Il presente documento è conforme all'originale contenuto negli archivi della Banca d'Italia

Firmato digitalmente da

Laura Studer

T2S EXTERNAL NETWORKS

TECHNICAL REQUIREMENTS

- Attachment 1 to the Licence Agreement -

TABLE OF CONTENT

1 Technical and operational criteria

The general architecture of the T2S Platform is set out in the GTD[1] document. It describes the platform and defines very high-level requirements for the Connectivity Services required for the remote access to the T2S Platform by its end users.

This chapter presents detailed technical criteria for the Solution, as defined in Art. 4.1 of the Agreement regarding a Licence for the Provision of Network and Connectivity Services for the TARGET2 Securities System ("**Licence Agreement**" or "**LA**").

1.1 General service description

The T2S infrastructure is deployed over three Regions. Two Regions (Region 1 – Banca d'Italia – and Region 2 - Deutsche Bundesbank) host the T2S core business applications (e.g. instructions settlement). The third Region (Banque De France – Region 3) hosts other T2S functions (e.g. Legal Archiving and Statistical Reports provisioning). To allow continuous operations without service interruptions (e.g. in the case of a power outage), each of the three regions consists of a primary and a secondary site which run independently from each other. Each site is established as a high availability data centre (e.g. redundant connections for power supply and use of Uninterruptible Power Supply).

While Region 1 is hosting the T2S production environment, Region 2 is hosting the T2S test & training environment. Regular swaps ("rotation") ensure proper precaution against regional disaster and keep technical and operational staff skilled in each region. Rotation activities in Regions 1 and 2 do not affect the systems in Region 3.

Technical infrastructure

Reference ID	T2S.UC.TC.11010

The Network Services Provider (NSP) shall deliver a technical infrastructure and necessary software components required to exchange in a secure and reliable manner messages and files between its Directly Connected T2S Actors and the T2S Platform.

Delivery point for Connectivity Services

Reference ID	T2S.UC.TC.11050

The NSP shall deliver Connectivity Services to each of the T2S sites in Region 1 and Region 2. The NSP shall not deliver Connectivity Services directly to Region 3. In order to reach T2S functions in Region 3 the Directly Connected T2S Actors will use the NSP Connectivity Services to reach Region 1 or Region

[1] General Technical Design document – for more detail please refer to the GTD document published on the T2S website (http://www.ecb.int/paym/t2s/about/keydocs/html/index.en.html)

2, and next T2S will forward their requests through the T2S internal network (4CBNet) to reach the T2S functions in Region 3.

The NSP shall deliver Connectivity Services to its Directly Connected T2S Actors.

Location of equipments

Reference ID	T2S.UC.TC.11060

The NSP shall install inside the Eurosystem premises (Region1 and Region2) only a minimal set of necessary devices to deliver its Connectivity Services to the T2S Platform i.e. only routers and VPN devices as illustrated on the Figure 1[2].

The NSP shall connect its equipment to the respective T2S communication endpoints at each T2S site in Region 1 and Region 2.

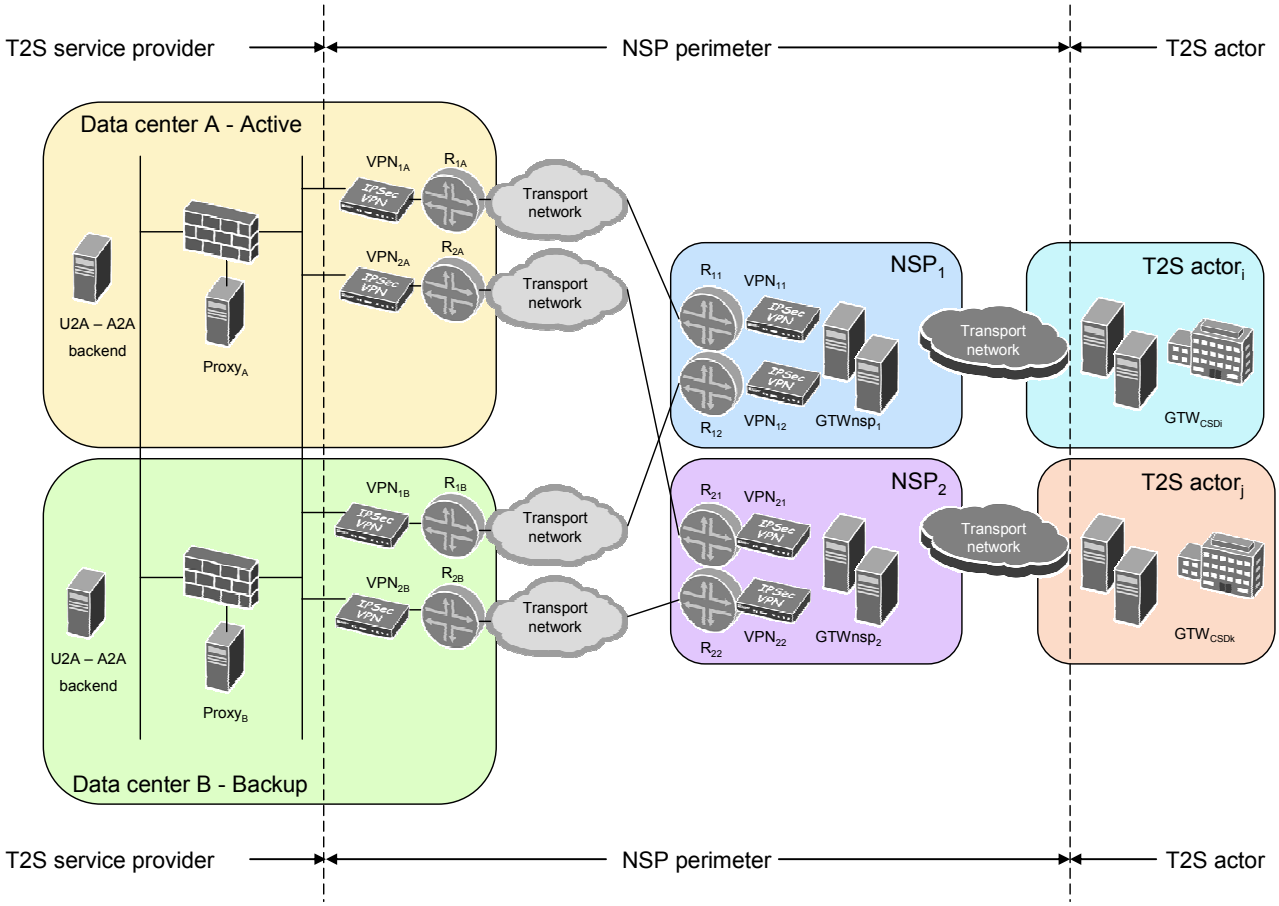

Figure 1 – Location of equipments and NSP demarcation point at the T2S Platform sites

(on this Figure only one Region is shown,

the same configuration shall be implemented on the second one)

Hosting agreement

Reference ID	T2S.UC.TC.11065

[2] Location of equipments on the NSP and its Directly Connected T2S Actor site shown on the Figure 1 have to be considered only as an example.

Terms and Conditions for hosting provisioning are detailed in attachment 3 to the license agreement

The boundaries of responsibility

Reference ID	T2S.UC.TC.11070

The demarcation line defining the responsibilities between T2S and the NSP shall be the interface between the NSP's VPN devices and the T2S Platform's safety devices provided by the NSP in a patch panel as described in section 2.1.2 Service Requirements for Network Services below and as set out in the Figure 1 above.

The NSP and its Directly Connected T2S Actors shall agree on the demarcation line, which shall clearly define areas of responsibility between them.

These two demarcation lines shall define the boundary of responsibility of the NSP. The NSP shall be fully responsible and liable for all services it offers to its Directly Connected T2S Actors and T2S within this boundary.

Chain of trust relationship

Reference ID	T2S.UC.TC.11080

The NSP shall be responsible for ensuring that the functional and non-functional requirements expressed in this document (e.g. performance, security) are satisfied also inside the NSP domain and in the relation between the NSP and its Directly Connected T2S Actors (chain of trust relationship).

Independence of interfaces on T2S and Directly Connected T2S Actors' sites

Reference ID	T2S.UC.TC.11090

The NSP shall ensure that the technical solution it adopts for the interface with the T2S Platform does not affect technical solutions adopted for the interface with its Directly Connected T2S Actors.

The NSP and its Directly Connected T2S Actors shall agree on and establish a connectivity interface on their site.

The two interfaces shall be technically decoupled by means of the NSP's services, in the sense that technical choices on one interface shall not affect the other.

Single interface on the T2S site

Reference ID	T2S.UC.TC.11100

The NSP shall comply with the T2S interface as described in sections 3.2 and 3.3.

T2S will rely on middleware and/or gateway functions[3] to link the T2S application with the NSP's Connectivity Services. The NSP's equipment will not be directly connected to the T2S middleware. In order to preserve security, the T2S Platform will employ sanitisation devices (XML firewall, reverse proxies and/or gateways procured, administered and managed by the Eurosystem).

Interface on the Directly Connected T2S Actor's site

Reference ID	T2S.UC.TC.11110

The NSP shall agree with its Directly Connected T2S Actors on the design and implementation of the interface on their site (i.e. is out of the scope of this document). Such interface shall, however, not limit compliance with the T2S security requirements, and shall not affect by any means the interface on the T2S Platform site (i.e. shall not require any special handling on the T2S site).

Security of interface at Directly Connected T2S Actor's site

Reference ID	T2S.UC.TC.11115

The NSP shall deliver to the Eurosystem a detailed description of security aspects of all offered user interfaces in order for Eurosystem to check their compliance with the T2S security requirements.

Monitoring facilities

Reference ID	T2S.UC.TC.11130

The NSP shall provide to the Eurosystem the facilities necessary for monitoring all technical operations that will be agreed and described in the "Operational manual", which are under the NSP's responsibility.

Time synchronisation

Reference ID	T2S.UC.TC.11140

In order to make the data exchange time consistent the NSP shall synchronise the date-time of his gateways with the same date-time source adopted by the T2S Platform. The synchronisation interval shall be one hour. The official time of T2S system will be the ECB time, i.e. the local time at the seat of the ECB.

[3] For more details please refer to the GTD document published on the T2S website (http://www.ecb.int/paym/t2s/about/keydocs/html/index.en.html)

2 Network Connectivity

2.1 Physical Connectivity Services

The NSP offers a single logical service which can be basically seen as two different Wide Area Networks (WAN), the first between the T2S Sites and the NSP's sites and the second between NSP's sites and Directly Connected T2S Actor's sites. The first one is qualified and quantified through the following requirements. The second one is just classified in this document. The NSP shall then specify and describe a portfolio offer to connect the Directly Connected T2S Actors.

