appl1,o=prod</dep:Sender>
  <dep:Receiver>cn=cust1,o=nsp-name1</dep:Receiver>
  <dep:TechnicalServiceId>service1.nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
  <dep:CommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:CommunicationId>
   <dep:ESMIGMessageId>MSGSNF.NSPname1.20110101000000.000005</dep:ESMIGMessageId>
  <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
  <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
  <dep:Compression>NONE</dep:Compression>
<dep:ExchangeStatus>OK</dep:ExchangeStatus>
 </dep:ExchangeHeader>
</dep:TechnicalAck>
```

DeliveryNotif failure message received by the ESMIG in the case of a delivery notification failure from the NSP's gateway:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:DeliveryNotification
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:ExchangeHeader>
  <dep:Version>2.0</dep:Version>
```

```
   <dep:Sender>cn=appl1,o=prod</dep:Sender>
   <dep:Receiver>cn=tcust1,o=nsp-name1</dep:Receiver>
   <dep:TechnicalServiceId>service1.nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
   <dep:CommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:CommunicationId>
   <dep:ESMIGMessageId>MSGSNF.NSPname1.20110101000000.000003</dep:ESMIGMessageId>
   <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
   <dep:SendTimestamp>2011-01-01T00:00:01</dep:SendTimestamp>
    <dep:DeliveryNotification>FAIL</dep:DeliveryNotification>
   <dep:NonRepudiationExchange>YES</dep:NonRepudiationExchange>
   <dep:ExchangeStatus>KO</dep:ExchangeStatus>
   <dep:ErrorDescription>
    <dep:ErrorCode>DEP999E</dep:ErrorCode>
    <dep:AdditionalInfo>Error occurred. Message/File exchange aborted</dep:AdditionalInfo>
   </dep:ErrorDescription>
  </dep:ExchangeHeader>
</dep:DeliveryNotification>
```

Detailed test procedure:	In guaranteed delivery (store-and-forward) mode send a message from ESMIG to Di.Co.A.. Inspect message at step #2, and at step #3. Repeat the test in negative mode. Repeat same test for a file.
Expected result:	The ESMIG sends a message in Store-and-forward mode to a Di.Co.A.. The message sequence matches the five steps in the Technical Requirements describing this sequence.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2.6 Store-and-Forward Incoming

Store-and-forward incoming management

Requirement ID	ESMIG.60450

The NSP must manage the store-and-forward incoming message pattern as detailed below.

An Incoming Store-and-Forward message is when the ESMIG receives a message/file in store-and-forward mode from a Di.Co.A.. This message pattern is shown in the following figure:

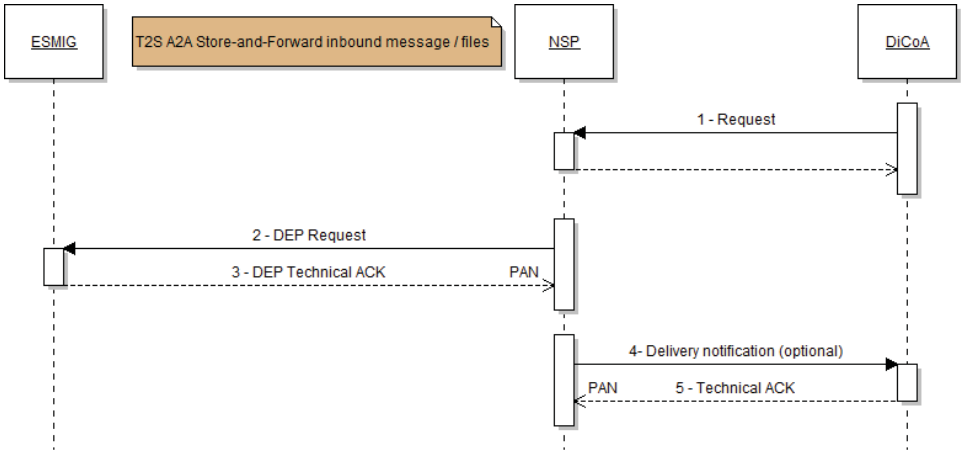


Figure 7 – Store-and-forward incoming flow

When the ESMIG needs to receive a message/file in store-and-forward mode from its clients, it will take the following steps.

STEP NUMBER	STEP DESCRIPTION
1)	The Di.Co.A. sends the message/file to the NSP's gateway
2)	The NSP's gateway sends back to the Di.Co.A. a "Technical Ack" after performing the check on the size of message/file (and rejecting the message if the check fails).
3)	If the ESMIG has enabled the store-and-forward traffic, the NSP's gateway sends the message/file to the ESMIG.

4)	The ESMIG receives the message/file and performs the validation check of the "envelope" part. If the ESMIG doesn't send the Technical Ack within 10 minutes the NSP shall manage the condition as described in the requirement ESMIG.60390. After the validation check, the ESMIG sends back to the NSP's gateway a PAN or NAN "Technical Ack" setting the "dep:ReceiveTimestamp" with the receiving time (MQMD.putime field of the WMQ message). If a NAN is returned, the NSP shall retry for up to 10 times the delivery after which a delivery failure notification is send back to the Di.Co.A. and the flow is completed.
5)	Depending on the connectivity service agreement between the NSP and the Di.Co.A., the NSP sends to the Di.Co.A. a delivery or delivery failure notification including the timestamp of the reception set by ESMIG in the field "dep:ReceiveTimestamp" mentioned above.

Detailed test procedure:	ESMIG receives a message in guaranteed delivery (store-and-forward) mode from a Di.Co.A.. The message goes through a five steps sequence. Verify all five steps are in line with what described in the Technical Requirements document. Repeat the test in negative mode. Repeat the same test for a file.
Expected result:	The NSP manages the Store-and-forward incoming message pattern as detailed in the Technical Requirements document.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2.7 Maintenance Window primitives

Enable/Disable/Query incoming store-and-forward traffic

Requirement ID	ESMIG.60460

The NSP must manage the store-and-forward incoming "traffic" as detailed below.

ESMIG shall be able to enable/disable the exchanging of store-and-forward traffic in order to avoid the reception of this kind of traffic during the "maintenance window" or for particular contingency reason.

When the ESMIG is ready to manage the store-and-forward traffic it sends an "EnableSnfTraffic" to the NSP's gateway. This is a "services" primitive and doesn't contain the "envelope" used for "business" message exchange. An example of this message is set out below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:EnableSnfTraffic
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
        <dep:Service>
                <dep:Name>service1.nsp-name1.MSGSNF.PROD</dep:Name>
                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                <dep:DestQueueName> NSPNAME1.MSGSNF.INCOMING.L01</dep:DestQueueName>
        </dep:Service>
        <dep:Service>
                <dep:Name>service1.nsp-name1.FILESNF.PROD</dep:Name>
                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                <dep:DestQueueName>NSPNAME1.FILESF.INCOMING.L01</dep:DestQueueName>
        </dep:Service>
</dep:EnableSnfTraffic>
```

An example of the response of the NSP's gateway to this message is the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:EnableSnfTrafficAck
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:Service>
  <dep:Name>service1.nsp-name1.MSGSNF.PROD</dep:Name>
  <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
  <dep:DestQueueName>NSPNAME1.MSGSNF.INCOMING.L01</dep:DestQueueName>
  <dep:Status>Activated</dep:Status>
  <dep:Reason/>
 </dep:Service>
 <dep:Service>
  <dep:Name>service1.nsp-name1.FILESNF.PROD</dep:Name>
  <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
  <dep:DestQueueName>NSPNAME1.FILESNF.INCOMING.L01</dep:DestQueueName>
  <dep:Status>Failed</dep:Status>
  <dep:Reason>Queue not accessible. MQRC=2035</dep:Reason>
 </dep:Service>
</dep:EnableSnfTrafficAck>
```

Detailed test procedure:	The ESMIG sends an "EnableSnfTraffic/DisableSnFTraffic" to the NSP. Inspect the message, then inspect the response to the message. Verify DisableSnfTraffic stop incoming store-and-forward traffic and EnableSnFTraffic restart it. Use the QuerySnFTraffic during the test to verify the correct status of the NSP.
Expected result:	The NSP manages the store-and-forward traffic as detailed in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Enable/Disable/Query incoming real-time traffic

Requirement ID	ESMIG.60470

The NSP must manage the real-time incoming "traffic" as detailed below.

ESMIG shall be able to enable/disable the exchanging of real-time traffic in order to avoid the reception of this kind of traffic during the "maintenance window" or for particular contingency reason.

When the ESMIG is ready to manage the real-time traffic it sends an "EnableRTTraffic" to the NSP's gateway. This is a "services" primitive and doesn't contain the "envelope" used for "business" message exchange. An example of this message is set out below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:EnableRTTraffic
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
        <dep:Service>
                <dep:Name>service1.nsp-name1.MSGRT.PROD</dep:Name>
                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                <dep:DestQueueName> NSPNAME1.MSGRT.INCOMING.L01</dep:DestQueueName>
        </dep:Service>
        <dep:Service>
                <dep:Name>service1.nsp-name1.FILERT.PROD</dep:Name>
                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                <dep:DestQueueName>NSPNAME1.FILERT.INCOMING.L01</dep:DestQueueName>
        </dep:Service>
</dep:EnableRTTraffic>
```

An example of the response of the NSP's gateway to this message is the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:EnableRTTrafficAck
 xmlns:dep="http://www.ecb.eu/dep-2.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.ecb.eu/dep-2.0 dep-20.xsd ">
 <dep:Service>
  <dep:Name>service1.nsp-name1.MSGRT.PROD</dep:Name>
  <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
  <dep:DestQueueName>NSPNAME1.MSGRT.INCOMING.L01</dep:DestQueueName>
  <dep:Status>Activated</dep:Status>
  <dep:Reason/>
 </dep:Service>
 <dep:Service>
  <dep:Name>service1.nsp-name1.FILERT.PROD</dep:Name>
  <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
  <dep:DestQueueName>NSPNAME1.FILERT.INCOMING.L01</dep:DestQueueName>
  <dep:Status>Failed</dep:Status>
  <dep:Reason>Queue not accessible. MQRC=2035</dep:Reason>
 </dep:Service>
</dep:EnableRTTrafficAck>
```

Detailed test procedure:	The ESMIG sends an "EnableRTTraffic/DisableRTTraffic" to the NSP. Inspect the message, then inspect the response to the message. Verify DisableRTTraffic stop incoming real-time traffic and EnableRTTraffic restart it. Use the QueryRTTraffic during the test to verify the NSP status.
Expected result:	The NSP manages the real-time traffic as detailed in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED

	If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Open/Close/Query traffic channel

Requirement ID	ESMIG.60480

The NSP must manage the traffic channel as detailed below.

In order to manage the Maintenance Window (MW), the following commands have to be managed by the NSP:

- CloseTrafficChannels, to inform NSP about the upcoming start of the MW
- OpenTrafficChannels, to inform NSP about the completion of the MW
- QueryTrafficChannels, to query the NSP about the status of the MW as known by the NSP

From the DEP perspective, the following primitives are defined:

- CloseTrafficChannels, sent by ESMIG to NSP's
- CloseTrafficChannelsAck, replied by the NSP's to ESMIG
- OpenTrafficChannels, sent by ESMIG to NSP's
- OpenTrafficChannelsAck, replied by the NSP's to ESMIG
- QueryTrafficChannels, sent by ESMIG to NSP's
- QueryTrafficChannelsAck, replied by the NSP's to ESMIG

Detailed test procedure:	The ESMIG sends an "OpenTrafficChannels/ CloseTrafficChannels" to the NSP. Inspect the message, then inspect the response to the message.

	Use the QueryTrafficChannels during the test to verify the correct status od the NSP.
Expected result:	The NSP manages the OpenTrafficChannels/CloseTrafficChannels/QueryTrafficChannel as detailed in the Technical Requirements.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Usage of CloseTrafficChannels

Requirement ID	ESMIG.60490

ESMIG uses the CloseTrafficChannels command to inform the NSP that the MW is going to start and therefore traffic connection should be stopped.

The normal behavioral pattern envisages ESMIG to:

- first disable all queues related to incoming traffic from Di.Co.A. (i.e. DisableSnfTraffic and DisableRTTraffic). This stops the incoming traffic only while outgoing traffic can still be sent.
- then notify the NSP DEP Gateway for the start of the MW (i.e. CloseTrafficChannels). This indicates that all traffic is stopped

When the NSP receives the CloseTrafficChannels command, the current status of the MW is checked and the CloseTrafficChannelsAck is sent back to the ESMIG.

In case the MW was not already running, an Ack with status CLOSING is returned (normal scenario).

Then, all remaining connections to WMQ queues related to traffic (i.e. all IN.FILE/MSG and OUT.FILE/MSG queues) are closed. Only the connections to the command queues (i.e. IN.CMD and OUT.CMD) remain active, so that NSP is able to get the OpenTrafficChannels or QueryTrafficChannels commands from the ESMIG. In case there is a need to stop also the queue manager (and therefore the command channels as well), the ESMIG Service Desk may inform the NSP, so that the NSP can stop their gateway through an operational command. The NSP may implement a delay in retrying to establish a new connection to the command channel after the CloseTrafficChannels command has been responded to. This delay is at least 60 seconds.

Detailed test procedure:	Send a CloseTrafficChannel from the ESMIG to the NSP and verify that only the connections to the command queues (i.e. IN.CMD and OUT.CMD) remain active.
Expected result:	The NSP is able to manage the CloseTrafficChannel.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Traffic management during MW

Requirement ID	ESMIG.60500

When the MW is started, all IN queues are disabled. Therefore:

- all in flight incoming RT traffic (waiting for Response from ESMIG), if any, is completed with a negative Response generated by the NSP with reason indicating that related ESMIG TechnicalServiceID is not available to receive traffic

- all new incoming RT traffic is immediately completed with a negative Response generated by the NSP with a reason indicating that related ESMIG TechnicalServiceID is not available to receive traffic

- SNF traffic is processed by the NSP but not forwarded to ESMIG, waiting for the EnableSnFTraffic command

With regard to the outgoing traffic sent from ESMIG:

- any Technical Ack related to outgoing traffic and currently being generated by the NSP is discarded and not sent to ESMIG.

Detailed test procedure:	Send messages and files from the Di.Co.A emulator during the MW and verify that the incoming traffic is completed by the NSP with a negative Response (real-time) or queued (store-and-forward).
Expected result:	The NSP is able to manage real-time and store-amd-forward traffic during the MW.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.3 A2A MEPT

MEPT Application to Application (A2A) mode

Requirement ID	ESMIG.60510

The NSP must support exchange of messages in A2A mode via "instant" transfer in "push" mode only. The NSP supports exchange of files in A2A mode via "store-and-forward" transfer in "push" mode only.

Detailed test procedure:	Part I: Send messages (A2A mode) via the "instant" transfer with "push" mode, also check that no other modes are allowed (ie. push only). Part II: Send files (A2A mode) via the "store-and-forward" transfer with "push" mode, also check that no other modes are allowed (ie. push only). Verify that all messages and files have been received.
Expected result:	The NSP exchange messages in the A2A mode via the "instant" transfer and "store-and-forward" file transfer in the "push" mode only.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____

	date ____/____/____ NSP testing team _____ date ____/____/____

MEPT A2A NSP Network Gateway High availability and resiliency

Requirement ID	ESMIG.60520

The NSP must provide the Network Gateways in high availability, to support the 24x7x365 requirement of the "instant" message exchange.

The NSP must support Network Gateways in active-active configuration in the same site and also over multiple sites.

Detailed test procedure:	Check the NSP Technical Solution to verify it is possible to achieve the required service level (desk check). Run some tests from a Di.Co.A. emulator: • Send continuously messages to the ESMIG for 24 hours and check that all messages are delivered to the receiver; • Send messages to the ESMIG during the week-end and check that they are always delivered to the receiver; • Check that it is possible to use all NSP's gateways.
Expected result:	The Network Gateways and network devices provided by the NSP are configured in high availability, active-active mode, and can operate 24x7x365.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____

	_____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

MEPT A2A NSP Load balancing

Requirement ID	ESMIG.60530

The NSP must provide load-balancing features, by supporting the traffic exchange over multiple MEPT Network Gateways, with no requirement for any specific application logic to be implemented in the ESMIG.

Detailed test procedure:	Send a bunch of messages from a test Di.Co.A. and check that all the Network Gateways are used for the delivery to the Platform. Verify that the NSP provides an effective way to check which gateway is sending each message. For example the Network Gateway ID which took care of the message is reported in the message itself.
Expected result:	The traffic is spread among all the available Network Gateways transparently to the ESMIG.

MEPT A2A message delivery approach

Requirement ID	ESMIG.60540

The NSP must deliver messages at most once. In case of error or doubt conditions, no retry mechanism are implemented to avoid any risk of message duplication.

Detailed test procedure:	Send a message from a test Di.Co.A., then check that the message is correctly delivered to the ESMIG. On the MQ Server simulate a communication error (either

	disabling the MQ PUT for the queues used for the incoming traffic or disabling the MQ at channel level), then send a message from a test Di.Co.A.. After a few minutes enable the MQ PUT on the queues and check that the message is not delivered to the ESMIG.
Expected result:	Messages are sent by the NSP to the ESMIG only once; no duplicates and no retry mechanism are carried out.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

MEPT A2A messages independency

Requirement ID	ESMIG.60550

The NSP must manage each "instant" message as an individual message, with no correlation between messages (for example, messages belonging to the same business transaction), thus allowing the message "completing" a business transaction to be delivered through a network access point different from the access point used to send the message initiating the business transaction.

Detailed test procedure:	Send from a Di.Co.A. (using the Di.Co.A. emulator) the same business message several times and verify that each one is

	handled independently, running through different gateways. Send from a Di.Co.A. (using the Di.Co.A.r emulator) several business transactions and verify that the messages belonging to the same transaction are handled by different Network Gateways, (e.g. by checking the Network Gateway ID put in the messages). [on field]
Expected result:	A2A messages can be routed through any of the available NSP network access points regardless the content of the message.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

NSP Network Gateway scalability

Requirement ID	ESMIG.60560

The NSP must support horizontal scalability of the Network Gateway, to enable the addition of Network Gateways in case an additional traffic load is required. The deployment of a new Network Gateway does not impact the availability of the service in the involved infrastructure.

Detailed test procedure:	Send bunches of messages from a Di.Co.A. (using the Di.Co.A. emulator) to the ESMIG while the NSP adds a new Network Gateways. Check that there is no impact to the service availability. For example the NSP could consider to initially deliver two Network Gateways, then – while these two Network Gateways are being used – deploy two additional Network Gateways and verify this horizontal scaling does not impact the service availability. After the deployment, verify the additional Network Gateways are actually in use. [on field]
Expected result:	New Network Gateways can be added to the infrastructure without any impact to the service availability.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

MEPT WMQ message structure

Requirement ID	ESMIG.60570

The NSP manages the exchange of message based on a WMQ message. A WMQ message is composed by a "Message Description" part (MQMD) and by a "Message Text" part. The WMQ message structure is described in the following.

Detailed test procedure:	Inspect the WMQ message and identify the two different parts a "Message Description" (MQMD) and a "Message Text" part. Verify the WMQ message structure is in line with the requirements.
Expected result:	The NSP manages the message based on a WMQ message. Message Descriptions and Message Text are correctly handled system wide.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message end-to-end information transport

Requirement ID	ESMIG.60580

The NSP allows the exchange of end-to-end information from the sender application to the receiver application together with the “instant” message (i.e. from the Di.Co.A. to the ESMIG and vice versa).

Detailed test procedure:	Generate a set of “instant” messages (i.e. "SendRequest"

	primitive requests), from a test Di.Co.A. emulator to the ESMIG and vice versa. Inspect the generated messages and check the exchange of end-to-end information from the sender application to the receiver application through with the “instant” message.
Expected result:	The NSP is able to exchange end-to-end information from the sender application to the receiver application together with the “instant” message.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message unique identification

Requirement ID	ESMIG.60590

The NSP must identify each exchanged “instant” message with a universally unique "network" message identifier. The unique "network" message identifier of every exchanged message is provided to the receiver, together with the "instant" message, for diagnose and non-repudiation purposes. The unique "network" message identifier is also notified to the sender, if needed.

Detailed test procedure:	Generate a set of "SendRequest" primitive requests, from a test Di.Co.A. emulator to the ESMIG. Inspect the generated messages. Verify that a unique "network" message identifier

	is provided to the receiver, together with the "instant" message. Verify that a unique "network" message identifier is provided to the sender through Technical ACK and/or Notify primitives, whenever applicable.
Expected result:	The unique "network" message identifier of every exchanged message is provided to the receiver, together with the "instant" message, for diagnose and non-repudiation purposes. Every “instant” message has a unique "network" message identifier.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Gateway control application

Requirement ID	ESMIG.60600

The NSP must provide a control application, running on ESMIG RHEL server, in order to manage the NSP gateways via a GUI interface. Such control will allow:

- To start and stop a gateway (optional feature);

- To disable/enable a gateway from processing traffic (optionally, with the possibility to disable/enable outgoing traffic towards Di.Co.A. and incoming traffic arriving from Di.Co.A.);
- To login/logout of a gateway to/from the network;
- To display the gateway status and to monitor traffic;
- To renew the LAU symmetric key between the ESMIG application and all the gateways;
- To display information about the LAU symmetric key (last renewal time, time left before next renewal, adoption time of last key on each gateway).

Detailed test procedure:	Check the documentation provided by the NSP describing the interface, assess the usability and eventually approve it (desk check). Through the "Gateway control application" instruct control operations toward the NSP gateway (for example start/stop the gateway, renew the LAU symmetric keys, display gateway status, etc.), and verify that the outcome is the expected one.
Expected result:	NSP provides a description of the "easy-to-use" interface, approved by the ESMIG Operator. NSP provides the "Gateway control application".
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

TIPS A2A traffic primitives management

Requirement ID	ESMIG.60610

The NSP must manage the following primitives to exchange messages with the ESMIG:

- *SendRequest*: the ESMIG uses this primitive to send a message to the Di.Co.A.;
- *Notify*: the NSP's Network Gateway uses this primitive to notify a positive/negative outcome of the initial processing of a SendRequest or FileSend operation to the ESMIG;
- *ReceiveIndication*: the NSP's Network Gateway uses this primitive to deliver a message sent from the Di.Co.A. to the ESMIG;
- *Technical Ack*: the NSP's Network Gateway uses this primitive to notify a positive/negative completion of the exchange;
- *FileSend*: the ESMIG uses this primitive to send a file to the Di.Co.A..

Detailed test procedure:	Generate a set of "SendRequest" primitive requests, from a test Di.Co.A. to the ESMIG and vice versa, varying different header properties (for example: notification option, technical ack option, message type, ...). Generate a set of "FileSend" primitive requests, from the ESMIG to a test Di.Co.A., varying different header properties (for example: notification option, FileName, ...). Verify that the related notifications and technical ACKs are correctly generated, when expected. Verify that the NSP correctly delivers the message/file to the specified part, with the correct primitive type, or that a delivery error is generated when expected. Verify that the header properties of the received messages are the expected ones, according to the MEPT specifications.
Expected result:	The NSP manages the primitives to exchange messages in line with the ESMIG.
Outcome:	Please describe the test result: [] PASSED

	[] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.3.1 A2A Instant Messaging

For the A2A instant messaging mode, the ESMIG communicates with Di.Co.A. only using “stateless” messages and it does not support "store-and-forward". This implies that if the receiver is unavailable no retry mechanism is in place.

The communication is in "push" mode, both from the ESMIG to the Di.Co.A. and from the Di.Co.A. to the ESMIG. The expression "push mode” refers to when the originator of a message is pushing it to the final receiver.

The A2A message exchange between ESMIG and the NSP is based on a set of rules named MEPT and described hereafter. The MEPT relies on XML messages, transported over an MQ connection and containing all the relevant information to address and describe messages. The NSP gateways physically hosted in ESMIG datacentres are in charge of the connection between the NSP and the ESMIG.

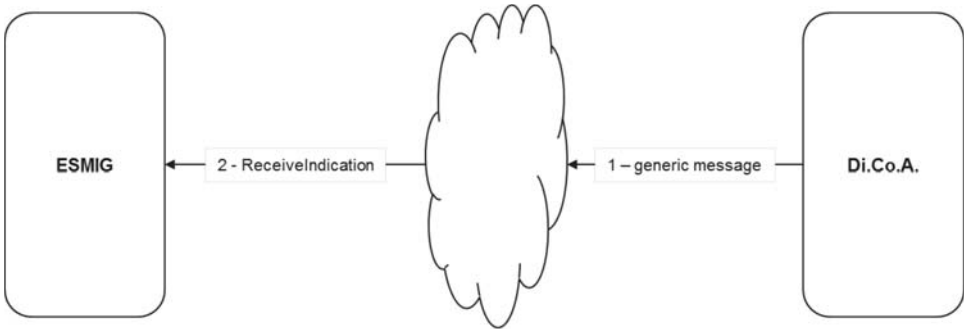
Each NSP offers connectivity services and manages the bi-directional data exchange between his Di.Co.A. and the ESMIG according to the MEPT.

The NSP provides several functionalities: Technical Sender Authentication, CGU, non-repudiation, encryption, NSP protocol transformation to and from MEPT messages.

A2A Instant Messaging - Incoming flow management

Requirement ID	ESMIG.60620

The NSP must manage the instant incoming message pattern as detailed in the following picture:



When the ESMIG receives a message from the NSP's Network Gateway it will go through the following steps:

1) The Di.Co.A. sends the message to the NSP Gateway;
2) The Network Gateway of the ESMIG receives the message from the sender (Di.Co.A.) and performs the validation of the received signature. If the validation process is successful, the Network Gateway running on ESMIG site sends a ReceiveIndication primitive to the ESMIG. The ESMIG receives the message and performs the validation check of the "Local Security" header.

   The message is then passed on to the application.

The primitive used for the incoming message processing is:

A ***ReceiveIndication*** primitive, used whenever a message is delivered from the NSP to the ESMIG. This type of message provides all the information which describes the message itself (such as sender, receiver, signature, etc.) and the transported business message.

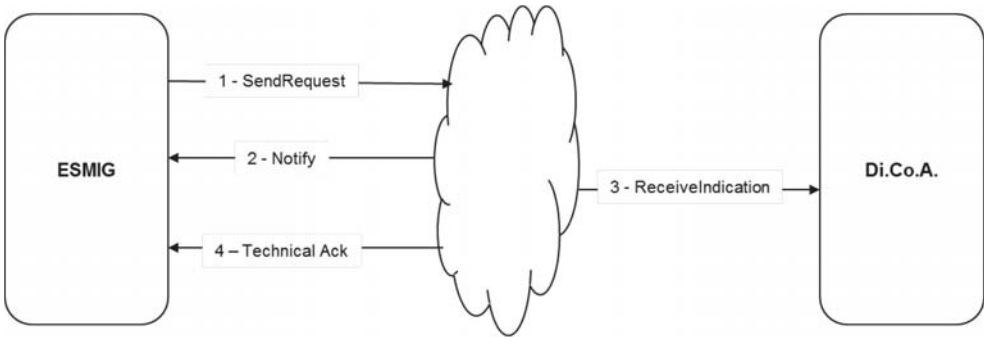
Detailed test procedure:	Part 1: The Di.Co.A. (emulated with the Di.Co.A. Emulator) sends the message to the NSP gateway. The NSP gateway receives and validates the messages. In case of successful validation of the message the NSP gateway sends a ReceiveIndication primitives to the platform. Part 2: Repeat the test with message failing the validation and verify that the NSP gateway send back an error and stops sending .

Expected result:	Verify that the format of ReceiveIndication received at the platform is the expected one (Part 1) and the expected behaviour of NSP gateway(Part 2)
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Instant Messaging - Outgoing flow management

Requirement ID	ESMIG.60630

The NSP must manage the instant outgoing message pattern as detailed in the following picture:



When the ESMIG needs to send a message to a Di.Co.A. it will go through the following steps:

1) The ESMIG sends a “SendRequest” primitive to its Network Gateway
2) The Network Gateway of the ESMIG receives the message and performs the validation check of the "Local Security" header. If the validation process is successful, a unique network message identifier is generated and the message is signed.

   If there is an error, the Network Gateway of the ESMIG sends a negative Notify back to the ESMIG and the flow is completed. If the processing is successful, the Network Gateway of the ESMIG sends the message to the Di.Co.A.. If the sending to the Di.Co.A. is successful, the Network Gateway of the ESMIG sends a positive Notify back to the ESMIG.
3) The Di.Co.A. receives the message from the Network Gateway of the ESMIG and performs the validation of the received signature.
4) The Network Gateway of the sender (ESMIG) receives the outcome of the processing and sends back a positive/negative Technical Ack to the ESMIG depending on:
   - a failure in the validation, performed on the Di.Co.A. side, on the received message
   - the outcome (positive or negative) of the delivery of the message to the Di.Co.A.

The primitives used for the outgoing message processing are:

A ***SendRequest*** primitive, activated by ESMIG when a message has to be delivered to a Di.Co.A.. This type of message provides the NSP with all the information which describes the message itself (such as sender, receiver, etc.) and the business message to be transported.

A ***Notify*** primitive is provided for each request to send a message or a file between the ESMIG and the NSP Network Gateway in order to notify the outcome of the initial processing performed by the Network Gateway: local security check, addressing resolution, header validation etc. If the result is negative, a reason code for the detected error is returned. If the result is positive, the unique "network" message / file identifier and the signature of the message are sent back.

A ***Technical Ack*** primitive is provided for each request to send a message between the ESMIG and the NSP Network Gateway in order to notify the completion of the exchange. If the result is negative, a reason code for the detected error is returned. If

the result is positive, the unique "network" message / file identifier, a timestamp of the delivery of the message / file to the Di.Co.A. are sent back.

Additionally, for the outbound file transfer, the primitive used in the ESMIG - NSP communication is called ***FileSend*** (further elaborated in a subsequent chapter of this document) and its purpose is to convey the information about the delivery of the file (e.g. the receiver) and not the file itself.

Detailed test procedure:	Generate a set of "SendRequest" primitives from the ESMIG to test both positive and negative cases. Part 1 Send a "SendRequest" from the Platform. The NSP Network Gateway (i) validates the message, (ii) sends back a Notify, (iii) forwards the message to the intended receiver and, (iv) sends back a Technical Ack to the ESMIG. Part 2 Send a faulty "SendRequest" (e.g. with a missing mandatory field or a wrong signature). The message is discarded by the NSP Network Gateway and a negative Notify is returned to the ESMIG. Part 3 Send a "SendRequest" to a receiver that has a local issue (for example it is not connected to the network in that moment). The NSP Network Gateway sends a Notify to the ESMIG and then a negative Technical Ack upon the failed delivery.
Expected result:	Verify that the exchange of the communication primitives (SendRequest, Notify, Technical Ack) correctly happens according to the MEPT protocol.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Instant Messaging – Message size

Requirement ID	ESMIG.60640

The NSP must support the exchange of messages which have a maximum length of 10KB (1 KB = 1.024 bytes). The maximum length refers to the business content of the transferred message, without taking into account the communication protocol overheads.

The NSP shall reject as soon as possible any message that is not compliant with the allowed size range.

The NSP shall reject the operation by sending a negative acknowledgement message back to the originator with the explanation of the error (e.g. "Message size out of allowed range.").

Detailed test procedure:	Part 1 Send from a Di.Co.A. emulator and from the ESMIG an Instant Message with size less than 10KB. In both cases the message is accepted by the NSP. Repeat the test with a message of size equal to 10KB. Part 2 Send from a Di.Co.A. emulator and from the ESMIG an Instant Message with size greater than 10KB. The message is discarded by the NSP Network Gateway and an error message is returned to the sender.

Expected result:	Verify that the NSP Network Gateways does not accept oversized messages.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A File store-and-forward

Requirement ID	ESMIG.60650

The file transfer operates in store-and-forward mode and, as such, enables a sender to transmit files even when a receiver is unavailable. If the receiver is temporarily unavailable, the NSP stores the files for 14 calendar days (for PROD environment) and delivers them as soon as the receiver becomes available again.

The maximum size is 1 GB.

File transfer mode is used by the ESMIG only for outgoing exchange, there is no business case that involves the use of such mode for communications from Di.Co.A. to the ESMIG.

When a file has to be sent, as a first step, ESMIG stores it on an dedicated RHEL server (located in the SSP ESMIG perimeter). Then the file transmission starts from ESMIG by sending an MQ message to the Gateway using the same rules (MEPT) described ahead and specifying the primitive name *FileSend*. The message contains the file name and the file system path to be used to get the file. The NSP Gateway, then, has the responsibility to get the file that has been stored beforehand by ESMIG and to send it to the recipient.

The notify primitive is used to indicate to ESMIG that the NSP Gateway has read the file and taken the responsibility to send the file. This allows ESMIG to remove the file.

Detailed test procedure:	ESMIG sends a file to the Di.Co.A. emulator (using the MEPT protocol), while the Di.Co.A. emulator is online. The file is correctly delivered and received by the Di.Co.A. emulator. ESMIG sends a file to the Di.Co.A. emulator, while the Di.Co.A. emulator is offline. After 60 minutes the Di.Co.A. emulator returns online and the file is correctly delivered, without any ESMIG involvement. Both files are expected to be correctly received.
Expected result:	The NSP store-and-forward file transfer interacts with ESMIG following the ruleset.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.3.2 Messaging rules – MEPT (Message Exchange Processing for TIPS)

A generic MEPT message is composed by two main sections:

- The **message header**: this section contains all the information that enriches the message but is not strictly related to the message content (routing, signature, etc..)

- the **message payload**: this section contains the ISO business message or the payload of the specific MEPT message such as *TechnicalAck* or *Notification*

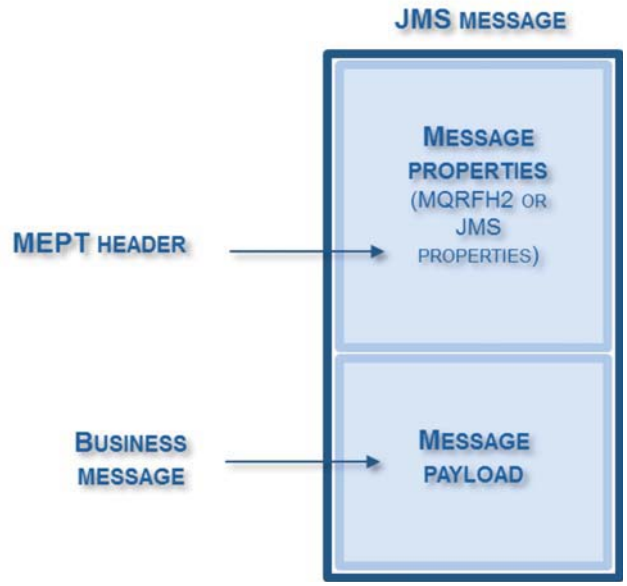


FIGURE 1 – SECTIONS OF A MESSAGE

A2A Message header

Requirement ID	ESMIG.60660

The message header completes a message with a set of information strictly related to the message's lifecycle; IBM WMQ is the target technology for message exchange, the message header is composed by the JMS properties listed in the following table. A message refers to a primitive and all the properties are used or not depending on the primitive. The following table shows which primitive uses each property. The table shows also which property is used in HMAC calculation and which property is stored by ESMIG for "non-repudiation of origin" purposes.