2.1.1 Interface with the T2S Pplatform (between T2S and NSP)

T2S has two sites which are hosted in Region 1 in Rome, Italy and two sites which are hosted in Region 2 in Frankfurt am Main, Germany (together the "**T2S Sites**"). The NSP shall connect all four sites to its Network and provide the number of WAN links required to connect all the four T2S Sites to its sites. The following requirements describe what each of the above links has to match.

Requirements are classified by layer in the classification of the ISO Open System Interconnection model (OSI). Layer 1 and 2 requirements apply link-to-link, i.e. between the two WAN link endpoints. All upper requirements (layer 3 to 7) apply end-to-end, i.e. between two service demarcation lines.

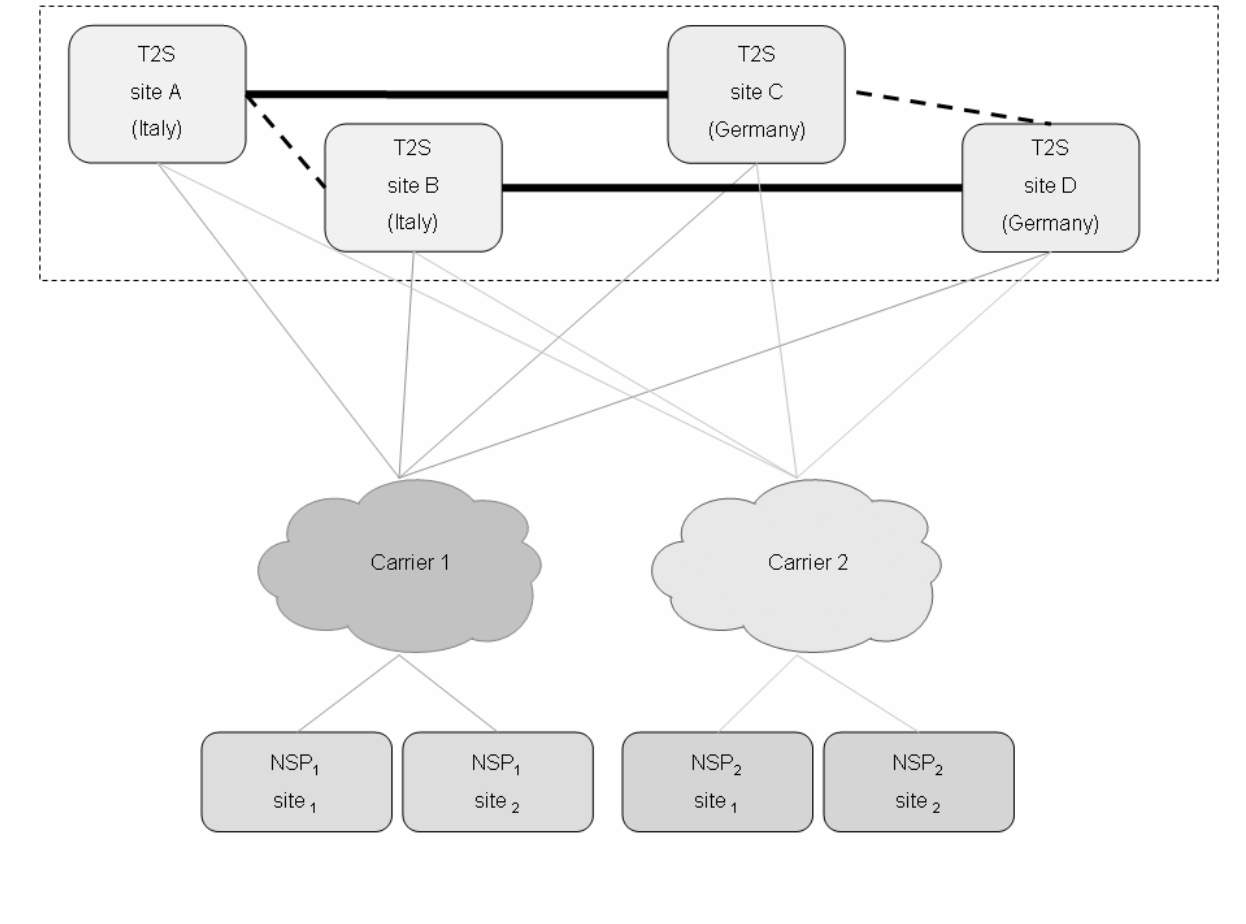

Figure 2 – Links between NSP and T2S Platform sites

The picture describes the connections, if two network services providers are licensed to provide Connectivity Services to T2S. WAN lines between the site A,B,C,D are not in the scope of the Selection Procedure. Due to the fact, that the T2S Sites within a Region are inter connected (pictured in black dashed above), this layer 2 connections could be used for contingency purposes. However the usage of these links is under the control of the Eurosystem.

Layer 1 requirement - **T2S sites served by WAN links**

Reference ID	T2S.UC.TC.20100

The four T2S Sites are served by the WAN links of NSP. The NSP shall insure that all sites which it uses to fulfil the overall Service Availability requirements are connected to all four T2S Sites.

Layer 1 requirement - **Link bandwidth**

Reference ID	T2S.UC.TC.20105

Each link has an available maximum bandwidth of 1Gbps.

Layer 1 requirement - **Link delay**

Reference ID	T2S.UC.TC.20115

Each link has a one way delay of maximum 40 msec.

Layer 1 requirement - **Link recovery time**

Reference ID	T2S.UC.TC.20120

Any link is able to recover a single failure within 50 msec.

Layer 1 requirement - **Link Bit Error Rate (BER).**

Reference ID	T2S.UC.TC.20125

Each link has a Bit Error Rate (BER) less or equal to 10^{-14}.

Layer 1 requirement - **Regional link service availability**

Reference ID	T2S.UC.TC.20130

Two links within the same region (regional links) have an availability of 99.9%.

Layer 1 requirement - **Link port specification (1Gbps Ethernet local interface)**

Reference ID	T2S.UC.TC.20135

The NSP delivers to T2S the connectivity service via network equipments having 1 Gigabit Ethernet ("**GbE**") ports, either IEEE 802.3ab (1000Base-T) with RJ-45 connectors or IEEE 802.3 clause 38 (aka IEEE 802.3z) (1000Base-SX) with LC connectors. The duplex mode shall be full duplex. Auto-negotiation shall be disabled.

Layer 1 requirement - **Path diversification**

Reference ID	T2S.UC.TC.20140

Paths from the site to local POPs are served by local loops. Each local loop has a diversified path from the site to the POP. Paths are also diversified from the POP to backbone and throughout the whole path across the backbone itself.

Layer 1 requirement - **All links from the same NSP are provided by a single network provider**

Reference ID	T2S.UC.TC.20145

The NSP shall be responsible for all links between the four T2S Sites and the NSP's sites. Thereby the NSP has to guarantee the full path diversification end-to-end, by knowing and maintaining all physical paths.

Layer 2 requirement - **Layer 2 connectivity at continental distances**

Reference ID	T2S.UC.TC.20150

Links are able to transport layer 2 protocols end-to-end. A multicast or a broadcast transmitted on one end of the link is received on the other end of the link.

Layer 3 requirement - **IPv4**

Reference ID	T2S.UC.TC.20155

Internet Protocol (IP) version 4 (IPv4) protocol is used between the T2S, Directly Connected T2S Actors and the NSP.

Layer 3 requirement - **IP addressing schema**

Reference ID	T2S.UC.TC.20160

The NSP has to use an IP address range which is "public" in terms of RFC1918. Address Allocation for Private Internets, i.e. 10.0.0.0 - 10.255.255.255 (10/8 prefix), 172.16.0.0 - 172.31.255.255 (172.16/12 prefix), 192.168.0.0 - 192.168.255.255 (192.168/16 prefix).

Layer 3 requirement - **Confidentiality and integrity of data in transit across the public soil**

Reference ID	T2S.UC.TC.20165

The NSP takes appropriate measures and installs sufficient networking facilities to protect all data in transit between T2S Sites and the NSP's sites and between the NSP sites and the Directly Connected T2S Actor's sites. An example of an "appropriate measure" is an IPSec VPN tunnel. All traffic must be encrypted and authenticated.

Only authenticated parties shall be able to access the Network and the T2S Services.

The links between the NSP and the T2S Sites shall be closed to traffic from other sources or to other destinations than authenticated parties.

Layer 3 requirement – **Data compression**

Reference ID	T2S.UC.TC.20170

Data shall be compressed using market standard algorithms.

Layer 3 requirement – **Static Routing**

Reference ID	T2S.UC.TC.20175

Between NSP and T2S only static routes will be used.

Layer 4 requirement - **Load balancing among the two NSP links within a region.**

Reference ID	T2S.UC.TC.20180

For contingency reasons load balancing of TCP sessions across the two links within the same region (where "region" is site A + site B or site C + site D) shall be possible. Before its actual usage, an agreement between the NSP and the Eurosystem must be negotiated and concluded in good faith at the Eurosystem's request.

Layer 4 requirement – **TCP/UDP.**

Reference ID	T2S.UC.TC.20181

End-to-end TCP and UDP communication shall be possible between T2S and the Directly Connected T2S Actors. The set of these transport protocols may be expanded in the future.

Layer 7 requirement - **Domain Name System**

Reference ID	T2S.UC.TC.20185

The NSP shall offer a DNS service for hostname resolution. This service shall support forwarding of DNS requests for T2S hostnames to (authoritative) name servers of T2S. The NSP shall provide for a unique domain name.

2.1.2 Service Requirements for Network Services

Service requirements - **One face to the customer**

Reference ID	T2S.UC.TC.20300

From a service management perspective the NSP is a single interface to T2S. All links share the same Service Level Agreement (SLA), same Network Operations Centre (NOC), and same Service Desks (SD).

Service requirements - **Each site is able to work autonomously**

Reference ID	T2S.UC.TC.20301

The NSP has to support that the link to each single T2S site is able to handle the whole traffic. In the case of a site failure within a region the link to the remaining T2S site shall handle the whole traffic.

Service requirements - **Demarcation line between the NSP and T2S**

Reference ID	T2S.UC.TC.20305

The NSP shall deliver at the four T2S sites one or more network devices (for example DWDM + router + VPN or DWDM + VPN), which present a 1GbE interface to the T2S Platform. The NSP delivers this interface in a patch panel defining the demarcation line between NSP and T2S.

2.1.3 Interface with the users (between NSP and Directly Connected T2S Actors)

NSP's sites are then interconnected to Directly Connected T2S Actors via a transport network, which is the interface with the end users. The following diagram pictures the two transport networks, represented as clouds, interconnecting NSP's sites with Directly Connected T2S Actors' sites.

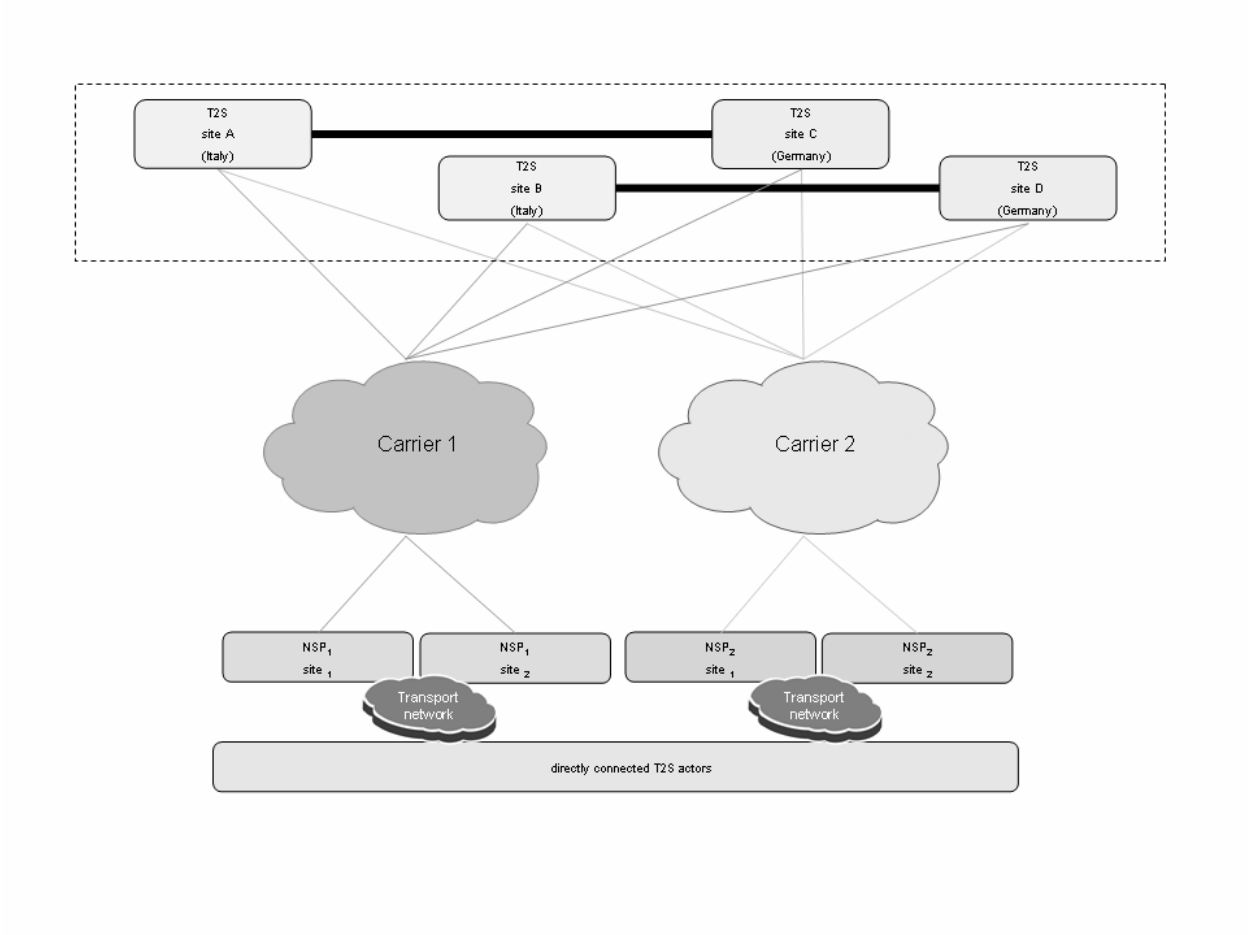

Figure 3 – Interconnections between NSP and T2S sites

The NSP shall decide on the connectivity details of the transport network offered to the Directly Connected T2S Actors insofar as they are not determined by the Licence Agreement or any Attachment thereto, including these Technical Requirements.

3 Messaging services

This chapter details the requirements for NSP to comply with the T2S Platform in order to manage the A2A and U2A data flows.

3.1 High Level Description of the Services

The T2S Platform can be accessed by the Directly Connected T2S Actors in two modes: "application to application" (A2A) and "user to application" (U2A).

In the A2A mode, business data will be exchanged as a "message" or a "file". A "message" is a data structure containing a financial instruction or information based on the XML format (ISO20022 standard), while a "file" is a data structure containing one or more messages in the XML format.

For the A2A mode, the T2S Platform communicates with the Directly Connected T2S Actors with two transfer modes: the "real-time" and the "store-and-forward". Both messages and files can be exchanged via the "real-time" and the "store-and-forward".

- The "real-time" message and file transfer requires that both parties, a sender and a receiver, are available at the same time to exchange messages or files. In the case of an unavailability of the receiver no retry mechanism is foreseen.
- The "store-and-forward" message or file transfer enables a sender to transmit messages or files even when a receiver is unavailable. In the case of a temporary unavailability of the receiver, the NSP stores messages and files and delivers them as soon as the receiver becomes available again.

For the "real-time" transfer the T2S Platform will exchange messages and files only in the "push" mode. The "push" mode refers to the originator of a message or file pushing it to the final receiver.

In the context of the U2A specification, Directly Connected T2S Actors will access the T2S application via a browser using the HTTPs protocol. Although it is expected that the U2A will be utilised mainly to inquire T2S data, it can be used also to submit updates.

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

Reference ID	T2S.UC.TC.30010

The NSP shall offer the data exchanging services in the A2A and the U2A modes to all its Directly Connected T2S Actors and to the T2S Platform.

The "real-time" and "store-and-forward" transfers

Reference ID	T2S.UC.TC.30020

The NSP shall offer exchange of messages and files in the A2A mode via the "real-time" and the "store-and-forward" transfers to all its Directly Connected T2S Actors and to the T2S Platform.

Real-time timeout management and flexibility

Reference ID	T2S.UC.TC.30030

The NSP shall manage the timeout for real-time message exchange. This timeout, with an initially requested value of 60 seconds, could be changed in flexible way successively. The timeout will occur if the exchange of the message will not be completed in the timeout timeframe duration.

The "application to application" (A2A) mode

Reference ID	T2S.UC.TC.30040

The NSP shall support exchange of messages in the A2A mode via the "real-time" and "store-and-forward" transfers in the "push" mode only.

The NSP shall support exchange of files in the A2A mode via the "real-time" and "store-and-forward" transfer in the "push" mode only.

The "user to application" (U2A) mode

Reference ID	T2S.UC.TC.30050

The NSP shall support the U2A mode interactions through the web access (HTTPs protocol) from Directly Connected T2S Actor to the T2S Platform.

3.2 Application to Application (A2A) Mode Requirements

The following section describes the requirements for the A2A mode in the scope of the data exchange between the T2S Platform and the NSP. The NSP shall choose appropriate procedures to handle the data exchange between it and Directly Connected T2S Actors.

3.2.1 Data Exchange Protocol (DEP)

This paragraph describes the "Data Exchange Protocol" (DEP in the following) used to handover the data between the T2S Platform and the NSP. It is a protocol that exploits the functionality of transport layer service.

DEP is a protocol that foresees a list of primitives for managing the exchange of messages and files between the T2S Platform and the NSP. In general, it is based on an "Exchange Header" for exchanging information with the NSP, and a set of rules to follow for the exchanging of messages and files.

DEP usage for messages and files

Reference ID	T2S.UC.TC.30060

The NSP shall manage message /files exchanged with the T2S Platform in the following format:

- The Exchange Header section contains all "service information" needed for the transport layer, exchanged between the NSP and the T2S Platform 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 the sender or receiver. The business layer does not fall into the scope of this document.

DEP maintenance and evolution

Reference ID	T2S.UC.TC.30065

The NSP shall support the Eurosystem staff in the maintenance and evolution of the DEP protocol. Updates to the protocol will be agreed upon between NSP and Eurosystem.

3.2.2 Interface Description

In this chapter the interface between the T2S Platform and the NSP is described, it should be not confused with the “Interface” domain described in the T2S General Functional Specification (GFS) document.

3.2.2.1 General Requirements

A2A message and file size limitations

Reference ID	T2S.UC.TC.30070

The NSP shall 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	n.a.	32 KB
File	>32KB	32 MB

Table 2 – size limit of messages and files

A2A message and file size flexibility

Reference ID	T2S.UC.TC.30075

The NSP shall be able to implement changes to the values at the Eurosystem's request within a reasonable period of time agreed with the Eurosystem.

A2A message and file size management

Reference ID	T2S.UC.TC.30080

The NSP shall reject as soon as possible any message or file that is not in the allowed size range.

The NSP shall reject the operation by sending back to the originator a negative acknowledgement message with the explanation of the error (e.g. "Message or file size out of allowed range.").

No message/file duplication

Reference ID	T2S.UC.TC.30085

The NSP shall deliver messages and files once, and only once.

Message against file priority

Reference ID	T2S.UC.TC.30090

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

3.2.2.2 A2A WebSphere MQ Requirements.

To manage A2A services, the NSP shall connect to the WebSphere MQ ("**WMQ**") architecture of T2S Platform. The NSP shall comply with the following requirements.

WebSphere MQ product version

Reference ID	T2S.UC.TC.30095

The NSP shall connect to the T2S Sites using the IBM WebSphere Message Queuing ("**MQ**") transport protocol. The NSP shall use a WMQ product version compliant with the WMQ version adopted by T2S Platform.

WebSphere MQ channels

Reference ID	T2S.UC.TC.30100

At least one WMQ channel shall be set up for each kind of flows for each NSP:

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

WebSphere MQ channels SSL connection

Reference ID	T2S.UC.TC.30105

Channel connections shall be secured with usage of SSL certificates exchanged by T2S Platform and NSP. SSL certificates for WMQ channel will be distributed by the Eurosystem.

WebSphere MQ channels type

Reference ID	T2S.UC.TC.30110

The NSP can choose to connect to the T2S Platform WMQ in server-server (channels SDR/RCVR located at both site) or client-server mode (channels SVRCONN located at The T2S Sites). The name of channels shall follow the T2S naming convention.

WebSphere MQ message queues

Reference ID	T2S.UC.TC.30115

A set of queues for each specific traffic flow shall be set up for incoming and outgoing traffic. The name of queues shall follow the T2S naming convention. The NSP shall present a proposal on the WMQ configuration that has to be accepted by the Eurosystem.