Property	**Description**	**Where it is used**	**Used in HMAC calcula-tion**	**Stored for NRO**
HMAC	Hash Message Authentication Code for Local AUtentication between ESMIG and NSP gateway	In all types of message	No	No

HMACKeyId	Identifier of the bilateral key to be used for HMAC check	In all types of message	No	No
HMAC2	Second (optional) HMAC for Local AUthentication, to be used when the NSP needs to protect the communication beyond the link between ESMIG and the NSP gateway. ESMIG adds HMAC2 only when all the following conditions are met: - The message is a *SendRequest* - *SignatureRequired* = yes - The gateway control application already sent to ESMIG the values for the HMAC2 Key and HMAC2 KeyId	SendRequest	No	No
HMAC2KeyId	Identifier of the bilateral key to be used for (optional) HMAC2 check	SendRequest	No	No
MsgSignature	Message signature (maximum length 3000 bytes)	*ReceiveIndication,* *Notify*	No	No
ProtocolVersion	The MEPT version	In all types of message	Yes	No
Service	The service name (e.g. PRODUCTION, TEST)	In all types of message	Yes	Yes
Sender	The distinguished name of the actor sending the message. For *Notify* and *TechnicalAck* it refers to the original message	In all types of message	Yes	Yes
Receiver	The distinguished name of the actor receiving the message. For *Notify* and *Technical Ack* it refers to the original message	In all types of message	Yes	Yes
PrimitiveType	*SendRequest, ReceiveIndication, Notify, TechnicalAck, FileSend*	In all types of message	Yes	No
MsgType	The ISO message type	*ReceiveIndication,*	Yes	No

		SendRequest *FileSend*		
SendTimestamp	Timestamp from when the message has been retrieved from the sender's gateway (start of the NSP perimeter). It is exposed as YYYY-MM-DDTHH:MM:SS.SSSZ, where **T** is the delimiter between date and time and **Z** is a zone designator for the zero UTC offset. For *Notify* and *TechnicalAck* it refers to the original *SendRequest*	*ReceiveIndication,* *Notify,* *TechnicalAck*	Yes	Yes
ReceiveTimestamp	Timestamp from when the message has been put on the receiver's queue (end of NSP perimeter). It is exposed as YYYY-MM-DDTHH:MM:SS.SSSZ, where **T** is the delimiter between date and time and **Z** is a zone designator for the zero UTC offset. For *TechnicalAck* it refers to the original *SendRequest*	*ReceiveIndication,* *TechnicalAck*	Yes	No
MsgBizIdentifier	Unique business identifier assigned by the sender. For business messages it is a copy of the message identifier transported in the payload. For *Notify* and *TechnicalAck* it refers to the original *SendRequest message*	In all types of message	Yes	No
MsgNetworkIdentifier	Unique message identifier assigned by the NSP. For *Notify* and *TechnicalAck* it refers to the original *SendRequest message*	*ReceiveIndication,* *Notify,* *TechnicalAck*	Yes	Yes
FileName	Full path to the file to be sent to the receiver	*FileSend*	Yes	No
FileDigest	Digest of the file used in HMAC	*FileSend*	Yes	No
PDMFlag	Possible duplicate message flag	*SendRequest,* *ReceiveIndication* *FileSend*	Yes	No

SignatureRequired	Flag asking to add the signature to the message	*SendRequest*	Yes	No
NotificationRequired	Requires a *Notify*. “A” ⇔ always, “N” ⇔ “Never”, “E” ⇔ only in case of errors	*SendRequest,* *FileSend*	Yes	No
TechnicalAckRequired	Requires a *TechnicalAck*. “A” ⇔ always, “N” ⇔ “Never”, “E” ⇔ only in case of errors	*SendRequest* *FileSend*	Yes	No
SignatureAddInfo	Additional information included in the signature calculation (optional). This information are is only stored by the ESMIG for NRO purposes (maximum length 400 bytes)	*ReceiveIndicati on* *FileSend*	Yes	Yes
CompressionAlgo	Algrorithm used for compression of the message payload if used	*FileSend*	Yes	No
PrimitiveReturnCode	Return code of the ESMIG primitive The return codes are: OK (if successful) KO (in case of failures)	*TechnicalAck,* *Notify*	Yes	No
PrimitiveReasonCode	Reason code of the TIPS primitive The following list of reason codes is not exhaustive and some others can be added by the NSPs: TIPS.UnknownHMACKeyId TIPS.UnknownHMAC2KeyId TIPS.InvalidHMAC TIPS.MissingProperty.<Property> TIPS.InvalidProperty.<Property> TIPS.FailedDelivery TIPS.FileNotFound NSP errors are prefixed by the NSP id and agreed with ESMIG platform.	*TechnicalAck,* *Notify*	Yes	No

From a technical point of view, note that for IBM MQ all the properties will be inserted into the RFH2 part of the message.

Detailed test procedure:	Part 1 Generate a "SendRequest" from a Di.Co.A. Emulator towards the ESMIG and viceversa. Generate a "FileSend" from the ESMIG towards a Di.Co.A. Emulator. Inspect the WMQ Message Description block for all the primitives exchanged between the ESMIG and the NSP Network Gateway. All the required fields must be present. Part 2 Send some "SendRequest" and "FileSend" primitives from the ESMIG to the NSP Network Gateway by removing some mandatory fields. The Gateway must discard the messages.
Expected result:	Verify that all the required fields are present in all the primitives exchanged between the ESMIG and the NSP Network Gateway.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

HMAC check strings

Requirement ID	ESMIG.60670

All messages are subject to **Local AUtentication (LAU)** via a message authentication code computed with a symmetric key (HMAC).

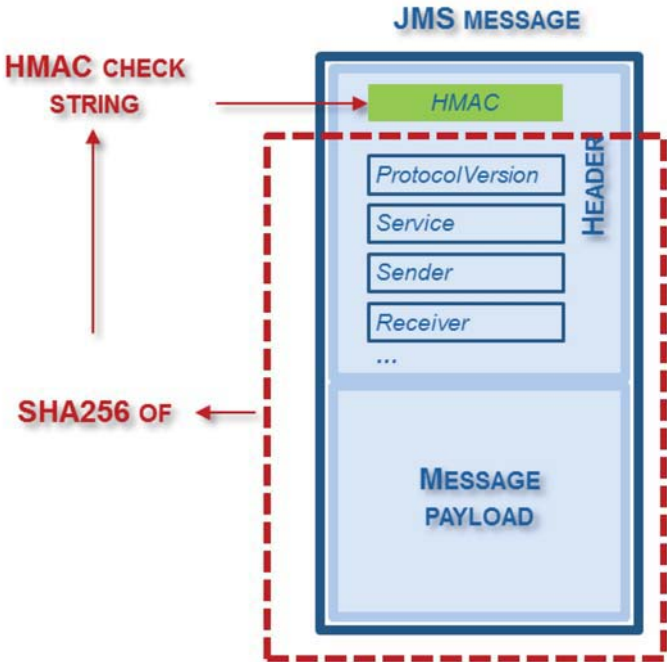


Figure 2 – Calculation of HMAC for Local AUthentication

The HMAC code is calculated using the header properties listed as specified in the last column of the table from the previous paragraph plus the full payload (plus the HMAC symmetric key as required by the HMAC technique).

The values of the properties shall be concatenated with no names or delimiters in the order of the list above, using the actual values and suppressing all trailing blanks.

The HMAC2 code is optional, it is calculated and added to the header only when the ESMIG is sending a message (*SendRequest* primitive) that must be signed by the NSP gateway (*SignatureRequired* = yes). Additionally, the NSP gateway control application must have communicated in advance to the ESMIG this additional key and its Key Id.

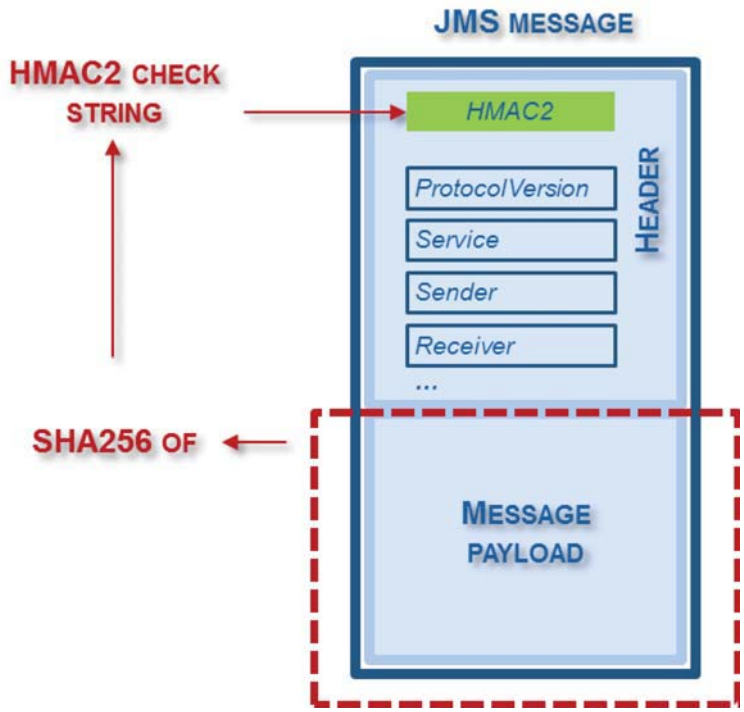


Figure 3 – Calculation of HMAC2

The HMAC2 code is calculated using only the message payload (with no header information).

The assignment and renewal of the symmetric keys is described in the paragraph dedicated to LAU. The hash function used for the HMAC calculation is SHA256. The HMAC code is computed by ESMIG when sending a message and passed to the NSP gateway in the HMAC and HMAC2 fields of the message header. The NSP is responsible for checking these hashes in order to ensure that they refer to the transported message and to the two most recent symmetric keys previously exchanged (in order to smoothly manage the renewal of the symmetric key).

For incoming messages, the gateway is responsible for computing and adding the HMAC field while ESMIG checks the hash to ensure that it refers to the transported message payload and to one of the two most recent symmetric keys previously exchanged.

The HMAC an HMAC2 fields are encoded as a base64 value.

Detailed test procedure:	Part I: A new session is opened from a Di.Co.A. with no LAU or a wrong LAU and verify the NSP's Network Gateway rejects the session.

	Part II: A new session is opened from a Di.Co.A. with the correct LAU and verify the NSP's Network Gateway accepts the session. Part III: When a message is exchanged, the NSP is in charge of verifying the integrity of the message by checking the HMAC(s) field(s). Depending on the direction of the flow, HMAC(s) are either generated from the NSP itself or from the Di.Co.A. or from the ESMIG. During the tests the teams will first inspect the message header and verify the HMAC(s) field(s) is(are) there; then the originator of the message will manipulate either the message or the HMAC(s) field(s) to ensure the NSP is rejecting the manipulated content.
Expected result:	Every time a new session is opened the NSP authenticates both the Di.Co.A. and the ESMIG (through the A2A NSP's Network Gateway). The NSP has set up an appropriate measure, for example HMAC based (with a periodical keys renewal). NSP successfully completes the message partners authentication, for example using a Local AUthentication key (LAU).
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____

	date ____/____/____

Gateway-backend channel security (LAU)

Requirement ID	ESMIG.60680

The Local authentication between ESMIG and the NSP gateways provides both message integrity and authentication. Optionally, the communication beyond the NSP gateway can be protected by a further HMAC code (HMAC2).

HMAC must be calculated and provided to the other side. The calculation of the HMAC starts from the message payload, part of the header and the symmetric keys stored on both sides.

HMAC2, when used, must be calculated and provided from the ESMIG to the NSP. The calculation of the HMAC2 starts from the message payload and the dedicated symmetric keys stored on both sides.

The receiver repeats the calculation using the key that they own and checks that the HMAC provided in the header is equal to the value just calculated.

The symmetric keys specifically identified within the message header must be used for HMAC/HMAC2 verification. During the asynchronous renewal of a key both the Gateway and the application will update the Key-Id to store the reference of the currently valid symmetric key.

Calculation and renewal of the symmetric key(s) is done by the **gateway control application** and the communication to TIPS and to the gateway must use a secure technique to protect the key exchange and to prevent its disclosure.

The length of the symmetric key must be minimum 160 bits.

The key renewal process starts with the calculation of an integer value for the key and assigning to this key a Key-Id; this is done by the gateway control application. Then the process invokes synchronously a specific ESMIG component (Java method invocation) to pass the values for the key and Key-Id. Finally, the Gateway and the application start using the new key by using the new Key-Id on each message sent to the counterparty.

The steps to be executed for the key renewal process are summarized in the following list:

1. The gateway control application triggers the key renewal functions
2. The gateway control application calculates the new key and assigns to it a new Key-Id

3. The gateway control application communicates the new key and its id to the gateway(s) in a secure way; The NSP gateway stores the new key internally but it doesn't start using it yet
4. The gateway control application provides the ESMIG with the new key and the id
5. From this moment (just after the ESMIG has been successfully invoked) the NSP gateway and ESMIG can use the new key when sending message. The old key is still valid and it can be used when sending messages and it must be considered as valid when receiving messages.

Detailed test procedure:	Part I: Perform the key renewal using the GCA. A new session is opened from ESMIG with the old LAU (key1) and verify the NSP's Network Gateway accepts the session. A new session is opened from ESMIG with the new LAU (key2) and verify the NSP's Network Gateway accepts the session. Part II: Perform again the key renewal using the GCA (generate key3, overwriting key1). A new session is opened from ESMIG with the old LAU (key1) and verify the NSP's Network Gateway rejects the session. New sessions are opened from ESMIG with the old LAUs key2 and the new LAU key3 and verify the NSP's Network Gateway accepts both the sessions.
Expected result:	Verify that NSP has setup an effective procedure for LAU key renewal.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

TIPS Signature

Requirement ID	ESMIG.60690

A signature is expected on all incoming business messages to ESMIG and in some outgoing messages sent by ESMIG.

The following figure shows which are the signed messages for an SCT-Inst payment[3]:

a. Signature by the Originator Di.Co.A. is necessary for the input pacs.008 (number 2 below) for payment orders sent to TIPS;

b. Signature by TIPS is necessary for the output pacs.008 (number 3 below) – message forwarded to the beneficiary Di.Co.A.;

c. Signature by the Beneficiary Di.Co.A. is necessary for the input authorization of the Beneficiary Di.Co.A. for pacs.002 (number 4 below);

d. No signature is necessary on confirmation messages sent by ESMIG (pacs.002 number 5 and 7) to the originator Di.Co.A. and beneficiary Di.Co.A. as final confirmation.

[3] In any case, as far as MEPT is concerned, the decision to sign a message sent by the ESMIG is instructed by the SignatureRequired field in the header.

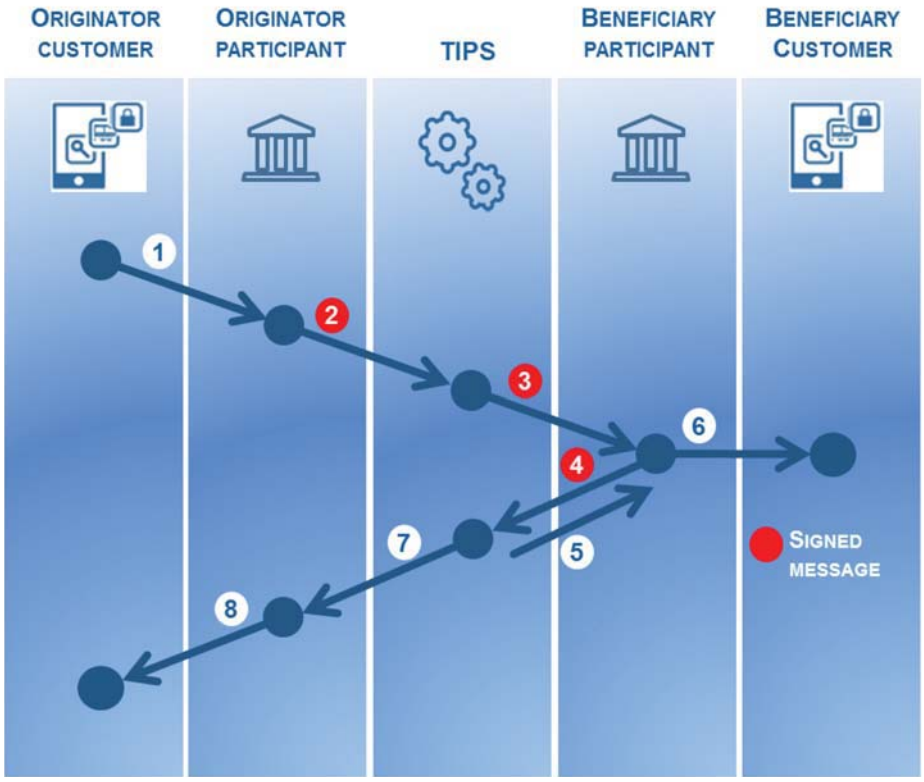


Figure 4 – Signatures

The message payload and, optionally, some of the header properties are signed and the signature is included in the message header.