WebSphere MQ messages management – load balancing

Reference ID	T2S.UC.TC.30120

The NSP shall manage the load balancing across WMQ queues for incoming messages/files. The load balancing mechanism shall be based in a round-robin across the queues dedicated to each kind of flow.

WebSphere MQ messages management – grouping and segmentation

Reference ID	T2S.UC.TC.30125

The NSP shall manage the WMQ message grouping and segmentation if requested by the Eurosystem.

WebSphere MQ message description section – CCSID

Reference ID	T2S.UC.TC.30130

The NSP shall handle the WMQ message description section field CCSID based on the one used by T2S Platform (character set name: UTF-8, CCSID: 1208).

WebSphere MQ message description section – MsgType

Reference ID	T2S.UC.TC.30135

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

WebSphere MQ message description section – Format

Reference ID	T2S.UC.TC.30140

The NSP shall manage the WMQ messages having the following Format: String. 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.

WebSphere MQ additional headers – RFH2

Reference ID	T2S.UC.TC.30145

The NSP shall support additional WMQ standard headers in received messages (e.g. the additional RFH2 header structure RFH2.s) and ignore any contained information.

WebSphere MQ message structure

Reference ID	T2S.UC.TC.30150

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 T2S Platform when a message/file is exchanged:

- MQMD.MsgType: request/reply/report/datagram values are allowed;
- MQMD.Format: e.g. MQFMT_NONE;
- MQMD.Enconding;
- MQMD.CodeCharacterSetId;
- MQMD.Report option: set to the value MQRO_PAN+MQRO_NAN;
- MQMD.Expiry: this field could be used only for real-time traffic setting the value equal to the real-time time-out timeframe (e.g. 60 seconds). In this way it is possible to avoid unnecessary management of messages already expired.

In the "Message Text" part there will be:

- the Exchange Header
- the Business Messages (composed by the Business Application Header and by the Business Payload)
- the signature of the sender (NSP or T2S Platform) of the message (if the NR flag in the exchange header is set) based on the “Exchange Header + Business Message” content.

3.2.2.3 DEP Message Structure

A2A Primitives management

Reference ID	T2S.UC.TC.30155

The NSP shall manage the following primitives to exchange messages/files with the T2S Platform:

- Request: The T2S Platform uses this message type to send a message/file to a T2S end user and vice versa. This kind of primitive shall be used in both real-time and store-and-forward mode;
- Response: The T2S Platform uses this message type to answer to a previously received request. This kind of primitive is used only in real-time mode;
- DeliveryNotif: The NSP's gateway sends a message to inform the T2S Platform 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 T2S Platform sends to NSP's gateway the request to enable the exchanging store-and-forward traffic;
- DisableSnFTraffic: The T2S Platform sends to NSP's gateway the request to disable the exchanging store-and-forward traffic

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/t2s-0.2"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
    <dep:ExchangeHeader>
        <dep:Version>0.2</dep:Version>
        <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
        <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
        <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
        <dep:T2SMessageId>T2S.MSGRT.NSPname1.20110101000000.000001</dep:T2SMessageId>
        <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
        <dep:DeliveryMode>RT</dep:DeliveryMode>
        <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 NSP's gateway in order to exchange data with T2S Platform.

Tag name	Tag description	Allowed Values
dep:Version	Version of Data Exchange Protocol	e.g. "0.1"
dep:Sender	NSP user identification for T2S System User that sends the message	Not Applicable
dep:Receiver	NSP user identification for T2S System User that receives the message	Not Applicable
dep:TechnicalServiceId	Name of the service used to send messages and files	NSP Name+"."+ one of the following string MSGRT MSGSNF FILERT FILESNF + "."+ environment: EAC/UTEST/PROD Example: NET1.MSGRT.PROD
dep:NSPCommunication ID	Identification of the message assigned by the NSP. It must have the following format: NSP name+ NSPGatewayId+ datetime+ sequence number.	Not Applicable
dep T2SMessageId	Identification of the message sent by T2S Platform	Not Applicable

dep:T2SActorMessageId	Unique message identifier generated at Directly Connected T2S Actor site	
dep:EntryTimestamp	Timestamp of the NSP's gateway reception	Not Applicable
dep:SendTimestamp	Timestamp of the sending of message	Not Applicable
dep:ReceiveTimestamp	Timestamp of the receiving of message	Not Applicable
dep:DeliveryMode	Identification of real time or store-and-forward exchange	RT for Real-Time SF for Store-and-forward
dep:PDMHistory	History of the deliveries of the message/file in case that the message was already sent but not correctly acked	Not Applicable
dep:DeliveryNotification	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
dep:NonRepudiationExchange	Flag that indicates that a non-repudiation on exchange is requested for this message/file exchange	YES or NO.
dep:Encryption	Flag that indicates that the message/file is encryptded	YES or NO.
dep:EncryptionAlgorithm	Algoritnm used for encryption	
dep:Compression	Flag that indicates the algorithm used to compress the payload or NONE (if compression is not used)	Currently, the only value allowed is NONE.

dep:FileFormat	Format of file (e.g. ISO20022 or ISO)	
dep:ExchangeStatus	Status of the exchange	"OK" in the case of successful exchange "KO" in case of failure
dep:ErrorDescription	Description of the error occurred during the exchanging (dep:ExchangeStatus = "KO")	
dep:MessageDigest	Digest of the Message/File exchanged (The digest has to be applied to the full "Message Text" part of the WebSphere MQ messages)	

Table 3 – Exchange Header

Message and file exchange header

Reference ID	T2S.UC.TC.30160

The NSP shall manage payload (file/message) exchanged by Directly Connected T2S Actors and T2S Platform based on an "exchange header" containing relevant information.

Exchange Header management and validation

Reference ID	T2S.UC.TC.30165

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 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 T2S and for the message/file that the NSP sends to the T2S Platform.

The validation of the Exchange Header shall be based on the following XML Schema Definition (XSD):

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.ecb.eu/t2s-0.2" elementFormDefault="qualified"
xmlns="http://www.w3.org/2001/XMLSchema"
    xmlns:t2s="http://www.ecb.eu/t2s-0.2">

    <simpleType name="DistinguishedNameType">
        <restriction base="string">
            <maxLength value="100"/>
```

```
    </restriction>
</simpleType>

<simpleType name="TechnicalServiceIdType">
    <restriction base="string">
        <pattern value=".+(MSGRT|MSGSNF|FILERT|FILESNF).(EAC|UTEST|PROD)"/>
        <maxLength value="60"/>
    </restriction>
</simpleType>

<simpleType name="NSPCommunicationIDType">
    <restriction base="string">
        <maxLength value="100"/>
    </restriction>
</simpleType>

<simpleType name="T2SMessageIdType">
    <restriction base="string">
        <maxLength value="100"/>
    </restriction>
</simpleType>

<simpleType name="DeliveryModeType">
    <restriction base="string">
        <enumeration value="RT"/>
        <enumeration value="SF"/>
   </restriction>
</simpleType>

<simpleType name="CompressionIndicatorType">
    <restriction base="string">
        <enumeration value="NONE"/>
    </restriction>
</simpleType>
```

```
<simpleType name="FileFormatType">
    <restriction base="string">
        <maxLength value="100"/>
    </restriction>
</simpleType>

<simpleType name="RetentionPeriodType">
    <restriction base="int">
        <maxInclusive value="14"/>
        <minInclusive value="1"/>
        <whiteSpace value="collapse"/>
    </restriction>
</simpleType>

<simpleType name="TimestampType">
    <restriction base="dateTime"/>
</simpleType>

<simpleType name="ServiceNameType">
    <restriction base="string">
        <maxLength value="50"/>
    </restriction>
</simpleType>

<simpleType name="SnFQueueManagerNameType">
    <restriction base="string">
        <maxLength value="48"/>
    </restriction>
</simpleType>

<simpleType name="SnFQueueNameType">
    <restriction base="string">
        <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="EncryptionType">
    <restriction base="string">
        <enumeration value="Yes"/>
        <enumeration value="No"/>
    </restriction>
</simpleType>

<simpleType name="ReasonType">
    <restriction base="string">
        <maxLength value="100"/>
    </restriction>
</simpleType>

<simpleType name="ErrorCodeType">
    <restriction base="string">
        <pattern value="T2S[0-9]{3}E"></pattern>
    </restriction>
</simpleType>
```

```
<simpleType name="AdditionalInfoType">
  <restriction base="string">
    <maxLength value="200"></maxLength>
  </restriction>
</simpleType>

<simpleType name="VersionType">
    <restriction base="string">
        <enumeration value="0.2"></enumeration>
    </restriction>
</simpleType>

<simpleType name="T2SActorMessageIdType">
    <restriction base="string">
        <maxLength value="100"></maxLength>
    </restriction>
</simpleType>

 <simpleType name="MessageDigestType">
    <restriction base="string">
        <maxLength value="1024"></maxLength>
    </restriction>
</simpleType>



<simpleType name="ExchangeStatusType">
    <restriction base="string"></restriction>
</simpleType>

<complexType name="SnFServiceType">
    <sequence>
        <element name="Name" type="t2s:ServiceNameType"/>
        <element name="DestQmanagerName" type="t2s:SnFQueueManagerNameType"/>
        <element name="DestQueueName" type="t2s:SnFQueueNameType"/>
    </sequence>
```

```
    </complexType>

    <complexType name="SnFServiceAckType">
        <complexContent>
            <extension base="t2s:SnFServiceType">
                <sequence>
                    <element name="Status" type="t2s:SnFStatusType"/>
                    <element name="Reason" type="t2s:ReasonType" minOccurs="0" maxOccurs="1"/>
                </sequence>
            </extension>
        </complexContent>
    </complexType>

    <complexType name="SnFTrafficCommandType">
        <sequence>
            <element name="Service" type="t2s:SnFServiceType" minOccurs="1"
maxOccurs="unbounded"></element>
        </sequence>
    </complexType>

    <complexType name="SnFTrafficCommandAckType">
        <sequence>
            <element name="Service" type="t2s:SnFServiceAckType" minOccurs="1"
maxOccurs="unbounded"></element>
        </sequence>
    </complexType>

    <complexType name="BusinessApplicationHeaderType">
        <complexContent>
            <extension base="anyType"></extension>
        </complexContent>
    </complexType>

    <complexType name="BusinessMessageType">
        <complexContent>
```

```
            <extension base="anyType"></extension>
        </complexContent>
    </complexType>

    <complexType name="ErrorDescriptionType">
        <sequence>
            <element name="ErrorCode" type="t2s:ErrorCodeType"></element>
            <element name="AdditionalInfo" minOccurs="0" type="t2s:AdditionalInfoType">
            </element>
        </sequence>
    </complexType>

    <complexType name="ExchangeHeaderType">
        <annotation>
            <documentation>Unique message identifier generated at T2S actor site</documentation>
        </annotation>
        <sequence>
            <element name="Version" type="t2s:VersionType">
                <annotation>
                    <documentation>Version of Data Exchange Protocol</documentation>
                </annotation>
            </element>
            <element name="Sender" type="t2s:DistinguishedNameType">
                <annotation>
                    <documentation>NSP user identification for T2S System User that send the
message</documentation>
                </annotation>
            </element>
            <element            name="OriginalSender"            type="t2s:DistinguishedNameType"
minOccurs="0"></element>
            <element name="Receiver" type="t2s:DistinguishedNameType">
                <annotation>
                    <documentation>NSP user identification for T2S System User that receive the
message</documentation>
                </annotation>
```

```
            </element>
            <element            name="FinalReceiver"            type="t2s:DistinguishedNameType"
minOccurs="0"></element>
            <element name="TechnicalServiceId" type="t2s:TechnicalServiceIdType">
                <annotation>
                    <documentation>
                        Name of the service used to send messages and files

                        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: EAC UTEST PROD
                    </documentation>
                </annotation>
            </element>
            <element  name="NSPCommunicationId"  type="t2s:NSPCommunicationIDType"  minOccurs="0"
maxOccurs="1">
                <annotation>
                    <documentation>
                        Identification  of  the  message  assigned  by  the  NSP.  It  must  have  the
following format:

                        NSP name + NSPGatewayId + &lt;datetime&gt; + &lt;msg-sequence-number&gt;
                    </documentation>
                </annotation>
            </element>
            <element name="T2SMessageId" type="t2s:T2SMessageIdType" minOccurs="0">
                <annotation>
                    <documentation>Identification     of     the     message     set     by     T2S
Platform</documentation>
                </annotation>
            </element>
            <element name="T2SActorMessageId" minOccurs="0" type="t2s:T2SActorMessageIdType">
                <annotation>
```

```
                    <documentation>Unique message identifier generated at T2S actor site</documentation>
                </annotation>
            </element>
            <element name="EntryTimestamp" type="t2s:TimestampType" minOccurs="0">
                <annotation>
                    <documentation>Timestamp of the NSP's gateway reception</documentation>
                </annotation>
            </element>
            <element name="SendTimestamp" type="t2s:TimestampType">
                <annotation>
                    <documentation>Timestamp of the sending of message</documentation>
                </annotation>
            </element>
            <element name="ReceiveTimestamp" type="t2s:TimestampType">
                <annotation>
                    <documentation>Timestamp of the receiving of message</documentation>
                </annotation>
            </element>

            <element name="PDMHistory" type="t2s:TimestampType">
                <annotation>
                    <documentation>Timestamp of the attempting of the delivery of the message </documentation>
                </annotation>
            </element>

            <element name="DeliveryMode" type="t2s:DeliveryModeType">
                <annotation>
                    <documentation>Identification of real time or store-and-forward exchange</documentation>
                </annotation>
            </element>
            <element name="DeliveryNotification" type="string" 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
                    </documentation>
                </annotation>
            </element>
            <element  name="NonRepudiationExchange"  type="t2s:NonRepudiationType"  minOccurs="0"
maxOccurs="1">
                <annotation>
                    <documentation>
                        Flag that indicates that the non-repudiation is requested or not
                    </documentation>
                </annotation>
            </element>

            <element name="Encryption" type="t2s:EncryptionType" minOccurs="0" maxOccurs="1">
                <annotation>
                    <documentation>
                        Flag that indicates that the message is encrypted or not
                    </documentation>
                </annotation>
            </element>
            <element    name="Compression"    type="t2s:CompressionIndicatorType"    minOccurs="0"
maxOccurs="1">
                <annotation>
                    <documentation>
                        Flag that indicates the algorithm used to compress the payload or NONE
(if compression is not
                        used)
                    </documentation>
```

```
            </annotation>
        </element>

        <element name="FileFormat" minOccurs="0">
            <annotation>
                <documentation>Format of file (e.g. ISO20022 or ISO…)</documentation></annotation>
            <simpleType>
                <restriction base="string">
                    <maxLength value="100"></maxLength>
                </restriction>
            </simpleType>
        </element>
        <element name="ExchangeStatus">
            <annotation>
                <documentation>
                    Status of the exchange
                    "OK" in the case of a successful exchange "KO" in case of failure
                </documentation>
            </annotation>
            <simpleType>
                <restriction base="t2s:ExchangeStatusType">
                    <enumeration value="OK"></enumeration>
                    <enumeration value="KO"></enumeration>
                </restriction>
            </simpleType>
        </element>
        <element name="ErrorDescription" type="t2s:ErrorDescriptionType" minOccurs="0" maxOccurs="1">
            <annotation>
                <documentation>Description of the error occurred during the exchanging</documentation>
            </annotation>
        </element>
        <element name="MessageDigest" type="t2s:MessageDigestType" minOccurs="0">
```

```
                <annotation>
                    <documentation>Digest of the Message/File exchanged (The digest has to be applied to the full Message Text part of the WebSphere MQ messages)</documentation>
                </annotation>
            </element>
        </sequence>
    </complexType>

    <complexType name="BusinessEnvelopeType">
        <sequence>
            <element name="BusinessApplicationHeader" type="t2s:BusinessApplicationHeaderType"></element>
            <element name="BusinessMessage" type="t2s:BusinessMessageType"></element>
        </sequence>
    </complexType>

    <complexType name="ExchangeEnvelopeType">
        <sequence>
            <element name="ExchangeHeader" type="t2s:ExchangeHeaderType"></element>
            <element name="BusinessEnvelope" type="t2s:BusinessEnvelopeType"></element>
        </sequence>
    </complexType>

    <complexType name="TechnicalAckType">
        <sequence>
            <element
                name="ExchangeHeader"
                type="t2s:ExchangeHeaderType">
            </element>
        </sequence>
    </complexType>

    <complexType name="DeliveryNotificationType">
      <sequence>
        <element
```

```
            name="ExchangeHeader"
            type="t2s:ExchangeHeaderType">
          </element>
        </sequence>
      </complexType>

      <element name="Request" type="t2s:ExchangeEnvelopeType"/>

      <element name="Response" type="t2s:ExchangeEnvelopeType"/>

      <element name="EnableSnfTraffic" type="t2s:SnFTrafficCommandType"/>

      <element name="EnableSnfTrafficAck" type="t2s:SnFTrafficCommandAckType"/>

      <element name="DisableSnfTraffic" type="t2s:SnFTrafficCommandType"/>

      <element name="DisableSnfTrafficAck" type="t2s:SnFTrafficCommandAckType"/>

      <element name="TechnicalAck" type="t2s:TechnicalAckType"></element>

      <element name="DeliveryNotification" type="t2s:DeliveryNotificationType"></element>
</schema>
```

Compression flag and compression algorithm management

Reference ID	T2S.UC.TC.30170

The NSP shall 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. Currently, this is the only value supported.

Non-repudiation Exchange flag management

Reference ID	T2S.UC.TC.30175

The NSP shall manage the non-repudiation flag on exchanging of incoming and outgoing messages/files. In the following is described the process that the T2S Platform and the NSP shall manage in case of non-repudiation in addition to the processes described in the sections 3.2.3.3, 3.2.3.4, 3.2.3.5, 3.2.3.6.

If the non-repudiation is requested for a message / file:

- the sending part (i.e. T2S) shall add a signature at the end of the message based on the "Exchange Header+Business Message" content;
- The receiving part (i.e. the NSP) shall verify the validity of the signature and send back an error messages (NAN Technical ack) if the check fails (Code T2S999E);
- The receiving part shall set the field "dep:MessageDigest" with the digest value of the "ExchangeHeader+BusinessMessage"
- The receiving part shall add, at the end of the Technical Ack, a signature based on the content of the Exchange Header (updated with the digest value and with the other fields as described in the sections 3.2.3.3, 3.2.3.4, 3.2.3.5, 3.2.3.6) and of the Business Message received from the sending part;
- The sending part shall check the validity of the signature added to the Technical Ack and store the message

All the signatures shall be based on XML Advanced Electronic Signature (XAdES) standard: in particular shall be adopted the XAdES-T format which include the timestamp to provide protection against repudiation. In the following is shown (only as example) a message with the signature:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <dep:Request xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd">
- <dep:ExchangeHeader>
  <dep:Version>0.2</dep:Version>
  <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
  <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
  <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
  <dep:T2SMessageId>T2S.MSGRT.NSPname1.20110101000000.000001</dep:T2SMessageId>
  <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
  <dep:DeliveryMode>RT</dep:DeliveryMode>
  <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>
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature-GS3PV">
- <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
- <ds:Reference URI="">
- <ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
    </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <ds:DigestValue>LIHRJV8PK0bC3IeEdt58C1rOXKQ=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
  <ds:SignatureValue>RP3xxY+CMnc4YrgzbG+Qv6FXjhdYR4DSpWQS68oHUFuZGEwOuWYIFD/yElnNBVrE3TUuBkiwtd1BXukYs2EIoiK4qqgj/ECbsK7pEE/QnAPkXruU8dUq+6ASNhKNw7IxnJdkY430F9StF0GCvPQ6js1HpV4lLn1s+pCxdPL3P/I=</ds:SignatureValue>
- <ds:KeyInfo>
- <ds:X509Data>
  <ds:X509Certificate>MIICujCCAiOgAwIBAgIBHzANBgkqhkiG9w0BAQUFADCBhzELMAkGA1UEBhMCSVQxDjAMBgNVBAgTBUl0YWx5MQ0wCwYDVQQHEwRSb21lMRcwFQYDVQQKEw5CYW5jYSBkJ0l0YWxpYTEnMCUGA1UECxMeVFNTUCAtIFRhcmdldDIgSW50ZXJuZXQgQWNjZXNzMRcwFQYDVQQDEw5UMklBIC0gQ0EgVGVzdDAeFw0xMDA5MjQxMTAwNTNaFw0zMjA4MTkxMTAwNTNaMIGXMQswCQYDVQQGEwJJVDENMAsGA1UEBxMEUm9tZTEXMBUGA1UEChMOQmFuY2EgZCdJdGFsaWExJzAlBgNVBAsTHlRTU1AgLSBUYXJnZXQyIEludGVybmV0IEFjY2VzczEZMBcGA1UEAxMQVDJJQVVzZXIwMDAwMDAwMTEcMBoGA1UEBRMTSVQ6VDJJQVVzZXIwMDAwMDAwMTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA2vSpS7CO4BX/kauuCUlApAF1rwhQYl3iHxwklz0i5bwKqJ0G42EoZdUvk7jWeQbV+zZqB7H9t
```