The header properties that the NSP can use when it calculates the signature are the ones that the ESMIG stores for Non-Repudiation of Origin (NRO), specified in the header description (cfr 3.1). The NSP can include these values into the signature calculation or it can use only some of them or it can decide to sign only the payload; in any case the ESMIG stores all these signature-eligible properties in order to be allow the NSP to perform, on demand, a re-calculation of the signature.

If the NSP signature requires additional fields not included in the header, the NSP can provide the needed values to ESMIG using the SignatureAddInfo header property; this optional field is stored by ESMIG for NRO purposes.

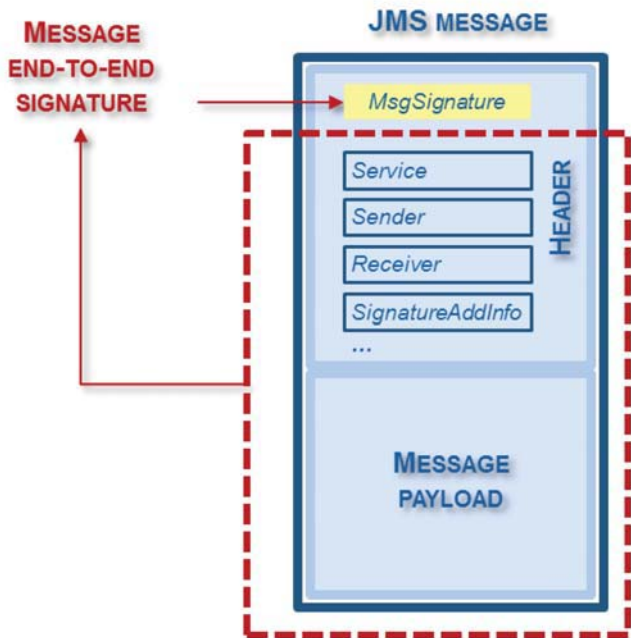


Figure 5 – Message signature

In outgoing communication, the signature is added by the NSP gateway on behalf of ESMIG, using ESMIG' private key.

In incoming communication, the signature has to be added by the NSP gateway on behalf of Di.Co.A. using a NSP certificate and its validity is checked by the NSP gateway on behalf of ESMIG.

The NSP will put in place all the necessary activities related to the digital signature, e.g. signing, verification of signature, checks against directory services (such as CRL and/or CSL).

The certificates used are issued by the NSP PKI for both outgoing and incoming cases and belong to a specific certificate class with a strong level of authentication and non-repudiation. The validity period of these certificates is 24 months.

Detailed test procedure:	Part 1 Send an Instant Message from a Di.Co.A. to the ESMIG. The signature is added by the NSP Gateway on behalf of Di.Co.A. using a NSP certificate and its validity (including CRL check) is checked by the NSP gateway on behalf of ESMIG. Part 2 Send an Instant Message from the ESMIG to a Di.Co.A.. The signature is added by the NSP gateway on behalf of ESMIG, using ESMIG' private key.

Expected result:	Verify that the signature is correctly inserted on the message header on both cases.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message payload

Requirement ID	ESMIG.60700

The message payload transported by the MQ message contains information that depends on the MEPT primitive the message refers to. The following table specifies the information transported by the message payload.
If the primitive refers to a business message (ISO message), no further information shall be included in such a payload other than the business message itself.

TIPS primitive	**Payload content**
SendRequest	The ISO message to be sent by TIPS, e.g. pacs.008, pacs.002.
ReceiveIndication	The ISO message received from TIPS, e.g. pacs.008, pacs.002.
TechnicalAck	Empty payload. Other relevant information for *TechnicalAck* are stored in the header (e.g. message identifiers, PrimitiveReasonCode)
Notify	Empty payload. Other relevant information for *Notify* are stored in the

	header (e.g. MsgSignature, message identifiers, PrimitiveReasonCode)
FileSend	Empty payload

Detailed test procedure:	Analyze one message for each primitive type
Expected result:	Check that the payload format is the expected one for each primitive
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

MQMD descriptor usage

Requirement ID	ESMIG.60710

The following table shows fields used in the MQMD:

MQMD field	**SendRequest/ ReceiveIndication/FileSend**	**Notify/Technical Ack**
MQMD.MsgType	DATAGRAM	REPORT
MQMD.Format	MQFMT_RF_HEADER_2	MQFMT_NONE
MQMD.MsgId	Present Used as CorrelId for Notify	Present

MQMD field	SendRequest/ ReceiveIndication/FileSend	Notify/Technical Ack
MQMD.CorrelId	Absent	Equal to MQMD.MsgId of the message it corresponds to (only for Notify)
MQMD.ReportOption	0	MQRO_PAN for positive Notify/TechnicalAck MQRO_NAN for negative Notify/TechnicalAck
MQMD.Feedback	MQFB_NONE	0 for MQRO_PAN 1000 for MQRO_NAN 2000 for MQRO_NAN when garbage was received
MQMD.CodedCharSetID	1208 (UTF-8)	1208 (UTF-8)
MQMD.Expiry	MQEI_UNLIMITED	MQEI_UNLIMITED at the beginning. It will be possible to set the property by assigning a value that will prevent the TIPS Platform from being overwhelmed by "old" messages that will be timed out.
MQMD.ApplIdentityData	Not used – ignored	Not used -ignored
MQMD.Encoding	MQENC_NATIVE	MQENC_NATIVE
MQMD.ReplyToQ	Empty	Empty
MQMD.ReplyToQMgr	Empty	Empty
MQMD.AccountingToken	MQACT_NONE	MQACT_NONE
MQMD.Persistence	MQPER_NOT_PERSISTENT	MQPER_NOT_PERSISTENT

The MQMD.CorrelId will be used only if it is not possible to generate a Notify or Technical Ack that contains the RFH2 field MsgBizIdentifier to be used for reconciliation of the Notify or Technical Ack.

In this case the only way to reconcile is to use the MQMD.CorrelId. If this is the case, then the value of the MQMD.Feedback property will be 2000.

The fields in the RFH2 for such Notify or Technical Ack would not include any unknown fields but would indicate what fields are filtered out in the ReasonCode.

Detailed test procedure:	Part I For each primitive type received by the platform analyse the MQMD format directly on the WMQ server Part II Put directly in WMQ queue (with mqm samp utility) a wrongly formatted message to generate the Corrid scenario
Expected result:	Verify the MQMD content on both cases
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

MQ queues, MQ channels and affinity

Requirement ID	ESMIG.60720

There is a set of queues containing SendRequest, a set of queues containing ReceiveIndication, a set of queues containing SendFile and a set of queues containing Notify and TechnicalAck.
It is possible to configure the same queue used for ReceiveIndication to be used for Notify and TechnicalAck.

The set of queues can be over multiple Queue Managers running on different hosts. Each NSP gateway will establish MQI connections to each of the Queue Managers.

There is no affinity between SendRequest queues and queues containing Notify and TechnicalAck. It is possible that a Notify is put on a queue of a different Queue Manager than the Queue Manager of the queue from which the request was taken.

The Queue Manager is dedicated for a given Service.

Detailed test procedure:	Send from the ESMIG a set of SendRequest
Expected result:	Verify that the various Notify and Technical Ack are not necessarily put on the same WMQ instance and queue where the related SendRequest was sent.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.4 U2A

User to Application (U2A) mode

Requirement ID	ESMIG.60730

The NSP must support the U2A connectivity enabling HTTPs traffic between the Di.Co.A. and the ESMIG.

Detailed test procedure:	Open an U2A HTTPs session from the Di.Co.A. to the ESMIG (via the NSP). Verify that the connection is successfully established (for example using the "netstat –a" on the https server). Verify that is not possible to establish a connection in plain HTTP.
Expected result:	The NSP supports the U2A mode interactions through the web access using HTTPs protocol to the ESMIG Platform.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

U2A user authentication

Requirement ID	ESMIG.60740

The NSP must distribute to the end users the credential to access the web interface of the ESMIG. The NSP must deliver the certificates for the U2A access to the end users.

U2A authentication message flow is as follow:

- the NSP performs a check whether the end user is authorised to access the requested URL: the check will be based on the "closed group of users";
- if the check is successful, the end user is able to establish an HTTPs session with the ESMIG;
- the ESMIG will perform the identification and authentication of the end user based on client certificate provided in the HTTPs request;
- the ESMIG checks NSP's PKI for certificate validation (CRL, CSL);
- the ESMIG sends an acknowledgement via HTTPs session.

Detailed test procedure:	Verify that the ESMIG Services Operator and a Di.Co.A. cooperating in the test (if available) has received valid credential - from the NSP - in form of a smart-card / USB token / remote HSM and the certificates stored in such device are valid for the authentication respectively against the ESMIG Services U2A interface.
Expected result:	The NSP produced and distributed to the end users the credential, stored in a smart-card, USB token or remote HSM, to access the U2A interface of the ESMIG.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____

	NSP testing team _____ date ____/____/____

U2A closed group of user authorisation

Requirement ID	ESMIG.60750

The NSP must check the authorisation of the end users to access the ESMIG. The end user is requested to open a VPN connection (performing identification and authentication) with the NSP in order to be able to establish a HTTPs session with the ESMIG.

Detailed test procedure:	1. Check that the end user connection to the ESMIG can be established via HTTPs by using an authentication token whose certificate belongs to the ESMIG U2A CGU; the connection must be successful. 2. Try to open an HTTPs tunnel with a certificate not belonging to the CGU; the connection must fail.
Expected result:	The end user is able to establish a HTTPs session with the ESMIG Platform only after the VPN connection with the NSP is established and only if the U2A certificate is part of the relevant CGU.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____

	date ____/____/____ NSP testing team _____ date ____/____/____

U2A Alternative access

Requirement ID	ESMIG.60760

The NSP must provide U2A alternative access to Di.Co.A.; thus each Di.Co.A. might have an U2A access in addition to the A2A and U2A solution described in ESMIG.60010. The two solutions must be provided by different NSPs.

The NSPs guarantees a service level in line with ESMIG.30340

Detailed test procedure:	The NSP offers to the Di.Co.A a connectivity package with only the U2A to be used for alternative access. [desk check]
Expected result:	The NSP is able to provide U2A alternative Access.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Low volume U2A access

Requirement ID	ESMIG.60770

The NSP must provide, in U2A mode only, a cost-effective access for low volume Di.Co.A.. The NSPs must guarantee ease of access for U2A low volume mode as well as the service level described in ESMIG.30340

Detailed test procedure:	The NSP offers to the Di.Co.A a connectivity package with only the U2A to be used for low volume Di.Co.A.. [desk check]
Expected result:	The NSP is able to provide U2A Low volume access.
Outcome:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____ _____ _____
Formal acceptance:	ESMIG testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Annex 1 - Common definitions

- Desk Check: some tests are run on the field, while other tests are run as a desk check. A desk check in the Compliance Check Procedure focuses on the formal availability of the documentation. The evaluation is usually done as a paper based proofreading. It aims at identifying errors and gaps at an early stage of evaluation. A desk check assumes the testing engineers make sure to have traversed through all possible paths and make use of every scenario has been assessed.

- On field: practical test have to be run on the environment.

- Eurosystem - The European System of Central Banks (ESCB) consists of the European Central Bank (ECB) and the national central banks (NCBs) of all 28 member states of the European Union (EU).

- Region 1 includes ESMIG site A and B.

- Region 2 includes ESMIG site C and D.

- Di.Co.A. Emulator: message routing software emulating a real Di.Co.A.

- ESMIG Operator is synonym of Eurosystem.

- ESMIG is the infrastructure run by the ESMIG Operator and hosted in region 1 and region 2

- 4CBNet the internal network interconnecting eight data centres in four regions

Annex 2 - DEP XSD

```
<?xml version="1.0" encoding="utf-8"?>
<schema targetNamespace="http://www.ecb.eu/dep-2.0"
                        xmlns="http://www.w3.org/2001/XMLSchema"
                        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                        xmlns:dep="http://www.ecb.eu/dep-2.0"
                        elementFormDefault="qualified"
>
<import
                        namespace="http://www.w3.org/2000/09/xmldsig#"
                        schemaLocation="xmldsig-core-schema.xsd"
/>

 <!-- SIMPLE TYPE DEFINITION -->
 <simpleType name="VersionType">
  <restriction base="string">
   <enumeration value="2.0" />
  </restriction>
 </simpleType>
 <simpleType name="DistinguishedNameType">
  <restriction base="string">
   <minLength value="1" />
   <maxLength value="100" />
  </restriction>
 </simpleType>
 <simpleType name="TechnicalServiceIdType">
  <restriction base="string">
   <maxLength value="60" />
   <pattern
value=".+(MSGRT|MSGSNF|FILERT|FILESNF)\.(INTEG|IAC|EAC|UTEST|PROD)" />
  </restriction>
 </simpleType>
 <simpleType name="SnFTechnicalServiceIdType">
  <restriction base="string">
   <maxLength value="60" />
   <pattern value=".+(MSGSNF|FILESNF)\.(INTEG|IAC|EAC|UTEST|PROD)" />
  </restriction>
 </simpleType>
 <simpleType name="RTTechnicalServiceIdType">
          <restriction base="string">
           <maxLength value="60" />
           <pattern value=".+(MSGRT|FILERT)\.(INTEG|IAC|EAC|UTEST|PROD)" />
          </restriction>
 </simpleType>
 <simpleType name="CommunicationIDType">
  <restriction base="string">
```

```
    <minLength value="1" />
    <maxLength value="100" />
  </restriction>
</simpleType>
<simpleType name="ESMIGMessageIdType">
  <restriction base="string">
    <minLength value="1" />
    <maxLength value="100" />
  </restriction>
</simpleType>
<simpleType name="CompressionIndicatorType">
  <restriction base="string">
    <enumeration value="NONE" />
    <enumeration value="ZIP" />
  </restriction>
</simpleType>
<simpleType name="TimestampType">
  <restriction base="dateTime" />
</simpleType>
<simpleType name="SnFQueueManagerNameType">
  <restriction base="string">
    <minLength value="1" />
    <maxLength value="48" />
  </restriction>
</simpleType>
<simpleType name="SnFQueueNameType">
  <restriction base="string">
    <minLength value="1" />
    <maxLength value="48" />
  </restriction>
</simpleType>
<simpleType name="SnFStatusType">
  <restriction base="string">
    <enumeration value="FAILED" />
    <enumeration value="ACTIVATED" />
    <enumeration value="DEACTIVATED" />
  </restriction>
</simpleType>
<simpleType name="NonRepudiationType">
  <restriction base="string">
    <enumeration value="YES" />
    <enumeration value="NO" />
  </restriction>
</simpleType>
<simpleType name="ReasonType">
  <restriction base="string">
    <minLength value="1" />
    <maxLength value="100" />
  </restriction>
```

```
</simpleType>
<simpleType name="ErrorCodeType">
 <restriction base="string">
  <pattern value="DEP[0-9]{3}E" />
 </restriction>
</simpleType>
<simpleType name="AdditionalInfoType">
 <restriction base="string">
  <minLength value="1" />
  <maxLength value="2000" />
 </restriction>
</simpleType>
<simpleType name="ActorMessageIdType">
 <restriction base="string">
  <minLength value="1" />
  <maxLength value="100" />
 </restriction>
</simpleType>
<simpleType name="MessageDigestType">
 <restriction base="string">
  <minLength value="1" />
  <maxLength value="1024" />
 </restriction>
</simpleType>
<simpleType name="ExchangeStatusType">
 <restriction base="string">
  <enumeration value="OK" />
  <enumeration value="KO" />
 </restriction>
</simpleType>
<simpleType name="PDMAnnotationType">
 <restriction base="string">
  <minLength value="1" />
  <maxLength value="100" />
 </restriction>
</simpleType>
<simpleType name="DeliveryNotificationMode">
 <restriction base="string">
  <enumeration value="YES" />
  <enumeration value="NO" />
  <enumeration value="FAIL" />
 </restriction>
</simpleType>
<simpleType name="RequestType">
 <restriction base="string">
  <minLength value="1" />
  <maxLength value="30" />
 </restriction>
</simpleType>
```

```
<simpleType name="EnvType">
                <restriction base="string">
                        <maxLength value="5" />
                        <pattern value="(INTEG|IAC|EAC|UTEST|PROD)" />
                </restriction>
        </simpleType>
        <simpleType name="MWStatusType">
                <restriction base="string">
                        <enumeration value="FAILED" />
                        <enumeration value="CLOSING" />
                        <enumeration value="CLOSED" />
                        <enumeration value="OPEN" />
                </restriction>
        </simpleType>
 <!-- COMPLEX TYPE DEFINITION -->
 <complexType name="SnFServiceType">
  <sequence>
   <element name="Name" type="dep:SnFTechnicalServiceIdType" />
   <element name="DestQmanagerName" type="dep:SnFQueueManagerNameType"
/>
   <element name="DestQueueName" type="dep:SnFQueueNameType" />
  </sequence>
 </complexType>
 <complexType name="SnFQueryServiceType">
  <sequence>
   <element name="Name" type="dep:SnFTechnicalServiceIdType" />
  </sequence>
 </complexType>
 <complexType name="SnFServiceAckType">
  <complexContent>
   <extension base=" dep:SnFServiceType">
    <sequence>
     <element name="Status" type=" dep:SnFStatusType" />
     <element name="Reason" type=" dep:ReasonType" minOccurs="0" />
    </sequence>
   </extension>
  </complexContent>
 </complexType>
 <complexType name="SnFTrafficCommandType">
  <sequence>
   <element name="Service" type=" dep:SnFServiceType" maxOccurs="unbounded" />
  </sequence>
 </complexType>
 <complexType name="SnFTrafficQueryCommandType">
  <sequence>
   <element name="Service" type=" dep:SnFQueryServiceType" />
  </sequence>
 </complexType>
 <complexType name="SnFTrafficCommandAckType">
```

```
   <sequence>
    <element name="Service" type=" dep:SnFServiceAckType"
maxOccurs="unbounded" />
   </sequence>
 </complexType>
          <!--  RT -->
          <complexType name="RTServiceType">
                    <sequence>
                              <element name="Name" type="
dep:RTTechnicalServiceIdType" />
                              <element name="DestQmanagerName" type="
dep:SnFQueueManagerNameType" />
                              <element name="DestQueueName" type="
dep:SnFQueueNameType" />
                    </sequence>
          </complexType>
          <complexType name="RTTrafficCommandType">
                    <sequence>
                              <element name="Service" type=" dep:RTServiceType"
maxOccurs="unbounded" />
                    </sequence>
          </complexType>

          <complexType name="RTTrafficQueryCommandType">
                    <sequence>
                              <element name="Service" type=" dep:RTQueryServiceType"
/>
                    </sequence>
          </complexType>
          <complexType name="RTQueryServiceType">
                    <sequence>
                              <element name="Name" type="
dep:RTTechnicalServiceIdType" />
                    </sequence>
          </complexType>
          <complexType name="RTServiceAckType">
                    <complexContent>
                              <extension base=" dep:RTServiceType">
                                        <sequence>
                                                  <element name="Status" type="
dep:SnFStatusType" />
                                                  <element name="Reason" type="
dep:ReasonType" minOccurs="0" />
                                        </sequence>
                              </extension>
                    </complexContent>
          </complexType>
          <complexType name="RTTrafficCommandAckType">
                    <sequence>
```

```
                        <element name="Service" type=" dep:RTServiceAckType"
maxOccurs="unbounded" />
                </sequence>
        </complexType>

        <!--  MW -->
        <complexType name="MWType">
                <sequence>
                        <element name="Env" type=" dep:EnvType" />
                </sequence>
        </complexType>
        <complexType name="MWAckType">
                <complexContent>
                        <extension base=" dep:MWType">
                                <sequence>
                                        <element name="Status" type="
dep:MWStatusType" />
                                        <element name="Reason" type="
dep:ReasonType" minOccurs="0" />
                                </sequence>
                        </extension>
                </complexContent>
        </complexType>
 <complexType name="ErrorDescriptionType">
  <sequence>
   <element name="ErrorCode" type=" dep:ErrorCodeType" />
   <element name="AdditionalInfo" type=" dep:AdditionalInfoType" minOccurs="0" />
  </sequence>
 </complexType>
 <complexType name="PDMType">
  <sequence minOccurs="1" maxOccurs="10">
   <element name="TimeStamp" type=" dep:TimestampType" />
   <element name="AdditionalInfo" type=" dep:PDMAnnotationType" minOccurs="0"
/>
  </sequence>
 </complexType>
 <complexType name="ExchangeHeaderType">
  <sequence>
   <element name="Version" type=" dep:VersionType">
    <annotation>
     <documentation>Version of Data Exchange Protocol</documentation>
    </annotation>
   </element>
   <element name="Sender" type=" dep:DistinguishedNameType">
    <annotation>
     <documentation>Identification for the Technical Sender that sends the
     message</documentation>
    </annotation>
   </element>
```

```
    <element name="Receiver" type=" dep:DistinguishedNameType">
     <annotation>
      <documentation>Identification for the Technical Receiver that receives the
      message</documentation>
     </annotation>
    </element>
    <element name="TechnicalServiceId" type=" dep:TechnicalServiceIdType">
     <annotation>
      <documentation>Name of the service used to send messages and files
&lt;Service&gt;+”.”+NSP Name+ "." + &lt;msg-pattern&gt; + "." + &lt;environment&gt;
where &lt;msg-pattern&gt; is one
       of: MSGRT MSGSNF FILERT FILESNF and &lt;environment&gt; is one of:
       INTEG,IAC,EAC,UTEST,PROD.</documentation>
     </annotation>
    </element>
    <element name="RequestType" type=" dep:RequestType">
     <annotation>
      <documentation>Type of the request, to classify message content. In case of
different
       request types in the same BusinessEnvelope, the "MultiRequest" value shall be
used as
       RequestType</documentation>
     </annotation>
    </element>
    <element name="CommunicationId" type=" dep:CommunicationIDType"
minOccurs="0">
     <annotation>
      <documentation>Unique message identifier assigned by the ESMIG counterpart
(at DEP
       transport level).</documentation>
     </annotation>
    </element>
    <element name="ESMIGMessageId" type=" dep:ESMIGMessageIdType"
minOccurs="0">
     <annotation>
      <documentation>Unique message identifier generated by
ESMIG</documentation>
     </annotation>
    </element>
    <element name="ActorMessageId" type=" dep:ActorMessageIdType"
minOccurs="0">
     <annotation>
      <documentation>Unique message identifier generated at Di.Co.A.
site</documentation>
     </annotation>
    </element>
    <element name="EntryTimestamp" type=" dep:TimestampType" minOccurs="0">
     <annotation>
      <documentation>Timestamp of the NSP's gateway reception, based on UTC
```

```
        time</documentation>
      </annotation>
    </element>
    <element name="SendTimestamp" type=" dep:TimestampType">
      <annotation>
        <documentation>Timestamp of the sending of message, based on UTC
time</documentation>
      </annotation>
    </element>
    <element name="ReceiveTimestamp" type=" dep:TimestampType" minOccurs="0">
      <annotation>
        <documentation>Timestamp of the receiving of message, based on UTC
time</documentation>
      </annotation>
    </element>
    <element name="PDMHistory" type=" dep:PDMType" minOccurs="0">
      <annotation>
        <documentation>Timestamp's list of the attempting of the delivery of the
message, based
        on UTC time. This list contains a sequence of SendTimestamp
entries.</documentation>
      </annotation>
    </element>
    <element name="DeliveryNotification" type=" dep:DeliveryNotificationMode"
minOccurs="0">
      <annotation>
        <documentation>Delivery notification management. This field has to be set only
in the
        case of store-and-forward mode. The following values are foreseen: YES: the
delivery
        notification is requested always FAIL: the delivery notification is requested only in
        case of failure NO: the delivery notification is not requested (this is the DEFAULT
        value)</documentation>
      </annotation>
    </element>
    <element name="NonRepudiationExchange" type=" dep:NonRepudiationType">
      <annotation>
        <documentation>Flag that indicates if the non-repudiation is requested or
        not</documentation>
      </annotation>
    </element>
    <element name="Compression" type=" dep:CompressionIndicatorType">
      <annotation>
        <documentation>Flag that indicates the algorithm used to compress the payload
or "NONE"
        (if compression is not used)</documentation>
      </annotation>
    </element>
```

```
    <element name="ExchangeStatus" type=" dep:ExchangeStatusType"
minOccurs="0">
      <annotation>
        <documentation>Status of the exchange: "OK" in the case of a successful
exchange "KO" in
        case of failure This element must be present in DEP technical ack messages and in
        Response messages of R-T (message and file) exchange.</documentation>
      </annotation>
    </element>
    <element name="ErrorDescription" type="dep:ErrorDescriptionType"
minOccurs="0">
      <annotation>
        <documentation>Description of the error occurred during the
exchanging</documentation>
      </annotation>
    </element>
    <element name="MessageDigest" type=" dep:MessageDigestType" minOccurs="0">
      <annotation>
        <documentation>Digest of the Message/File exchanged (The digest has to be
applied to the
        DEP Exchange Header and to the Business Envelope) This element is used only in
Technical
        Ack primitive, when DEP:NonRepudiationExchange flag has been set. The digest
has to be
        based on the received DEP Exchange Header and Business
Envelope.</documentation>
      </annotation>
    </element>
  </sequence>
 </complexType>
 <complexType name="BusinessEnvelopeType">
  <complexContent>
   <extension base="anyType" />
  </complexContent>
 </complexType>
 <complexType name="ExchangeEnvelopeType">
  <sequence>
   <element name="ExchangeHeader" type=" dep:ExchangeHeaderType" />
   <element name="BusinessEnvelope" type=" dep:BusinessEnvelopeType" />
   <element ref="ds:Signature" minOccurs="0" />
  </sequence>
 </complexType>
 <complexType name="TechnicalAckType">
  <sequence>
   <element name="ExchangeHeader" type=" dep:ExchangeHeaderType" />
   <element ref="ds:Signature" minOccurs="0" />
  </sequence>
 </complexType>
 <complexType name="DeliveryNotificationType">
```

```
  <sequence>
    <element name="ExchangeHeader" type=" dep:ExchangeHeaderType" />
    <element ref="ds:Signature" minOccurs="0" />
  </sequence>
</complexType>

<!-- ELEMENT TYPE DEFINITION -->
<element name="Request" type=" dep:ExchangeEnvelopeType" />
<element name="Response" type=" dep:ExchangeEnvelopeType" />
<element name="TechnicalAck" type=" dep:TechnicalAckType" />
<element name="DeliveryNotification" type=" dep:DeliveryNotificationType" />
<element name="EnableSnfTraffic" type=" dep:SnFTrafficCommandType" />
<element name="DisableSnfTraffic" type=" dep:SnFTrafficCommandType" />
<element name="EnableSnfTrafficAck" type=" dep:SnFTrafficCommandAckType" />
<element name="DisableSnfTrafficAck" type=" dep:SnFTrafficCommandAckType" />
<element name="QuerySnfTraffic" type=" dep:SnFTrafficQueryCommandType" />
<element name="QuerySnfTrafficAck" type=" dep:SnFTrafficCommandAckType" />
<element name="EnableRTTraffic" type=" dep:RTTrafficCommandType" />
<element name="DisableRTTraffic" type=" dep:RTTrafficCommandType" />
<element name="EnableRTTrafficAck" type=" dep:RTTrafficCommandAckType" />
<element name="DisableRTTrafficAck" type=" dep:RTTrafficCommandAckType" />
<element name="QueryRTTraffic" type=" dep:RTTrafficQueryCommandType" />
<element name="QueryRTTrafficAck" type=" dep:RTTrafficCommandAckType" />
<element name="OpenTrafficChannels" type=" dep:MWType" />
<element name="OpenTrafficChannelsAck" type=" dep:MWAckType" />
<element name="CloseTrafficChannels" type=" dep:MWType" />
<element name="CloseTrafficChannelsAck" type=" dep:MWAckType" />
<element name="QueryTrafficChannels" type=" dep:MWType" />
<element name="QueryTrafficChannelsAck" type=" dep:MWAckType" />
 </schema>
```

Annex 3 - DEP maintenance window primitive samples

CloseTrafficChannels primitive

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:CloseTrafficChannels xmlns:dep="http://www.ecb.eu/dep-2.0">
  <dep:Env>INTEG</dep:Env>
</dep:CloseTrafficChannels>

 <!--
  MQMD.Expiry=-1
  MQMD.GroupID=
  MQMD.CodeCharacterSetId=1208
  MQMD.MsgType=Datagram
  MQMD.MessageID=414D5120444550514D4752534348524FF383185302E92620
  MQMD.Report=MQRO_NONE
  MQMD.Format=NONE
 -->
```

CloseTrafficChannelsAck primitive

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:CloseTrafficChannelsAck xmlns:dep="http://www.ecb.eu/dep-2.0" >
  <dep:Env>INTEG</dep:Env>
  <dep:Status>CLOSING</dep:Status>
</dep:CloseTrafficChannelsAck>

<!--
MQMD.ApplIdData=SIA-COLT-22000JSSCHRO
MQMD.Encoding=273
MQMD.Feedback=0
MQMD.Expiry=-1
MQMD.PutDateTime=16/02/2015 18:13:47.260
MQMD.CodeCharacterSetId=1208
MQMD.GroupID=
MQMD.MsgType=4
MQMD.MessageID=414D5120444550514D4752534348524FF383185303E82620
MQMD.Report=0
MQMD.Format=null
MQMD.CorrelationID=414D5120444550514D4752534348524FF383185302E92620
-->
```

OpenTrafficChannels

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:OpenTrafficChannels xmlns:dep="http://www.ecb.eu/dep-2.0" >
  <dep:Env>INTEG</dep:Env>
</dep:OpenTrafficChannels>

 <!--
  MQMD.Expiry=-1
  MQMD.GroupID=
  MQMD.CodeCharacterSetId=1208
  MQMD.MsgType=Datagram
  MQMD.MessageID=414D5120444550514D4752534348524FF383185302E92623
  MQMD.Report=MQRO_NONE
  MQMD.Format=NONE
 -->
```

OpenTrafficChannelsAck

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:OpenTrafficChannelsAck xmlns:dep="http://www.ecb.eu/dep-2.0" >
  <dep:Env>INTEG</dep:Env>
  <dep:Status>OPEN</dep:Status>
</dep:OpenTrafficChannelsAck>
 <!--
  MQMD.ApplIdData=xxxx-yyyy
  MQMD.Encoding=273
  MQMD.Feedback=0
  MQMD.Expiry=-1
  MQMD.PutDateTime=16/12/2018 18:13:47.260
  MQMD.CodeCharacterSetId=1208
  MQMD.GroupID=
  MQMD.MsgType=4
  MQMD.MessageID=414D5120444550514D4752534348524FF383185303E82621
  MQMD.Report=0
  MQMD.Format=null
  MQMD.CorrelationID=414D5120444550514D4752534348524FF383185302E92623
 -->
```

QueryTrafficChannels

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:QueryTrafficChannels xmlns:dep="http://www.ecb.eu/dep-2.0" >
  <dep:Env>INTEG</dep:Env>
</dep:QueryTrafficChannels>

 <!--
  MQMD.Expiry=-1
  MQMD.GroupID=
  MQMD.CodeCharacterSetId=1208
  MQMD.MsgType=Datagram
  MQMD.MessageID=414D5120444550514D4752534348524FF383185302E92623
  MQMD.Report=MQRO_NONE
  MQMD.Format=NONE
 -->
```

QueryTrafficChannelsAck

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:QueryTrafficChannelsAck xmlns:dep="http://www.ecb.eu/dep-2.0" >
   <dep:Env>INTEG</dep:Env>
   <dep:Status>CLOSED</dep:Status>
</dep:QueryTrafficChannelsAck>
 <!--
  MQMD.ApplIdData=xxxx-yyyy
  MQMD.Encoding=273
  MQMD.Feedback=0
  MQMD.Expiry=-1
  MQMD.PutDateTime=16/12/2018 18:13:47.260
  MQMD.CodeCharacterSetId=1208
  MQMD.GroupID=
  MQMD.MsgType=4
  MQMD.MessageID=414D5120444550514D4752534348524FF383185303E82621
  MQMD.Report=0
  MQMD.Format=null
  MQMD.CorrelationID=414D5120444550514D4752534348524FF383185302E92623
 -->
```

Annex 4 - MEPT examples

Instant payment request from the originator

```
<rfh2>
   <HMAC>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK...</HMAC>
   <HMACKeyId>1234</HMACKeyId>
   <MsgSignature>
      <Signature ...
      </Signature>
   </MsgSignature>
   <ProtocolVersion>1</ProtocolVersion>
   <Service>TIPS-TEST</Service>
   <Sender>cn=originator-dn,ou=...,o=...</Sender>
   <Receiver>cn=tips-dn,ou=...,o=...</Receiver>
   <PrimitiveType>ReceiveIndication</PrimitiveType>
   <MsgType>pacs.008.001.02</MsgType>
   <SendTimestamp>2016-12-19T12:00:01.222Z</SendTimestamp>
   <ReceiveTimestamp>2016-12-19T12:00:01.777Z</ReceiveTimestamp>
   <MsgBizIdentifier>MSG001</MsgBizIdentifier>
   <MsgNetworkIdentifier>NWX000001</MsgNetworkIdentifier>
</rfh2>
<Document                    xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.02">
   <FIToFICstmrCdtTrf>
      <GrpHdr>
         <MsgId>MSG001</MsgId>
         <CreDtTm>2016-12-19T12:00:01.222Z</CreDtTm>
         <NbOfTxs>1</NbOfTxs>
         <TtlIntrBkSttlmAmt Ccy="EUR">123.45</TtlIntrBkSttlmAmt>
         <IntrBkSttlmDt>2016-12-19</IntrBkSttlmDt>
         <SttlmInf>
            <SttlmMtd>INDA</SttlmMtd>
         </SttlmInf>
         <PmtTpInf>
            <SvcLvl>
               <Cd>SEPA</Cd>
            </SvcLvl>
            <LclInstrm>
               <Cd>INST</Cd>
            </LclInstrm>
         </PmtTpInf>
         <InstgAgt>
            <FinInstnId>
               <BIC>ORIGINATOR-BIC</BIC>
            </FinInstnId>
         </InstgAgt>
         <InstdAgt>
            <FinInstnId>
               <BIC>BENEFICIARY-BIC</BIC>
            </FinInstnId>
```

```
        </InstdAgt>
      </GrpHdr>
      <CdtTrfTxInf>
        <PmtId>
          <EndToEndId>ENDTOEND001</EndToEndId>
          <TxId>TRX001</TxId>
        </PmtId>
        <IntrBkSttlmAmt Ccy="EUR">123.45</IntrBkSttlmAmt>
        <AccptncDtTm>2016-12-19T12:00:01.222Z</AccptncDtTm>
        <ChrgBr>SLEV</ChrgBr>
        <DbtrAgt>
          <FinInstnId>
            <BIC>ORIGINATOR-BIC</BIC>
          </FinInstnId>
        </DbtrAgt>
        <CdtrAgt>
          <FinInstnId>
            <BIC>BENEFICIARY-BIC</BIC>
          </FinInstnId>
        </CdtrAgt>
      </CdtTrfTxInf>
    </FIToFICstmrCdtTrf>
</Document>
```