PXzqKTcWGQKh2PLiGLc6NpbQBQ96AfHk1OGrhG2JvDVkYtQI24/wuu0CyGguTiFol7zN7g2U1EHLSkFtKjaTgk
PFp9CPkWAy2sCAwEAAaMkMCIwCwYDVR0PBAQDAgOoMBMGA1UdJQQMMAoGCCsGAQUFBwMCMA0GCSqGSIb3DQEBB
QUAA4GBAHpuDb3dW+eGcQq0NyW5P+5Avo/ZPNO7WGq9cLZ4b/xEYQ7Rs1+pGUB2p756uETIZMkmGXGcLzO7g4Y
ENrTuuf3mtYaFIEXNae3/r3fa4JUMWlI8O9Cm9wAoGPW19LhfnV8B0hox/HFtwg3Piq3VHMD08c1auek+o2DG3
PPHbcQA

</ds:X509Data>

</ds:KeyInfo>

- <Object xmlns="http://www.w3.org/2000/09/xmldsig#">

- <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.3.2#" Target="#Signature-GS3PV">

- <UnsignedProperties>

- <UnsignedSignatureProperties>

- <SignatureTimeStamp Id="SignatureTimeStamp">

<CanonicalizationMethod xmlns="http://www.w3.org/2000/09/xmldsig#" Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />

<EncapsulatedTimeStamp Encoding="http://uri.etsi.org/01903/v1.2.2#DER">MIIKlwYJKoZIhvcNAQcCoIIKiDCCCoQCAQMxCz
AJBgUrDgMCGgUAMIHKBgsqhkiG
9w0BCRABBKCBugSBtzCBtAIBAQYEKgMEBTAhMAkGBSsOAwIaBQAEFF93EiYQKy9u
AE7MnYxZDPMng5RfAgcEnFJFsM8lGA8yMDExMDIxNTEzMzc1N1oCBgEuKYqsLqBk
pGIwYDEoMCYGA1UEAxMfU2FtcGxlcyBUU0EgU2VydmljZSBDZXJ0aWZpY2F0ZTEL
MAkGA1UEBhMCR0IxETAPBgNVBAoTCEFzY2VydGlhMRQwEgYDVQQLEwtEZXZlbG9w
bWVudKCCB7owggJrMIIB1KADAgECAgkBHYLdDlH7ge0wDQYJKoZIhvcNAQEFBQAw
VTEdMBsGA1UEAxMUQURTUyBTYW1wbGVzIFRlc3QgQ0ExCzAJBgNVBAYTAkdCMREw
DwYDVQQKEwhBc2NlcnRpYTEUMBIGA1UECxMLRGV2ZWxvcG1lbnQwHhcNMTAwMTEx
MTYzNDI0WhcNMTQwMTA5MTYzNDI0WjBgMSgwJgYDVQQDEx9TYW1wbGVzIFRTQSBT
ZXJ2aWNlIENlcnRpZmljYXRlMQswCQYDVQQGEwJHQjERMA8GA1UEChMIQXNjZXJ0
aWExFDASBgNVBAsTC0RldmVsb3BtZW50MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCbhrcWj7/UC55avkxw9/BVYQUXJzwagy1Bb5EMG4ytp3yYE6fTgtEsBRVS
OARg61pPvEoHuy6e8XQpjKTQpZJe5sOtZcj7xQhF6NabJ/a3JAH6chiN2t2yRRAE
Qx7Ra6IGGEfr6Hnb1v/H7kgIeuMPYmwJgYbhqEo5HosstW8wMQIDAQABozgwNjAO
BgNVHQ8BAf8EBAMCBsAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDAYDVR0TAQH/
BAIwADANBgkqhkiG9w0BAQUFAAOBgQATQVnkiYd7rYmKWe/mvHDL5wB/PnSouaO8
bCKq2CgFfMh+QuuI5GZosYV7NGhK6QpKk0JjkLZUzjq9yurOfrCjztg1tS8mskPo
ecGiNjNsiHgzkKykDdjaezpYvS4GVsORsli5IfcVd3ipy8f5S1L0Nc8Ghm+si6O7
KRaLs6pUyDCCApYwggH/oAMCAQICAgCKMA0GCSqGSIb3DQEBBQUAMG0xCzAJBgNV
BAYTAkdCMRkwFwYDVQQKExBBc2NlcnRpYSBMaW1pdGVkMScwJQYDVQQLEx5Bc2Nl

cnRpYSBTb2Z0d2FyZSBEaXN0cmlidXRpb24xGjAYBgNVBAMTEVRlbXBvcmFyeSBS
b290IENBMB4XDTEwMDExMTE1NDQ1MloXDTE1MDExMTE1NDIzOFowVTEdMBsGA1UE
AxMUQURTUyBTYW1wbGVzIFRlc3QgQ0ExCzAJBgNVBAYTAkdCMREwDwYDVQQKEwhB
c2NlcnRpYTEUMBIGA1UECxMLRGV2ZWxvcG1lbnQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALmnSThZdBXvj/EexAKshZKoPiZNpt5P0fBlrrF6gJYVYY4SPyju
XvZ7vvTiLSzfZLPd/FH9Q3L4u3282jKAlDidyrRPccwZvzwkYwkEGLpO+HzIh0XV
M11jFrO2Xy7bNpNVW765ZmygO2uBJw82tRKddRZb12AOoLDNwNOV25sRAgMBAAGj
XTBbMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQUQNhRrbRtRRUbdPJ9BP86ANdAAaow
DAYDVR0TBAUwAwEB/zAfBgNVHSMEGDAWgBSKJ8c94BU3lBl25RT5l7IcTS5f0zAN
BgkqhkiG9w0BAQUFAAOBgQAhD1Y7LDFm5vjUYEtkX3Vf4lw6amS4LZf87WM4O9Ee
+j5kK7TIOt2KXCydGzVqGo7Itur20Rxi57Jv8qVSSoVNkMA7zVR+uUNQnxPLlVjR
AC6FYZVniCWt8oby0J7lY7gT9Wd/nbD+CtQRFlPnkHjF0TvWZ2ShAbS6VY65GUUm
HTCCAq0wggIWoAMCAQICAUUwDQYJKoZIhvcNAQEFBQAwbTELMAkGA1UEBhMCR0Ix
GTAXBgNVBAoTEEFzY2VydGlhIExpbWl0ZWQxJzAlBgNVBAsTHkFzY2VydGlhIFNv
ZnR3YXJlIERpc3RyaWJ1dGlvbjEaMBgGA1UEAxMRVGVtcG9yYXJ5IFJvb3QgQ0Ew
HhcNMDcwMjEzMTAzNTAxWhcNMTUwMjEzMTAzMDE5WjBtMQswCQYDVQQGEwJHQjEZ
MBcGA1UEChMQQXNjZXJ0aWEgTGltaXRlZDEnMCUGA1UECxMeQXNjZXJ0aWEgU29m
dHdhcmUgRGlzdHJpYnV0aW9uMRowGAYDVQQDExFUZW1wb3JhcnkgUm9vdCBDQTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAo94dOQYcVRUwBAcb1D4+5xFa0iwQ
FFf2voVVvHmNqWgkk+Ref4c2IggCcBFPvGOv/7jl+fyInhX/LQOkUwEIz7DYVnIX
w4a5WcEOMVwZrGcG4UEa0WWe2Dr47QDMUkXZu07kfichlZpGTpBVhePlqdXJ9V3b
ntGhkIifKkMF8nsCAwEAAaNdMFswCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBSKJ8c9
4BU3lBl25RT5l7IcTS5f0zAMBgNVHRMEBTADAQH/MB8GA1UdIwQYMBaAFIonxz3g
FTeUGXblFPmXshxNLl/TMA0GCSqGSIb3DQEBBQUAA4GBAA/NlJlQRhnaaFU/kUMM
O3LbDFGHGWODBSPUqSSSjtjVBJ3Sh19LIN/9XTSZDAhiFPjyF73lNVTT7u3HgCyA
BdEjjE8y4TrSxHKNkquxz4XhvWEoWSYOzkXvdi7xHzi55tyjrUn09rr/ZPiDSU9+
Xm+nsHORU+6CdunJk6XYem3MMYIB5TCCAeECAQEwYjBVMR0wGwYDVQQDExRBRFNT
IFNhbXBsZXMgVGVzdCBDQTELMAkGA1UEBhMCR0IxETAPBgNVBAoTCEFzY2VydGlh
MRQwEgYDVQQLEwtEZXZlbG9wbWVudAIJAR2C3Q5R+4HtMAkGBSsOAwIaBQCggdow
GgYJKoZIhvcNAQkDMQ0GCyqGSIb3DQEJEAEEMCMGCSqGSIb3DQEJBDEWBBS07r+m
a3cEVbnXjbuPpLuHoZWIyzCBlgYLKoZIhvcNAQkQAgwxgYYwgYMwgYAwfgQUGmIc
lDoivG7oznzYv3BdgwdG+5UwZjBZpFcwVTEdMBsGA1UEAxMUQURTUyBTYW1wbGVz
IFRlc3QgQ0ExCzAJBgNVBAYTAkdCMREwDwYDVQQKEwhBc2NlcnRpYTEUMBIGA1UE
CxMLRGV2ZWxvcG1lbnQCCQEdgt0OUfuB7TANBgkqhkiG9w0BAQEFAASBgClSo7qD
5F3QA+x5xBSGlIOPqdpP4zO+KsghMpYCQ4EJ+9oW4hpdZMVkmBIQbevvj4wcFORf
qdua+cOByyexPTQeyG6EMEfuo1MBqoQguRWIOJ4YIeBL3KIiCtslronfUdXfOVm/
IlABIu4nikW5IDodGvI2w4stN2hWrbSBDx2r</EncapsulatedTimeStamp>

</SignatureTimeStamp>

</UnsignedSignatureProperties>

```
</UnsignedProperties>

</QualifyingProperties>

</Object>

</ds:Signature>

</dep:Request>
```

Message and file unique identification

Reference ID	T2S.UC.TC.30180

The NSP shall 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 T2S Platform and the NSP. The same identifier shall be used in the data exchange with the Directly Connected T2S Actors.

A2A Protocol Interface

Reference ID	T2S.UC.TC.30185

For each of the NSP's exchanges (messages and files), the NSP shall adopt the exchange header and the messaging flows that are specified in the next paragraph 3.2.3.

3.2.3 Protocol Description

3.2.3.1 Message Patterns

A2A Message patterns

Reference ID	T2S.UC.TC.30190

The NSP shall manage the exchange of messages and files with T2S 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 T2S Platform to confirm the reception of the message/file.