Instant payment request validated and to be forwarded to the beneficiary

```
<rfh2>
   <HMAC>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK...</HMAC>
   <HMACKeyId>1234</HMACKeyId>
   <ProtocolVersion>1</ProtocolVersion>
   <Service>TIPS-TEST</Service>
   <Sender>cn=tips-dn,ou=...,o=...</Sender>
   <Receiver>cn=beneficiary-dn,ou=...,o=...</Receiver>
   <PrimitiveType>SendRequest</PrimitiveType>
   <MsgType>pacs.008.001.02</MsgType>
   <MsgBizIdentifier>MSG001</MsgBizIdentifier>
   <SignatureRequired>Y</SignatureRequired>
   <NotificationRequired>E</NotificationRequired>
   <TechnicalAckRequired>E</TechnicalAckRequired>

</rfh2>
<Document                    xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.02">
   <FIToFICstmrCdtTrf>
      <GrpHdr>
        <MsgId>MSG001</MsgId>
        <CreDtTm>2016-12-19T12:00:01.222Z</CreDtTm>
        <NbOfTxs>1</NbOfTxs>
        <TtlIntrBkSttlmAmt Ccy="EUR">123.45</TtlIntrBkSttlmAmt>
        <IntrBkSttlmDt>2016-12-19</IntrBkSttlmDt>
        <SttlmInf>
          <SttlmMtd>INDA</SttlmMtd>
        </SttlmInf>
```

```
        <PmtTpInf>
          <SvcLvl>
            <Cd>SEPA</Cd>
          </SvcLvl>
          <LclInstrm>
            <Cd>INST</Cd>
          </LclInstrm>
        </PmtTpInf>
        <InstgAgt>
          <FinInstnId>
            <BIC>ORIGINATOR-BIC</BIC>
          </FinInstnId>
        </InstgAgt>
        <InstdAgt>
          <FinInstnId>
            <BIC>BENEFICIARY-BIC</BIC>
          </FinInstnId>
        </InstdAgt>
      </GrpHdr>
      <CdtTrfTxInf>
        <PmtId>
          <EndToEndId>ENDTOEND001</EndToEndId>
          <TxId>TRX001</TxId>
        </PmtId>
        <IntrBkSttlmAmt Ccy="EUR">123.45</IntrBkSttlmAmt>
        <AccptncDtTm>2016-12-19T12:00:01.222Z</AccptncDtTm>
        <ChrgBr>SLEV</ChrgBr>
        <DbtrAgt>
          <FinInstnId>
            <BIC>ORIGINATOR-BIC</BIC>
          </FinInstnId>
        </DbtrAgt>
        <CdtrAgt>
          <FinInstnId>
            <BIC>BENEFICIARY-BIC</BIC>
          </FinInstnId>
        </CdtrAgt>
      </CdtTrfTxInf>
    </FIToFICstmrCdtTrf>
</Document>
```

Positive response from the beneficiary

```
<rfh2>
  <HMAC>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK...</HMAC>
  <HMACKeyId>1234</HMACKeyId>
  <MsgSignature>
    <Signature ...
    </Signature>
  </MsgSignature>
  <ProtocolVersion>1</ProtocolVersion>
  <Service>TIPS-TEST</Service>
  <Sender>cn=originator-dn,ou=tips,o=...</Sender>
```

```
   <Receiver>cn=tips-dn,ou=tips,o=...</Receiver>
   <PrimitiveType>ReceiveIndication</PrimitiveType>
   <MsgType>pacs.002.001.03</MsgType>
   <SendTimestamp>2016-12-19T12:00:01.222Z</SendTimestamp >
   <ReceiveTimestamp>2016-12-19T12:00:01.777Z</ReceiveTimestamp >
   <MsgBizIdentifier>MSG002</MsgBizIdentifier>
   <MsgNetworkIdentifier>NWX000002</MsgNetworkIdentifier>
</rfh2>
<Document                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.002.001.03">
   <FIToFIPmtStsRpt>
      <GrpHdr>
         <MsgId>MSG002</MsgId>
         <CreDtTm>2016-12-19T12:00:01.222Z</CreDtTm>
         <InstgAgt>
            <FinInstnId>
               <BIC>BENEFICIARY-BIC</BIC>
            </FinInstnId>
         </InstgAgt>
         <InstdAgt>
            <FinInstnId>
               <BIC>TIPS-BIC</BIC>
            </FinInstnId>
         </InstdAgt>
      </GrpHdr>
      <OrgnlGrpInfAndSts>
         <OrgnlMsgId>MSG001</OrgnlMsgId>
         <OrgnlMsgNmId>pacs.008.001.02</OrgnlMsgNmId>
         <OrgnlCreDtTm>2016-12-19T12:00:01.222Z</OrgnlCreDtTm>
         <GrpSts>ACCP</GrpSts>
      </OrgnlGrpInfAndSts>
      <TxInfAndSts>
         <StsId>MSG001</StsId>
         <OrgnlEndToEndId>ENDTOEND001</OrgnlEndToEndId>
         <OrgnlTxId>TRX001</OrgnlTxId>
         <TxSts>ACCP</TxSts>
         <AccptncDtTm>2016-12-19T12:00:01.222Z</AccptncDtTm>
         <OrgnlTxRef>
            <IntrBkSttlmAmt Ccy="EUR">123.45</IntrBkSttlmAmt>
            <DbtrAgt>
               <FinInstnId>
                  <BIC>ORIGINATOR-BIC</BIC>
               </FinInstnId>
            </DbtrAgt>
            <CdtrAgt>
               <FinInstnId>
                  <BIC>BENEFICIARY-BIC</BIC>
               </FinInstnId>
            </CdtrAgt>
         </OrgnlTxRef>
      </TxInfAndSts>
   </FIToFIPmtStsRpt>
</Document>
```

Instant Payment completed

Response to be sent to the originator

```
<rfh2>
   <HMAC>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK...</HMAC>
   <HMACKeyId>1234</HMACKeyId>
   <ProtocolVersion>1</ProtocolVersion>
   <Service>TIPS-TEST</Service>
   <Sender>cn=tips-dn,ou=tips,o=...</Sender>
   <Receiver>cn=originator-dn,ou=tips,o=...</Receiver>
   <PrimitiveType>SendRequest</PrimitiveType>
   <MsgType>pacs.002.001.03</MsgType>
   <MsgBizIdentifier>MSG001@00001@dbtr</MsgBizIdentifier>
   <SignatureRequired>N</SignatureRequired>
   <NotificationRequired>E</NotificationRequired>
   <TechnicalAckRequired>E</TechnicalAckRequired>
</rfh2>
<Document                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.002.001.03">
   <FIToFIPmtStsRpt>
      <GrpHdr>
         <MsgId>MSG001@00001@dbtr</MsgId>
         <CreDtTm>2016-12-19T12:00:01.222Z</CreDtTm>
         <InstgAgt>
            <FinInstnId>
               <BIC>TIPS-BIC</BIC>
            </FinInstnId>
         </InstgAgt>
         <InstdAgt>
            <FinInstnId>
               <BIC>ORIGINATOR-BIC</BIC>
            </FinInstnId>
         </InstdAgt>
      </GrpHdr>
      <OrgnlGrpInfAndSts>
         <OrgnlMsgId>MSG001</OrgnlMsgId>
         <OrgnlMsgNmId>pacs.008.001.02</OrgnlMsgNmId>
         <OrgnlCreDtTm>2016-12-19T12:00:01.222Z</OrgnlCreDtTm>
         <GrpSts>ACCP</GrpSts>
      </OrgnlGrpInfAndSts>
      <TxInfAndSts>
         <StsId>MSG001</StsId>
         <OrgnlEndToEndId>ENDTOEND001</OrgnlEndToEndId>
         <OrgnlTxId>TRX001</OrgnlTxId>
         <TxSts>ACCP</TxSts>
         <AccptncDtTm>2016-12-19T12:00:01.222Z</AccptncDtTm>
         <OrgnlTxRef>
            <IntrBkSttlmAmt Ccy="EUR">123.45</IntrBkSttlmAmt>
            <DbtrAgt>
               <FinInstnId>
                  <BIC>ORIGINATOR-BIC</BIC>
               </FinInstnId>
            </DbtrAgt>
            <CdtrAgt>
               <FinInstnId>
```

```
                <BIC>BENEFICIARY-BIC</BIC>
              </FinInstnId>
            </CdtrAgt>
          </OrgnlTxRef>
        </TxInfAndSts>
    </FIToFIPmtStsRpt>
</Document>
```

Response to be sent to the beneficiary

```
<rfh2>
   <HMAC>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK...</HMAC>
   <HMACKeyId>1234</HMACKeyId>
   <ProtocolVersion>1</ProtocolVersion>
   <Service>TIPS-TEST</Service>
   <Sender>cn=tips-dn,ou=tips,o=...</Sender>
   <Receiver>cn=beneficiary-dn,ou=tips,o=...</Receiver>
   <PrimitiveType>SendRequest</PrimitiveType>
   <MsgType>pacs.002.001.03</MsgType>
   <MsgBizIdentifier>MSG001@00001@cdtr</MsgBizIdentifier>
   <SignatureRequired>N</SignatureRequired>
   <NotificationRequired>E</NotificationRequired>
   <TechnicalAckRequired>E</TechnicalAckRequired>

</rfh2>
<Document                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.002.001.03">
   <FIToFIPmtStsRpt>
      <GrpHdr>
         <MsgId>MSG001@00001@cdtr</MsgId>
         <CreDtTm>2016-12-19T12:00:01.222Z</CreDtTm>
         <InstgAgt>
            <FinInstnId>
               <BIC>TIPS-BIC</BIC>
            </FinInstnId>
         </InstgAgt>
         <InstdAgt>
            <FinInstnId>
               <BIC>BENEFICIARY-BIC</BIC>
            </FinInstnId>
         </InstdAgt>
      </GrpHdr>
      <OrgnlGrpInfAndSts>
         <OrgnlMsgId>MSG001</OrgnlMsgId>
         <OrgnlMsgNmId>pacs.008.001.02</OrgnlMsgNmId>
         <OrgnlCreDtTm>2016-12-19T12:00:01.222Z</OrgnlCreDtTm>
         <GrpSts>ACCP</GrpSts>
      </OrgnlGrpInfAndSts>
      <TxInfAndSts>
         <StsId>MSG001</StsId>
         <OrgnlEndToEndId>ENDTOEND001</OrgnlEndToEndId>
         <OrgnlTxId>TRX001</OrgnlTxId>
         <TxSts>ACCP</TxSts>
```

```
        <AccptncDtTm>2016-12-19T12:00:01.222Z</AccptncDtTm>
        <OrgnlTxRef>
          <IntrBkSttlmAmt Ccy="EUR">123.45</IntrBkSttlmAmt>
          <DbtrAgt>
            <FinInstnId>
              <BIC>ORIGINATOR-BIC</BIC>
            </FinInstnId>
          </DbtrAgt>
          <CdtrAgt>
            <FinInstnId>
              <BIC>BENEFICIARY-BIC</BIC>
            </FinInstnId>
          </CdtrAgt>
        </OrgnlTxRef>
      </TxInfAndSts>
    </FIToFIPmtStsRpt>
</Document>
```

Technical Ack received on Response sent to Beneficiary

```
<rfh2>
   <HMAC>odinf90sUSKDoUSLLio5S4d5VdWpoad4...</HMAC>
   <HMACKeyId>1234</HMACKeyId>
   <ProtocolVersion>1</ProtocolVersion>
   <Service>TIPS-TEST</Service>
   <Sender>cn=tips-dn,ou=tips,o=...</Sender>
   <Receiver>cn=beneficiary-dn,ou=tips,o=...</Receiver>
   <PrimitiveType>TechnicalAck</PrimitiveType>
   <SendTimestamp>2016-12-19T12:00:01.222Z</SendTimestamp>
   <MsgBizIdentifier>MSG001@00001@cdtr</MsgBizIdentifier>
   <MsgNetworkIdentifier>NWX000005</MsgNetworkIdentifier>
   <PrimitiveReturnCode>KO</PrimitiveReturnCode>
   <PrimitiveReasonCode>TIPS.FailedDelivery</PrimitiveReasonCode>
</rfh2>
```

Business requirements for ESMIG Network Service Providers

– Attachment 1.2 to the Concession Contract –

The following requirements principally aim at ensuring that NSPs observe a minimum set of non-technical requirements which are necessary for the Eurosystem to have reasonable confidence in the soundness and stability of the NSP and the Connectivity services. In some cases, they also define minimum service levels which may otherwise – despite competition between NSPs – be difficult to negotiate for Di.Co.A. with limited connectivity business. Consequently, these requirements should allow Di.Co.A.to obtain a sustainable minimum level of service, and/or a minimum amount of information allowing them to make informed decisions about their choice of NSP(s) and their preferred way of interaction with the ESMIG Services and Applications.

These requirements are specified in this document as minimum conditions to be fulfilled during the Term of the Concession Contract, as from the time indicated separately in this document for each of the requirements. Every breach of a requirement will – beyond any indemnities resulting from the application of the liability provisions of the Concession Contract – trigger payment of penalties as indicated for each of the requirements, and may ultimately result in the termination of the Concession Contract, according to the provisions specified below.

Upon termination of the concession for cause by the Eurosystem, the NSP is obliged to offer all Connectivity Services to the Eurosystem and to the Di.Co.A. that have an ESMIG Connectivity Services Agreement with this NSP, for a period of up two years after the Termination. During this period, any breaches of the Concession Contract will continue to be subject to the indemnities and penalties, set out below.

Taking into account the systemic relevance of the ESMIG Services and Applications as pan-European market infrastructures, NSPs are expected to be subject to the oversight requirements which the relevant Central Banks may define.

Table of Contents

1 Requirements applicable to the providers of Connectivity Services

1.1 Financial strength

Reference ID	ESMIG.UC.BC.010	

Objective

This requirement aims at mitigating the risk that the NSP becomes insolvent at short notice, or becomes financially weak enough for its creditors to cease offering services (or threatening to do so), as a result of which Di.Co.A. face service (continuity) problems.

Requirement

The NSP shall fulfil each of the following requirements:

1. Have a minimum value in own funds of 100m €;
2. Have a maximum level of indebtedness of 200%, calculated as the ratio of total debts over own funds;

In addition, the NSP shall – for information purposes only - provide the Eurosystem with the yearly turnover, as well as the share of the turnover that is covered by the provision of connectivity services and/or data transmission services.

The NSP shall fulfil each of these requirements, either at the level of the entity that will sign the Concession Contract, or at the consolidated level (if the NSP is a subsidiary and its accounts are consolidated according to internationally recognised standards).

Verification

As soon as the Concession Contract is signed, and within one month after every closure of the annual accounts, either of the NSP itself or of the entity at which level the NSP's annual accounts are consolidated, the NSP will provide the Eurosystem with a statement, certified by a competent accountant or auditor, specifying that the annual accounts have been audited according to internationally accepted standards, as well as the amount of own funds, the level of indebtedness and the level of profitability, calculated as specified above and according to internationally accepted accountancy standards.

If the NSP is a subsidiary or a branch, this statement will be accompanied by a guarantee, issued by the entity at which level the annual accounts are consolidated, that it will provide all necessary financial support to the NSP, allowing the latter to continue offering the required services during a minimum period of two years, both to the Eurosystem and to any Di.Co.A. that have a ESMIG Connectivity Services Agreement with that NSP.

Breaches

In the event that the NSP fails to deliver the required statement within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

In the event that the NSP delivers the required statement, but reaches a ratio between the required value and half of this value, the NSP will – together with the statement - explain the reasons behind the decline and present an action plan to redress the situation within the next 6 months. Provided the Eurosystem accepts the action plan, the NSP will provide quarterly updates on the progress achieved compared to the plan. If the required value is not reached at the next annual verification, the Eurosystem may terminate the Concession Contract.

In the event that the NSP delivers the required statement, but reaches a ratio below half of the required value, the Eurosystem may terminate the Concession Contract immediately.

1.2 Data protection policy

Reference ID	ESMIG.UG.BC.060	

Objective

This requirement aims at ensuring the protection of personal data and confidential data avoiding the risk that personal or confidential data about any instruction or account position can be accessed by any non-authorised entity, including a public entity, whether law enforcement or other, which has no jurisdictional competence over any of the EEA countries or Switzerland.