3.2.3.2 Technical Acknowledgement

Technical Acknowledgment management

Reference ID	T2S.UC.TC.30195

A Technical Ack is provided for each exchange between the T2S Platform 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 T2S 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 shall be returned the value 0 (zero) in the case a of PAN or a positive numeric value in the case of a NAN;
2. In the "Application Identity Data" of the MQMD, the system identification of the receiving application (the NSP's gateway hostname or the T2S Platform hostname) shall be returned.
3. In the "Correlation Id" field of the MQMD section shall be returned the "Message Id" value of the original message.
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 the case of a NAN the field "dep:ErrorDescription" must be filled with a error message as described in the requirement T2S.UC.TC.30200.
5. In the case of store-and-forward the NSP shall forward the full content of the “Message Text” part of the MQ message to the original sender in the delivery notification.

The Technical Ack shall be returned to the sender (T2S Platform or NSP) within a time-frame of an initial value of 10 minutes (this value could be changed in flexible way successively). For the real-time mode no particular actions are required in case of time exceeding because of the already foreseen time-out mechanism management. For store-and-forward incoming message flow (cfr T2S.UC.TC.30220), in the case that 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>

2011-01-01T00:00:00

2011-02-14 T00:10:01

</dep:PDMHistory>

As described in the requirement T2S.UC.TC.30220, 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 T2S Platform. An alarm shall be triggered in order to allow to the NSP staff to inform the Eurosystem staff that a problem is occurred in the store-and-forward channel.

Negative Technical Acknowledgment – Error description fields

Reference ID	T2S.UC.TC.30200

The NSP and T2S Platform shall 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:

Code	Error occurred	Error description field value
T2S010E	The message or file size is not in the allowed range	"Message or file size is not in the allowed size range"
T2S020E	One (or more) fields are not well formed	"Field xxxx not well formed"
T2S030E	One (or more) mandatory fields of Exchange Header are not present	"Field xxxx missing"
T2S040E	Timeout condition	"Timeout occurred"
T2S999E	All other errors	"ERROR occurred – Message/File exchange aborted"

Table 4 – Error messages

3.2.3.3 Outgoing Real-time Messages

Real-time outgoing management

Reference ID	T2S.UC.TC.30205

The NSP shall manage the real-time outgoing message pattern as detailed in the following.

The scenario considered is when the T2S Platform sends a message/file in real-time mode to a counterpart. This message pattern is shown in the following figure:

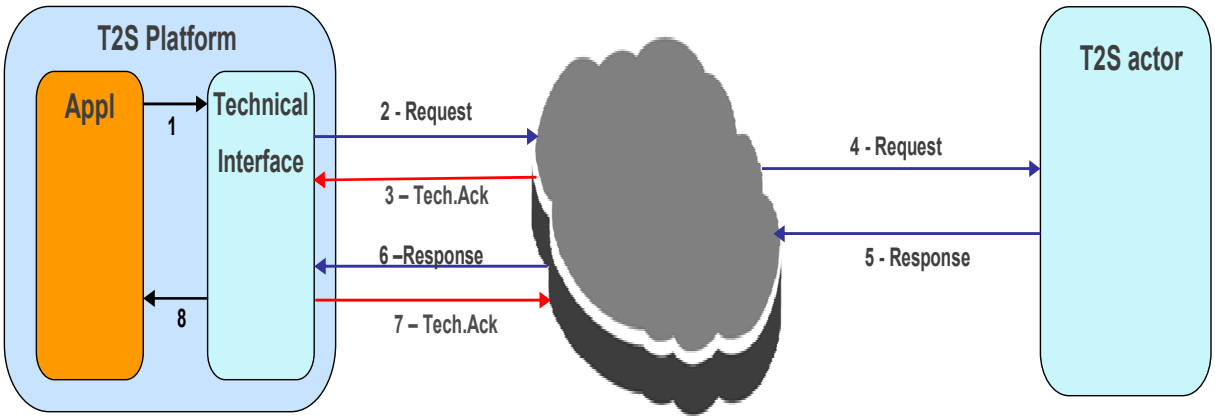

Figure 4 – Real-time outgoing flow

When the T2S Platform needs to send a message in real-time mode to its clients it will go through the following steps:

1. The T2S application passes a real-time message/file to send to the T2S network interface component.

2. The T2S Platform sends a "Request" primitive to the NSP's gateway. The "T2S Message Id" field has to be generated by the T2S Platform (this identifier shall be unique at T2S level). The "Delivery Mode" field is set to "RT".

3. 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 T2S Platform 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 to it a unique identification, stores this value in the "dep:NSPcommunicationID" field of the "Exchange Header", saves the current timestamp in the "dep:EntryTimestamp" field and sends back to T2S Platform the "PAN Technical Ack".

4. The NSP then sends the message to the final receiver. 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 T2S Platform 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 the case of an error will be not included in the message.

5. 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.

6. 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 T2S Platform 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 T2S Platform setting in the "Exchange Header":

- the same "dep:NSPcommunicationID" and "dep:Entry Timestamp" fields used for the original "request" ;
- the field "dep:T2SActorMessageId" with the unique identification generated at client site;
- the field "dep:SendTimestamp" with the time of the sending time (cfr. point 4)

7. The T2S Platform performs the "Exchange Header" validation and send back to the NSP's gateway a PAN or NAN "Technical Ack".

In the following is reported, as example, a set of possible messages for this pattern:

Message sent by T2S Platform to the NSP's gateway at the step no. 2:

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
    <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
    <dep:T2SMessageId>T2S.MSGRT.NSPname1.20110101000000.000003</dep:T2SMessageId>
    <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
    <dep:DeliveryMode>RT</dep:DeliveryMode>
    <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>
```

Technical Ack (data part) sent by the NSP's gateway to the T2S Platform at the step no. 3

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:TechnicalAck
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
    <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
    <dep:NSPCommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:NSPCommunicationId>
    <dep:T2SMessageId>T2S.MSGRT.NSPname1.20110101000000.000003</dep:T2SMessageId>
    <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
    <dep:SendTimestamp>2011-01-01T00:00:01</dep:SendTimestamp>
    <dep:DeliveryMode>RT</dep:DeliveryMode>
    <dep:ExchangeStatus>OK</dep:ExchangeStatus>
  </dep:ExchangeHeader>
</dep:TechnicalAck>
```

Response sent by NSP's gateway to T2S Platform at the step no. 6

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Response
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2s-cust1,o=nsp-name1</dep:Sender>
    <dep:Receiver>cn=t2sappl1,o=t2sprod</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
    <dep:NSPCommunicationId> nsp-name1.gtw134567.20100908185555.123456</dep:NSPCommunicationId>
    <dep:T2SActorMessageId>T2SActorGateway1.20100908175531.123456</dep:T2SActorMessageId>
```

```
    <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
    <dep:SendTimestamp>2011-01-01T00:00:00</dep:SendTimestamp>
    <dep:DeliveryMode>RT</dep:DeliveryMode>
    <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:Response>
```

3.2.3.4 Incoming Real-time Messages

Real-time incoming management

Reference ID	T2S.UC.TC.30210

The NSP shall manage the real-time incoming message pattern as detailed in the following.

Incoming real-time message means that the T2S Platform receives a message/file in real-time mode from a Directly Connected T2S Actor. This message pattern is shown in the following figure:

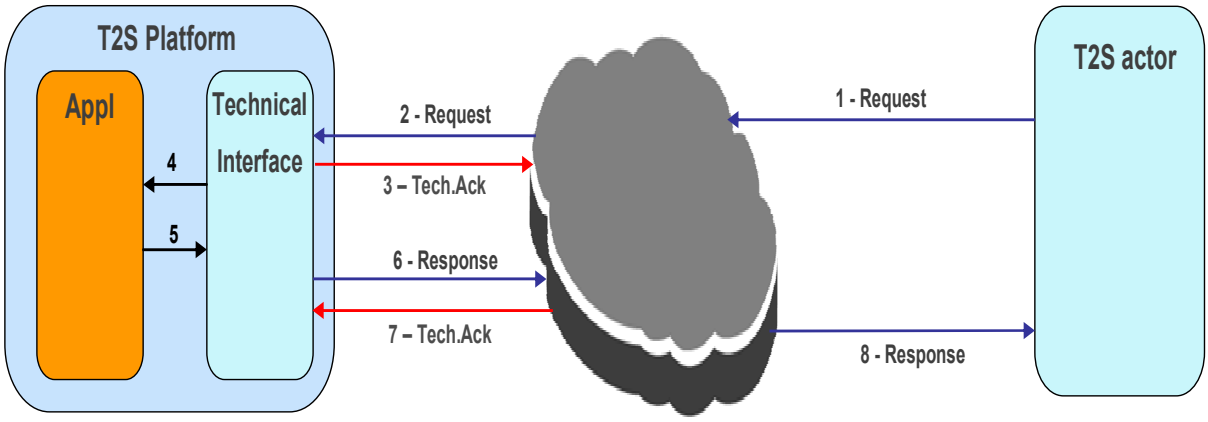

Figure 5 – Real-time incoming flow

When the T2S Platform receives a message/file in real-time mode from NSP's gateway it will go through the following steps:

1. The counterpart 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 Directly Connected T2S Actor.

2. The NSP's gateway sends a "Request" primitive to the T2S Platform. The "NSPCommunication Id" envelope field has to be generated by the NSP (this identifier shall be unique at NSP level). The T2SActorMessageId has to be set to the unique message identification generated at Directly Connected T2S Actor gateway site.

3. The T2S Platform 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 T2S Platform 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 T2S Platform doesn't answer with a response in the timeout timeframe, the NSP shall send a "timeout" information to the sender.

4. The message/file is passed to the T2S application

5. The T2S application passes the response to the T2S network interface component.

6. The T2S Platform sends the "response" message to the NSP's gateway, setting in the "Exchange Header" the "dep:T2SMessageId" to a unique identifier and keeping all other fields as received in the request.

7. 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 T2S Platform a "NAN Technical Ack" setting in appropriate way the "dep:ExchangeStatus" and "dep:ErrorDescription" fields. The NSP informs the sender about the failure with a response error messages. The flow is completed.

8. The NSP's gateway sends the "response" to the counterpart including the information of the T2SMessageId fields generated at the T2S Site (cfr step no.6)

The following messages describe, as an example, a set of possible messages for this pattern.

"Request" message received by T2S at step no. 2

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
```

```
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2s-cust1,o=nsp-name1</dep:Sender>
    <dep:Receiver>cn=t2sappl1,o=t2sprod</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGRT.PROD</dep:TechnicalServiceId>
    <dep:NSPCommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:NSPCommunicationId>
    <dep:EntryTimestamp>2011-01-01T00:04:00</dep:EntryTimestamp>
    <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
    <dep:DeliveryMode>RT</dep:DeliveryMode>
    <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>
```

3.2.3.5 Outgoing Store-and-Forward Messages

Store-and-forward outgoing management

Reference ID	T2S.UC.TC.30215

The NSP shall manage the store-and-forward outgoing message pattern as detailed in the following.