Requirement

The NSP shall comply with a data protection policy which is in full compliance with relevant EU legislation. In addition, data pertaining to Di.Co.A. falling under EU Data Protection legislation are not to be held on data stores located in – and should not be routed via – any country without a level of data protection at least equivalent to the one in the EU, unless necessary under extreme circumstances, strictly for the shortest time required to re-establish normal functioning conditions, and only according to procedures defined in Operations Manual. Finally, the NSP shall have appropriate measures in place to protect confidential data pertaining to Di.Co.A..

Verification

At the latest one year after the signature of the Concession Contract, the NSP shall demonstrate fulfilment of this requirement, either by means of a statement issued by the competent data protection authority, or by means of a legal opinion from an internationally recognised law firm, stating the adequacy of the NSP's data protection policy in conjunction with the EU data protection policy and its measures to protect confidential data from unauthorised access. In case of changes to the EU Data Protection legislation or to the NSP's data protection policy, the NSP will submit an updated version of the legal opinion, promptly in the former case. It will submit its proposed DPP changes to the Eurosystem for approval 12 months in advance in the latter case.

Breaches

In the event that the NSP fails to deliver the required legal opinion within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

In the event that the legal opinion shows some risks, either the impact or the likelihood of which is declared as low, the NSP will – together with the legal opinion - present an action plan to redress the situation within 6 months, and will explain how the risks will be mitigated

in the meantime. Provided the Eurosystem accepts the action plan, the NSP will provide quarterly updates on the progress achieved compared to the plan. If the risks have not disappeared within the period of 6 months, the Eurosystem may terminate the Concession Contract.

In the event that the legal opinion states that the impact or the likelihood of the risks identified is other than low, the Eurosystem may terminate the Concession Contract.

1.3 Operational risk management framework

Reference ID	ESMIG.UG.BC.090	

Objective

This requirement aims at ensuring that NSPs have the structures and processes in place to deliver reliable connectivity services, as well as high-quality support to Di.Co.A..

Requirement

The NSP shall have implemented an operational risk management framework or an information security management framework. The NSP shall explain to the Eurosystem which standard(s) or framework(s) it applies and which processes are used to implement it/them. Whenever a change to the framework(s) or the related processes have been agreed by the NSP's Board, the NSP shall seek the Eurosystem's approval at least 3 months before the implementation of such change.

Verification

At the latest one year after the signature of the Concession Contract, the NSP shall demonstrate fulfilment of this requirement by delivering to the Eurosystem the operational risk management policy or information security management policy, together with a statement from an external auditor, which certifies (i) that the policy is appropriate to the criticality of the Connectivity Services to be provided by the NSP in the context of ESMIG, and (ii) that adequate processes are in place to support the policy. The policy will explain the objective(s) and scope of the operational risk management framework or information security management framework, and on which methodology it is based (if it is internationally recognised), or give a comprehensive overview of the methodology (if it is a proprietary methodology). In addition, the policy will describe the approach to risk tolerance (in terms of likelihood and impact), as well as the roles and responsibilities in the risk management process, in particular with respect to risk acceptance.

In case of material changes to the framework, the policy or the processes, the NSP will seek approval of these changes to the Eurosystem at least 3 months before its envisaged implementation.

Breaches

In the event that the NSP fails to deliver the operational risk or information security management policy or the auditor's statement within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

If the auditor's statement reveals minor areas of improvement, either with respect to the policy or in relation to the supporting risk management processes, the NSP shall present – together with the auditor's statement – an action plan to eliminate these deficiencies within a period of 6 months. Provided the Eurosystem accepts the action plan, the NSP will provide quarterly updates on the progress achieved compared to the plan. If the deficiencies have not disappeared within 6 months, the Eurosystem may terminate the Concession Contract.

In the event that the auditor's statement shows other than minor deficiencies, the Eurosystem may terminate the Concession Contract.

1.4 Technology risk management framework

Reference ID	ESMIG.UG.BC.080	inclusion

Objective

This requirement aims at ensuring that the NSP uses mainstream technology which is widely supported, which has a proven track record, and the access to which is not limited by anti-competitive behaviour of the owners of the intellectual property rights on the technology.

Requirement

The NSP shall have implemented a technology risk management framework. The NSP shall explain to the Eurosystem which standard(s) or framework(s) it applies and which processes are used to implement it/them. Whenever a material change to the framework or the processes related to it have been agreed by the NSP's Board, the NSP shall seek the Eurosystem's approval for such change, at least 3 months before implementation.

Verification

At the latest one year after the signature of the Concession Contract, the NSP shalldemonstrate fulfilment of this requirement by delivering to the Eurosystem the technology risk management policy, together with a statement from an external auditor, which certifies (i) that the policy is commensurate to the criticality of the Connectivity Services to be provided by the NSP in the context of ESMIG, and (ii) that the adequate processes are in place to support the policy. The policy will explain the objective(s) and scope of the technology risk management framework and give a comprehensive overview of the methodology. As a minimum, the policy should cover the risk – for all layers in the Open Systems Interconnection (OSI) model – that a new technology that becomes mainstream in the industry diverges from the NSP's active technology and that the number of vendors of NSP-compatible technologies decreases. In addition, the policy will describe the approach to risk tolerance (in terms of likelihood and impact), as well as the roles and responsibilities in the risk management process, in particular with respect to risk acceptance.

In case of changes to the framework, the policy or the processes, the NSP will explain these changes to the Eurosystem within a period of 3 months.

Breaches

In the event that the NSP fails to deliver the technology risk management policy, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

In case the auditor's statement reveals minor areas of improvement, either with respect to the policy or in relation to the supporting risk management processes, the NSP shall present –

together with the auditor's statement – an action plan to eliminate these deficiencies within a period of 6 months. Provided the Eurosystem accepts the action plan, the NSP will provide quarterly updates on the progress achieved compared to the plan. If the deficiencies have not disappeared within this period, the Eurosystem may terminate the Concession Contract.

In the event that the auditor's statement shows other than minor deficiencies, the Eurosystem may terminate the Concession Contract.

2 Business criteria related to the Connectivity Services

2.1 User Documentation

Reference ID	ESMIG.UG.BC.100	

Objective

This requirement aims at facilitating a smooth "on-boarding" process and a resilient implementation of the required connectivity services on the Di.Co.A.' side.

Requirement

The NSP shall ensure the availability of comprehensive and clear documentation, as well as a support structure, that allows the directly connected market participantto implement the ESMIG connectivity services in a timely, cost-effective and resilient way.

Verification

At the latest six months after the Concession Contract has been signed, the NSP shall explain to the Eurosystem:

- which technical solutions are available at each layer of the Open Systems Interconnection (OSI) model for different types of Di.Co.A., and which options are available for Di.Co.A. to influence or deviate from those solutions;
- what documentation and support structure is available to potential Di.Co.A., and which procedures have to be followed, in order to allow them to make an informed decision about the viability and cost-effectiveness of the Di.Co.A.' ESMIG connectivity solutions;
- what documentation and support structure is available to actual Di.Co.A. and which procedures have to be followed, in order to allow them to implement their preferred ESMIG connectivity solution;
- which are the different stages of the implementation of an ESMIG connectivity solution is on the Di.Co.A.' side and which are the mandatory and/or optional validation points, and which testing opportunities (and support) are available at these points;

Breaches

In the event that the NSP fails to deliver the required information within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

In the event that the documentation provided by the NSP trigger additional questions from the Eurosystem, the NSP shall reply to these questions within a period of 1 month and, where needed, shall update its User Documentation within 3 months.

2.2 Operational risk reporting

Reference ID	ESMIG.UG.BC.110	

Objective

This requirement aims at ensuring that Di.Co.A. can make informed risk management decisions based on information that is made available by the NSP.

Requirement

The NSP shall make available to the Eurosystem and all its Di.Co.A. a yearly SAS70 Type II report or a report based on at least equivalent standards (such as ISAE 3402 or the US SSAE 16), covering all T2S connectivity services, together with a statement from an internal or external auditor that the report presents a fair overview of the risk situation at the NSP.

Verification

At the latest one year after the Concession Contract is signed, and every year thereafter until the termination of the Concession Contract, the NSP will transmit promptly after completion an annual SAS70 Type II report or a report based on at least equivalent standards (such as ISAE 3402 or the US SSAE 16) to the Eurosystem, together with the list of Di.Co.A. connected to any of the ESMIG Services and Applications via the NSP, and a statement from the NSP that all these entities have received the same report.

Breaches

In the event that the NSP fails to deliver the required report within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

In the event that the report reveals minor areas of improvement, the NSP shall – within 1 month after the delivery of the report to the Eurosystem – present an action plan to the Eurosystem to eliminate these deficiencies within a period of 6 months, and explain how the related risks will be mitigated until their elimination. Provided the Eurosystem accepts the action plan, the NSP will provide quarterly updates on the progress achieved compared to the plan. If the deficiencies have not been eleminated within 6 months, the Eurosystem may terminate the Concession Contract.

In the event that the report or the auditor's accompanying statement shows other than minor deficiencies, the Eurosystem may terminate the Concession Contract.

3 Publication of maximum prices

Reference ID	ESMIG.UG.BC.130	

Objective

This requirement aims at ensuring transparency among Di.Co.A. about the maximum prices that a NSP will charge to them for each of the ESMIG connectivity services, listed in the Attachment 1.4 of the Concession Contract (Economic Offer (maximum prices)).

Requirement

The NSP shall make available its maximum fees for each of the ESMIG connectivity services listed in Attachment 1.4 of the Concession Contract (Economic Offer (maximum prices)).

Verification

At the latest one month after the signature of the Concession Contract, the NSP shall deliver to the Eurosystem a price publication policy, indicating how the maximum fees for each of the ESMIG connectivity services have been and/or will be made public. In the event of any change in content of the published information or if the NSP intends to change the publication media, the latter shall notify the Eurosystem at least one month in advance.

The list of connectivity services for which the fee has to be made public are those listed in Attachment 1.4 of the Concession Contract (Economic Offer (maximum prices)). All prices shall be indicated in euro with a maximum precision of 4 decimals (i.e. 1/100 of eurocents), both in numbers and in letters. In case of discordance, the price expressed in letters shall be considered valid.

Breaches

In the event that the NSP fails to deliver the required information within the time specified above, the Eurosystem will – during the first month of delay – levy a penalty of 1.000 € per day delay. For every additional month of delay, this penalty will be increased by 1.000 € per day, up to a maximum of 10.000 € per day. Without prejudice to these penalties, upon a delay of three months, the Eurosystem may terminate the Concession Contract.

T2S, T2, TIPS, ECMS AND POTENTIALLY OTHER MARKET INFRASTRUCTURE SERVICES AND APPLICATIONS

HOSTING TERMS AND CONDITIONS

- Attachment 1.3 to the Concession Contract -

1 Objective

In line with the Technical Requirements listed in the Attachment 1.1 of the Concession Contract, the NSP is responsible for the external connectivity between Directly Connected market participant Actors and the ESMIG Services and Applications Platform. Therefore, the NSP will install the needed communication lines and network components for routing and encryption of the ESMIG Services and Applications related traffic in the primary and secondary 4CB Hosting Sites in the two Regions. The ESMIG Services and Applications Sites are hosted by Banca d' Italia ("**BdI"**) and by Deutsche Bundesbank ("**BBk"**) for the Eurosystem.

2 Preparation of Installation of Components

The NSP will provide to the Eurosystem a written list of all the components, including the number of racks and switches it will provide, with all their needs in respect of space, power, climatic resources, environmental controls, network connection etc. which are necessary for the provision of the Connectivity Services and which will be installed in each data centre. The Eurosystem once approved the inventory proposed by NSP, will provide the necessary space, power, climatic resources etc. for the installation of the components in the ESMIG Services and Applications Sites. The NSP will provide such a list at the latest thirty (30) Business Days before the installation of any devices at the ESMIG Services and Applications Sites to allow BdI and BBk sufficient time to prepare the ESMIG Services and Applications Sites in accordance with the description laid down in the said note.

The NSP and the Eurosystem will agree on the organizational details of the installation of the components at each data centre on the basis of the list of components.

3 Provision and Installation of Components

3.1 Provision of Components

The NSP shall be responsible for the provision of the components of its NSP Infrastructure as notified by the NSP, in accordance with clause 2.

The NSP will provide the necessary components for the NSP's Solution for ESMIG Services and Applications Connectivity as detailed in the List of Components to the Eurosystem. The components will be provided at the data centres located at:

- Banca d'Italia [concrete location of primary site; concrete reserved area]
- Banca d'Italia [concrete location of secondary site; concrete reserved area]

- Deutsche Bundesbank [concrete location of primary site; concrete reserved area]
- Deutsche Bundesbank [concrete location of secondary site; concrete reserved area]

3.2 Installation of Components

The NSP will install the devices in the specific areas in the data centres at the ESMIG Services and Applications Sites where BdI's and BBk's own equipment is also in use as agreed between BdI / BBk and the Eurosystem. The NSP will perform the installation and setup of all necessary components and devices in its sole responsibility.

The connection to power supply and climatic control as well as the connection to the TARGET internal network will be based on conditions already in place at each data centre and used for BdI and BBk components. The NSP shall verify and declare the suitability of these conditions for the installation and use of the components installed by the NSP for the provision of the Connectivity Services.

4 Access to and Use of the Components

The NSP shall use remote access to its components installed on the ESMIG Services and Applications Sites. Physical access by the NSP's staff to the NSP's components on the Eurosystem's premises will be limited to the extent absolutely necessary. As far as physical access is necessary, it will be granted by the Eurosystem's on the basis of, and in accordance with the rules of access in place at each data centre. The NSP will be provided with these rules upon the installation of the components at the ESMIG Services and Applications Sites and declares to acknowledge these rules. Physical access to the TARGET Service Sites will be restricted to authorized personnel only. Access authorization must be requested by the NSP (information to be communicated: Name, Surname, Birth Date, ID number). Authorized personnel of the NSP shall always be escorted at the TARGET Service Sites by, and under the surveillance of, staff members of the hosting Institution (BdI or BBk) . Physical access to the TARGET Service Sites is possible on each day from 08:00 AM to 05:00 PM; access outside these hours is possible only in case of emergency.

The NSP will perform the end-to-end monitoring of the components (HW and SW) under its responsibility; NSP shall inform the ESMIG Services and Applications Operator in case of issue thereof in accordance with the applicable procedure(s) set out in the agreed Operations Manual (which includes also the escalation procedure).

The ESMIG Services and Applications Operator shall monitor the hosting Infrastructure (i.e. the connection to power supply and climatic control as well as the connection to the TARGET internal network) and, in the event of a natural disaster or other unforeseen circumstances of force majeure, as descripted in article 15 of the Concession Contract, which may adversely affect the continuity of the

hosting operations, the ESMIG Services and Applications Operator shall inform the NSP thereof in accordance with the applicable procedure(s) set out in the agreed Operations Manual (which includes also the escalation procedure).

The ESMIG Services and Applications Operator will inform the NSP reasonably in advance about any scheduled interventions or other activities that may adversely affect the hosting or operation of the NSP Infrastructure at the TARGET Sites.

Structural alterations within the BdI and BBk premises for the installation of the NSP's components which are necessary for the provision of the Connectivity Services will be limited to the extent absolutely necessary for the installation and use of the components If such structural alteration will be necessary, the NSP shall request the Eurosystem's consent to such alteration. The NSP shall bear the costs for such alteration, including any costs for returning the structure of the respective data centres to the original state upon the termination or expiration of the Concession Contract and / or these Hosting Terms and Conditions.

Each Party shall ensure, within its respective domain of responsibility under this Contract, that it does not adversely affect the operations of the other Party or of another NSP.

5 Security

The ESMIG Services and Applications Operator and the NSP shall agree on the security controls and arrangements, covering inter alia physical security, information security and confidentiality and application security. These controls and arrangements will be documented in the Operations Manual which is considered valid and enforceable only if expressly agreed by the Parties in writing.

6 Liability

The hosting of the NSP's equipment and components as specified above shall not be considered as a contract of safekeeping. The Eurosystem or the Eurosystem Central Bank hosting the NSP's equipment and components shall not have any obligation to safeguard, maintain or insure the NSP's equipment or any other obligation with regard to the NSP's equipment which is not expressly provided for in these Hosting Terms and Conditions or otherwise agreed by the Eurosystem and the NSP.

7 Governance, Change Management and Communications

The ESMIG Services and Applications Operator and the NSP shall agree the governance, change management and communications arrangements, which will underlie the relationship of the Parties in connection with the hosting of the NSP Infrastructure; these arrangements will be documented in the Operations Manual. Any change to this Contract shall only be valid and enforceable if expressly agreed by the Parties in writing.

8 Assistance

Without prejudice to either Party's obligations under this Contract, the Parties shall cooperate closely and transparently in order to enable each other to perform their respective obligations and responsibilities under this Contract in a timely and orderly manner. Each Party shall perform its obligations and responsibilities and exercise its rights and remedies under this Contract in good faith. Each Party shall, without undue delay, give the other Party notice of any facts, events, circumstances or other information that may reasonably be expected to materially affect its or the other Party's ability to perform its obligations and responsibilities under this Contract or, in the case of the NSP, the provision of the TARGET and ECMS Connectivity Services to the ESMIG Services and Applications Sites.

9 Holding of NSP infrastructure

Unless otherwise agreed by the Parties, the NSP shall hold the NSP infrastructure at the TARGET Sites in accordance with this Contract until the expiration or termination of this Contract. Upon the expiration or termination of this Contract, the NSP shall continue to hold the NSP Infrastructure at the TARGET Sites and shall use reasonable efforts to ensure an orderly transition of the connectivity services to the Eurosystem or to such other persons or entities designated by the Eurosystem to assume the provision of the Connectivity Services (the "Successor Network Service Provider") until such time as the Eurosystem has notified the NSP of the completion of the transition to the Successor Network Service Provider but in no event longer than two (2) years from the effective date of the termination or the expiration of this Contract (the "Transition Period"). During the Transition Period, the Network Service Provider shall, in particular, provide to the Eurosystem or the Successor Network Service Provider any information or documentation reasonably required to render the Connectivity Services.

Attachment 1.4 - Economic Offer (maximum prices)

Information section		
The MAXIMUM TOTAL SCORE accepted is 700.000. Bids whose TOTAL SCORE exceeds the maximum total score will be excluded.		
Prices with up to 6 decimals are accepted. Prices with more than 6 decimals will be rounded. If the seventh decimal digit is 4 or less, the price will be rounded down to the sixth decimal. If the seventh digit is 5 or more, the price will be rounded up to the sixth decimal.		
DATA VALUES 1 KB = 1024 bytes 1 MB = 1024 KB		
All prices are VAT excluded.		
Production - One-off fees		
A.1	Maximum price for installation of one single point of presence	
Maximum price for installation of a single point of presence (PoP). The standard connection includes a redundant configuration at a single Di.Co.A.'s site (i.e. installation with two incoming physical lines in a redundant set-up). Any costs related to necessary construction works at the Di.Co.A.'s premises are excluded. This service is shared between the production and the test and training traffic. Please refer to the technical requirements for more details.		
Price in Eur per PoP		**0.000000**
Weight of the parameter		**0.35**
A.1 score		**0.0000000000**
A.2	Maximum price for a minimum set of software and hardware components	
Maximum price for a minimum set of software (including the software needed to sign/verify the message payload) and hardware components required to access and utilise all the NSP's services in a secure and reliable way using the service A.1 (e.g. VPN, HSM, router …), and using a redundant set-up of that service. For the A2A mode, relevant software components shall allow communication with the Di.Co.A.'s middleware components using the Di.Co.A.'s TCP/IP network and at least one widely recognised, well documented and utilised communication protocol. For the U2A mode, relevant software components shall allow communication with the Di.Co.A.'s middleware using the Di.Co.A.'s TCP/IP network and the HTTPS protocol. Please refer to the technical requirements for more details.		
Price in Eur per Network interface		**0.000000**
Weight of the parameter		**1.45**
A.2 score		**0.0000000000**
A.3	Maximum price for a Di.Co.A.'s registration	
Maximum price for a Di.Co.A.'s registration with the NSP for all required services (e.g. for the purpose of the security services, messaging services, ...). Please refer to the technical requirements for more technical details.		
Price in Eur per registration		**10,000.000000**
Weight of the parameter		**0.28**
A.3 score		**2800.0000000000**
A.4	Maximum price for issuing one PKI certificate	
Maximum price for issuing one PKI certificate for securing traffic (A2A and U2A) Please refer to the technical requirements for more technical details.		
Price in Eur per PKI certificate		**0.000000**
Weight of the parameter		**3.32**
A.4 score		**0.0000000000**
D.1	Maximum price for a minimum set of software and hardware components (Low Volume access)	
Maximum price for a minimum set of software and hardware components required to access and utilise all the NSP's services in a secure and reliable way. For the U2A mode, relevant software components shall allow communication with the Di.Co.A.'s middleware using the Di.Co.A.'s TCP/IP network and the HTTPS protocol for Low volume. This service is shared between the production and the test and training traffic. Please refer to the technical requirements for more details.		

Price in EUR per network interface	**0.000000**	
Weight of the parameter	**20.77**	
D.1 score	**0.0000000000**	
D.2	Maximum price for a Di.Co.A.'s registration (Low Volume)	
Maximum price for a Di.Co.A.'s registration with the NSP for all required services (e.g. for the purpose of the security services, messaging services, ...) in case of Low volume access. Please refer to the technical requirements for more technical details.		
Price in EUR per registration	**10,000.000000**	
Weight of the parameter	**0.03**	
D.2 score	**300.0000000000**	
Production - Recurring fees		
B.1	Maximum yearly fee for utilisation and maintenance of a single PoP configuration	
Maximum yearly fee for utilisation and maintenance of a single point of presence configuration at a single Di.Co.A.'s site (refer to A.1). Please refer to the technical requirements for more technical details. This service is related to the A.1 service, which is shared between the production and the test and training traffic.		
Price in EUR per year per PoP maintenance contract	**2,500.000000**	
Weight of the parameter	**3.46**	
B.1 score	**8650.0000000000**	
B.2	Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components	
Maximum yearly fee for utilisation and maintenance of a minimum set of software (including the software needed to sign/verify the message payload) and hardware components required to access and utilise all the NSP's services (refer to A.2) including necessary upgrades of software and hardware components and replacement of failing hardware components upon a fault report by a Di.Co.A. or a fault detection by the NSP. Excluding any costs related to a Di.Co.A.'s expenses related to the hosting of these software and hardware components. Please refer to the technical requirements for more technical details.		
Price in EUR per year per network interface maintenance contract	**7,500.000000**	
Weight of the parameter	**1.87**	
B.2 score	**14025.0000000000**	
B.3	Maximum yearly fee for the customer support service	
Maximum yearly fee for the customer support service for participants with A2A access. Please refer to the technical requirements for more technical details. This service is shared between the production and the test and training environments.		
Price in EUR per year per service support contract	**4,250.000000**	
Weight of the parameter	**2.22**	
B.3 score	**9435.0000000000**	
B.4	Maximum yearly fee for PKI maintenance	
Maximum yearly fee for maintenance (including renewal) of one already issued PKI certificate for securing traffic (A2A and U2A). Please refer to the technical requirements for more technical details.		
Price in EUR per year per PKI certificate	**75.000000**	
Weight of the parameter	**39.87**	
B.4 score	**2990.2500000000**	
E.1	Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components (Low Volume)	

Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components required to access and utilise all the NSP's services (refer to D.1) including necessary upgrades of software and hardware components and replacement of failing hardware components within 48 hours upon a fault report by a Di.Co.A. or a fault detection by the NSP in case of Low volume access.
Excluding any costs related to a Di.Co.A.'s expenses related to the hosting of these software and hardware components.
Please refer to the technical requirements for more technical details.

Price in EUR per year per network interface maintenance contract	2,000.000000
Weight of the parameter	4.00
E.1 score	8000.0000000000

E.2	Maximum yearly fee for the customer support service (Low Volume access)

"Maximum yearly fee for the customer support service in case of Low volume access.
This service is related to the D.1 service, which is shared between the production and the test and training traffic.
Please refer to the technical requirements for more technical details.

Price in EUR per year per service support contract	0.000000
Weight of the parameter	10.00
E.2 score	0.0000000000

Production - Communication fees

C.1	Maximum price for transmission of a single message via the store-and-forward channel

Maximum price for transmission of a single message (of max. 32 kB) in A2A mode via the store-and-forward channel, including the delivery notification required in case of delivery failure, and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that message.
Please refer to the technical requirements for more technical details.

Price in EUR per A2A store-and-forward message	0.007000
Weight of the parameter	5,676,938.58
C.1 score	39738.5700600000

C.2	Maximum price for transmission of a single request-response via the real-time channel

Maximum price for transmission of a single request-response (of max. 32 kB request and max. 32 kB response) in A2A mode via the real-time channel, including all positive/negative technical acknowledgements required to finalise the sending and receipt of the request and the response.
Please refer to the technical requirements for more technical details.

Price in EUR per A2A real-time request-response exchange	0.007000
Weight of the parameter	19,910.65
C.2 score	139.3745500000

C.3	Maximum price for transmission of each 1 MB of a file or its part thereof via the store-and-forward channel

Maximum price for transmission of each 1 MB of a file or its part thereof (of max. 32 MB) in the A2A mode via the store-and-forward channel, including the delivery notification failure in case of a delivery failure and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that file.
Please refer to the technical requirements for more technical details.

Price in EUR per MB transmitted via A2A store-and-forward files	1.920000
Weight of the parameter	2,883.32
C.3 score	5535.9744000000

C.4	Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel

Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel.
Please refer to the technical requirements for more technical details.

Price in EUR per 1 MB transmitted in U2A	0.500000
Weight of the parameter	110.13
C.4 score	55.0650000000

C.5	TIPS - Maximum price for transmission of a message (of max. 10 kB) in A2A mode via the instant message channel

Maximum price for transmission of a TIPS message (of max. 10 kB) in A2A mode via the instant message channel, including all positive/negative notify and technical acknowledgements required to finalise the sending of the message. **The price cap for this item is € 0,0005. The price cell is set to accept prices up to the price cap. Bids where the price for this item exceeds the price cap will be excluded.** (Please refer to the technical requirements for more details.)								
Price in EUR per 1 A2A instant message exchange		**0.000500**						
Weight of the parameter		**27,621.37**						
C.5 score		**13.8106850000**						
C.6	TIPS - Report outgoing only - Maximum price for transmission of each 1 MB of a file or its part thereof via the store-and-forward channel							
TIPS - Report outgoing only - Maximum price for transmission of each 1 MB of a file or its part thereof (of max. 32 MB) in the A2A mode via the store-and-forward channel, including the delivery notification failure in case of a delivery failure and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that file. Please refer to the technical requirements for more technical details.								
Price in EUR per MB transmitted via A2A store-and-forward files		**1.920000**						
Weight of the parameter		**2,093.41**						
C.6 score		**4019.3472000000**						
C.7	DEP- A2A Message retrieval							
DEP- A2A Message retrieval. Please refer to the technical requirements for more technical details.								
Price in EUR per message		**0.038000**						
Weight of the parameter		**35,288.90**						
C.7 score		**1340.9782000000**						
F.1	Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel (Low Volume access)							
Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel for Low volume access. Please refer to the technical requirements for more technical details.								
Price in EUR per 1 MB transmitted in U2A		**0.500000**						
Weight of the parameter		**71.51**						
F.1 score		**35.7550000000**						
Test and Training - One-off fees								
A.2 T&T	Maximum price for a minimum set of software and hardware components							
Maximum price for a minimum set of software (including the software needed to sign/verify the message payload) and hardware components required to access and utilise all the NSP's services in a secure and reliable way using the service A.1 (e.g. VPN, HSM, router …), and using a redundant set-up of that service. For the A2A mode, relevant software components shall allow communication with the Di.Co.A.'s middleware components using the Di.Co.A.'s TCP/IP network and at least one widely recognised, well documented and utilised communication protocol. For the U2A mode, relevant software components shall allow communication with the Di.Co.A.'s middleware using the Di.Co.A.'s TCP/IP network and the HTTPS protocol. Please refer to the technical requirements for more details.								
Price in Eur per Network interface		**0.000000**						
Weight of the parameter		**0.15**						
A.2 T&T score		**0.0000000000**						
A.3 T&T	Maximum price for a Di.Co.A.'s registration							
Maximum price for a Di.Co.A.'s registration with the NSP for all required services (e.g. for the purpose of the security services, messaging services, ...). Please refer to the technical requirements for more technical details.								
Price in Eur per registration		**0.000000**						
Weight of the parameter		**0.03**						
A.3 T&T score		**0.0000000000**						
A.4 T&T	Maximum price for issuing one PKI certificate							
Maximum price for issuing one PKI certificate for securing traffic (A2A and U2A). Please refer to the technical requirements for more technical details.								
Price in Eur per PKI certificate		**0.000000**						

Weight of the parameter		0.33
A.4 T&T score		0.0000000000
D.2 T&T	Maximum price for a Di.Co.A.'s registration (Low Volume access)	
Maximum price for a Di.Co.A.'s registration with the NSP for all required services (e.g. for the purpose of the security services, messaging services, ...) in case of Low volume access. Please refer to the technical requirements for more technical details.		
Price in EUR per registration		0.000000
Weight of the parameter		0.01
D.2 T&T score		0.0000000000
Test and training - Recurring-fixed fees		
B.2 T&T	Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components	
Maximum yearly fee for utilisation and maintenance of a minimum set of software (including the software needed to sign/verify the message payload) and hardware components required to access and utilise all the NSP's services (refer to A.2) including necessary upgrades of software and hardware components and replacement of failing hardware components upon a fault report by a Di.Co.A. or a fault detection by the NSP. Excluding any costs related to a Di.Co.A.'s expenses related to the hosting of these software and hardware components. Please refer to the technical requirements for more technical details.		
Price in EUR per year per network interface maintenance contract		0.000000
Weight of the parameter		0.19
B.2 T&T score		0.0000000000
B.4 T&T	Maximum yearly fee for PKI maintenance	
Maximum yearly fee for maintenance (including renewal) of one already issued PKI certificate for securing traffic (A2A and U2A). Please refer to the technical requirements for more technical details.		
Price in EUR per year per PKI certificate		75.000000
Weight of the parameter		3.99
B.4 T&T score		299.2500000000
E.1 T&T	Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components (Low Volume access)	
Maximum yearly fee for utilisation and maintenance of a minimum set of software and hardware components required to access and utilise all the NSP's services (refer to D.1) including necessary upgrades of software and hardware components and replacement of failing hardware components within 48 hours upon a fault report by a Di.Co.A. or a fault detection by the NSP in case of Low volume access. Excluding any costs related to a Di.Co.A.'s expenses related to the hosting of these software and hardware components. Please refer to the technical requirements for more technical details.		
Price in EUR per year per network interface maintenance contract		0.000000
Weight of the parameter		0.40
E.1 T&T score		0.0000000000
Test and training - Communication fees		
C.1 T&T	Maximum price for transmission of a single message via the store-and-forward channel	
Maximum price for transmission of a single message (of max. 32 kB) in A2A mode via the store-and-forward channel, including the delivery notification required in case of delivery failure, and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that message. Please refer to the technical requirements for more technical details.		
Price in EUR per A2A store-and-forward message		0.003500
Weight of the parameter		567,693.86
C.1 T&T score		1986.9285100000
C.2 T&T	Maximum price for transmission of a single request-response via the real-time channel	

Maximum price for transmission of a single request-response (of max. 32 kB request and max. 32 kB response) in A2A mode via the real-time channel, including all positive/negative technical acknowledgements required to finalise the sending and receipt of the request and the response. Please refer to the technical requirements for more technical details.								
Price in EUR per A2A real-time request-response exchange	0.003500							
Weight of the parameter	1,991.06							
C.2 T&T score	6.9687100000							
C.3 T&T	Maximum price for transmission of each 1 MB of a file or its part thereof via the store-and-forward channel							
Maximum price for transmission of each 1 MB of a file or its part thereof (of max. 32 MB) in the A2A mode via the store-and-forward channel, including the delivery notification failure in case of a delivery failure and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that file. Please refer to the technical requirements for more technical details.								
Price in EUR per MB transmitted via A2A store-and-forward files	0.960000							
Weight of the parameter	288.33							
C.3 T&T score	276.7968000000							
C.4 T&T	Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel							
Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel. Please refer to the technical requirements for more technical details.								
Price in EUR per 1 A2A instant message exchange	0.250000							
Weight of the parameter	11.01							
C.4 T&T score	2.7525000000							
C.5 T&T	TIPS - Maximum price for transmission of a message (of max. 10 kB) in A2A mode via the instant message channel							
Maximum price for transmission of a TIPS message (of max. 10 kB) in A2A mode via the instant message channel, including all positive/negative notify and technical acknowledgements required to finalise the sending of the message. **The price cap for this item is € 0,00025. The price cell is set to accept prices up to the price cap. Bids where the price for this item exceeds the price cap will be excluded.** (Please refer to the technical requirements for more details.)								
Price in EUR per 1 A2A instant message exchange	0.000250							
Weight of the parameter	2,762.14							
C.5 T&T score	0.6905350000							
C.6 T&T	TIPS - Report outgoing only - Maximum price for transmission of each 1 MB of a file or its part thereof via the store-and-forward channel							
TIPS - Report outgoing only - Maximum price for transmission of each 1 MB of a file or its part thereof (of max. 32 MB) in the A2A mode via the store-and-forward channel, including the delivery notification failure in case of a delivery failure and including all positive/negative technical acknowledgements required to finalise the sending and receipt of that file. Please refer to the technical requirements for more technical details.								
Price in EUR per MB transmitted via A2A store-and-forward files	0.960000							
Weight of the parameter	209.34							
C.6 T&T score	200.9664000000							
C.7 T&T	DEP- A2A Message retrieval							
DEP- A2A Message retrieval. Please refer to the technical requirements for more technical details.								
Price in EUR per message	0.019000							
Weight of the parameter	3,528.89							
C.7 T&T score	67.0489100000							
F.1 T&T	Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel (Low Volume access)							
Maximum price for the transmission of each 1 MB volume or its part thereof via the U2A channel for Low volume access. Please refer to the technical requirements for more technical details.								
Price in EUR per 1 MB transmitted in U2A	0.250000							
Weight of the parameter	7.15							
F.1 score	1.7875000000							

The MAXIMUM TOTAL SCORE accepted is 700.000. Bids whose TOTAL SCORE exceeds the maximum total score will be excluded.								
TOTAL SCORE		99,922.3149600000						

Saskia Devolder (Signature)

Digitally signed by Saskia Devolder (Signature)
Date: 2019.03.25 18:01:12 +01'00'