Outgoing store-and-forward message means that theT2S Platform sends a message/file in store-and-forward mode to a Directly Connected T2S Actor. This message pattern is shown in the following figure:

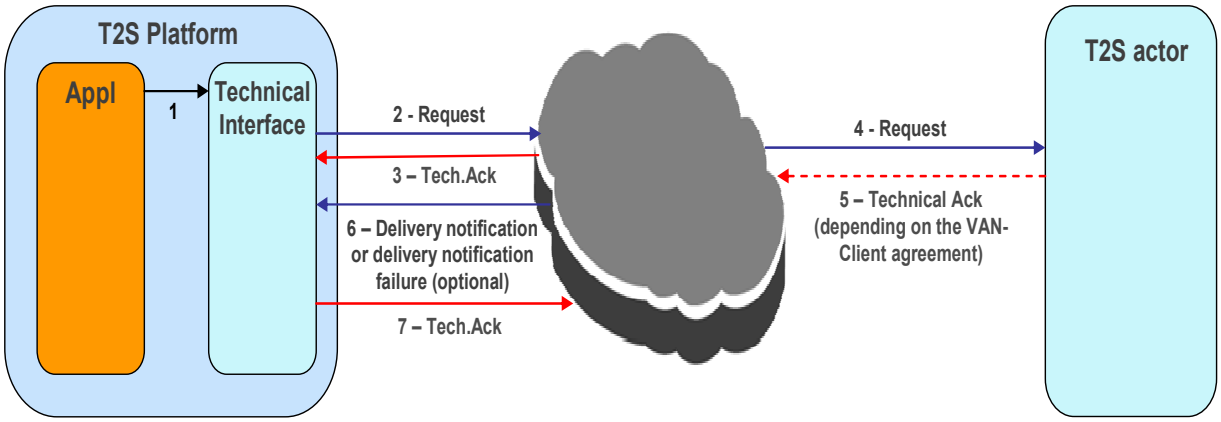

Figure 6 – Store-and-forward outgoing flow

When the T2S Platform needs to send a message in store-and-forward mode to its clients, it will take the following steps:

1. The T2S application passes the message/file to the T2S network interface component

2. The T2S Platform sends a "Request" primitive to the NSP's gateway. The "T2S Message Id" envelope field is generated by the T2S Platform (this identifier shall be unique at T2S level). The "Delivery Mode" field is set to "SF".

3. 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 T2S Platform 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 T2S Platform a "PAN Technical Ack" setting the "dep:NSPcommunicationId" and the "dep:Entry timestamp" fields of the Exchange Header.

4. If the receiving Directly Connected T2S Actor is available for store-and-forward traffic, the NSP's gateway shall send the message/file to it.

5. The receiving Directly Connected T2S Actor sends back to the NSP's gateway a "Technical Ack" (if and in the form agreed between the NSP and the Directly Connected T2S Actor).

6. If the delivery of message/file has failed for 10 times when the receiver is available, or the Directly Connected T2S Actor is unavailable for store-and-forward traffic for 14 calendar days, the NSP's gateway sends back to the T2S Platform a "DeliveryNotif" message with the same "NSP 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 "DeliveryNotif" message also in successful condition. When the "DeliveryNotif" is received by the T2S Platform, 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 T2S Platform at step no.2

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:Request
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
    <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
    <dep:T2SMessageId>T2S.MSGSNF.NSPname1.20110101000000.000005</dep:T2SMessageId>
    <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
    <dep:DeliveryMode>SF</dep:DeliveryMode>
    <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>
```

Data part of the Technical Ack received by the T2S Platform at step no. 3

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:TechnicalAck
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
```

```
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
    <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
    <dep:NSPCommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:NSPCommunicationId>
    <dep:T2SMessageId>T2S.MSGSNF.NSPname1.20110101000000.000005</dep:T2SMessageId>
    <dep:SendTimestamp>2011-01-01T00:04:01</dep:SendTimestamp>
    <dep:DeliveryMode>SF</dep:DeliveryMode>
    <dep:ExchangeStatus>OK</dep:ExchangeStatus>
  </dep:ExchangeHeader>
</dep:TechnicalAck>
```

DeliveryNotif failure message received by the T2S Platform in the case of a delivery notification failure from the NSP's gateway because the final receiver has not connected for 14 calendar days

```
<?xml version="1.0" encoding="UTF-8" ?>
<dep:DeliveryNotification
  xmlns:dep="http://www.ecb.eu/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:ExchangeHeader>
    <dep:Version>0.2</dep:Version>
    <dep:Sender>cn=t2sappl1,o=t2sprod</dep:Sender>
    <dep:Receiver>cn=t2s-cust1,o=nsp-name1</dep:Receiver>
    <dep:TechnicalServiceId>nsp-name1.MSGSNF.PROD</dep:TechnicalServiceId>
    <dep:NSPCommunicationId>nsp-name1.gtw134567.20100908185555.123456</dep:NSPCommunicationId>
    <dep:T2SMessageId>T2S.MSGSNF.NSPname1.20110101000000.000003</dep:T2SMessageId>
    <dep:EntryTimestamp>2011-01-01T00:00:00</dep:EntryTimestamp>
    <dep:SendTimestamp>2011-01-01T00:00:01</dep:SendTimestamp>
    <dep:DeliveryMode>SF</dep:DeliveryMode>
    <dep:ExchangeStatus>KO</dep:ExchangeStatus>
    <dep:ErrorDescription>
      <dep:ErrorCode>T2S040E</dep:ErrorCode>
      <dep:AdditionalInfo>Message expired.Receiver has not been connected for 14
days</dep:AdditionalInfo>
```

```
    </dep:ErrorDescription>
  </dep:ExchangeHeader>
</dep:DeliveryNotification>
```

3.2.3.6 Incoming Store-and-Forward Messages

Store-and-forward incoming management

Reference ID	T2S.UC.TC.30220

The NSP shall manage the store-and-forward incoming message pattern as detailed below.

Incoming Store-and-Forward message means that the T2S Platform receives a message/file in store-and-forward mode from a Directly Connected T2S Actor. This message pattern is shown in the following figure:

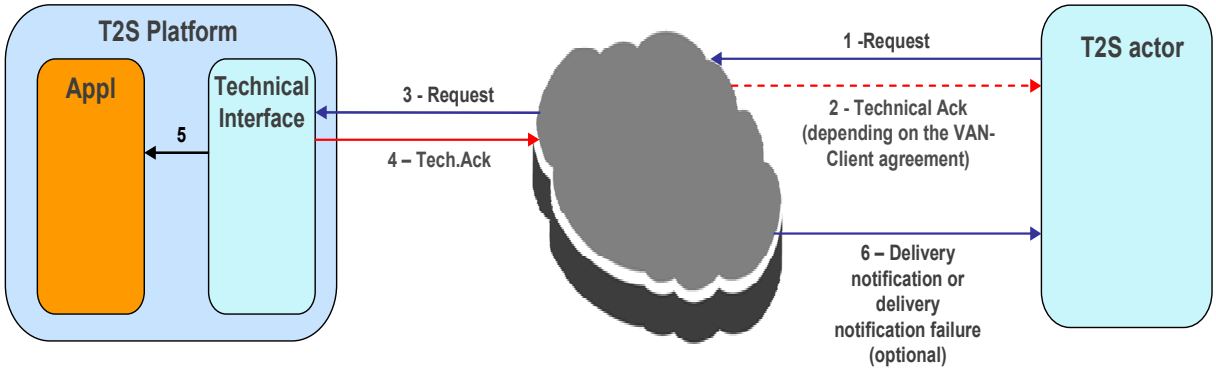

Figure 7 – Store-and-forward incoming flow

When the T2S Platform needs to receive a message/file in store-and-forward mode from its clients, it will take the following steps:

1. The Directly Connected T2S Actorsends the message/file to the NSP's gateway
2. The NSP's gateway sends back to the Directly Connected T2S Actora "Technical Ack" after performing the check on the size of message/file (and rejecting the message if the check fails).
3. If the T2S Platform has enabled the store-and-forward traffic, the NSP's gateway sends the message/file to the T2S Platform.
4. The T2S Platform receives the message/file and performs the validation check of the "envelope" part. In the case that the T2S Platform doesn’t send the Technical Ack within 10 minutes the NSP shall manage the condition as described in the requirement T2S.UC.TC.30195. After the validation check, the T2S Platform 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 Directly Connected T2S Actor and the flow is completed.

5. The message is passed to the T2S application.

6. Depending on the T2S Connectivity Service Agreement between the NSP and the Directly Connected T2S Actor, the NSP sends to the Directly Connected T2S Actor a delivery or delivery failure notification including the timestamp of the reception set by T2S Platform in the field “dep:ReceiveTimestamp” mentioned above.

3.2.3.7 Controlling of Store-and-Forward Traffic

Enable/Disable store-and-forward traffic

Reference ID	T2S.UC.TC.30225

The NSP shall manage the store-and-forward "traffic" as detailed below.

T2S Platform 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 daily "maintenance window" or for particular contingency reason.

When the T2S Platform 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/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
        <dep:Service>
                                                    <dep:Name>nsp-name1.MSGSF.PROD</dep:Name>
                                                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                                <dep:DestQueueName>IGN.NSPNAME1.MSGSF.INCOMING.L01</dep:DestQueueName>
        </dep:Service>
        <dep:Service>
                                                    <dep:Name>nsp-name1.FILESF.PROD</dep:Name>
                                                <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
                                <dep:DestQueueName>IGN.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/t2s-0.2"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ecb.eu/t2s-0.2 dep-02.xsd ">
  <dep:Service>
    <dep:Name>nsp-name1.MSGSF.PROD</dep:Name>
    <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
    <dep:DestQueueName>IGN.NSPNAME1.MSGSF.INCOMING.L01</dep:DestQueueName>
    <dep:Status>Activated</dep:Status>
    <dep:Reason/>
  </dep:Service>
  <dep:Service>
    <dep:Name>nsp-name1.FILESF.PROD</dep:Name>
    <dep:DestQmanagerName>WQI1</dep:DestQmanagerName>
    <dep:DestQueueName>IGN.NSPNAME1.FILESF.INCOMING.L01</dep:DestQueueName>
    <dep:Status>Failed</dep:Status>
    <dep:Reason>Queue not accessible. MQRC=2035</dep:Reason>
  </dep:Service>
</dep:EnableSnfTrafficAck>
```

3.3 User to application Application (U2A) requirements

For User to Application (U2A) mode, a HTTPs connection is provided, as shown in the figure below:

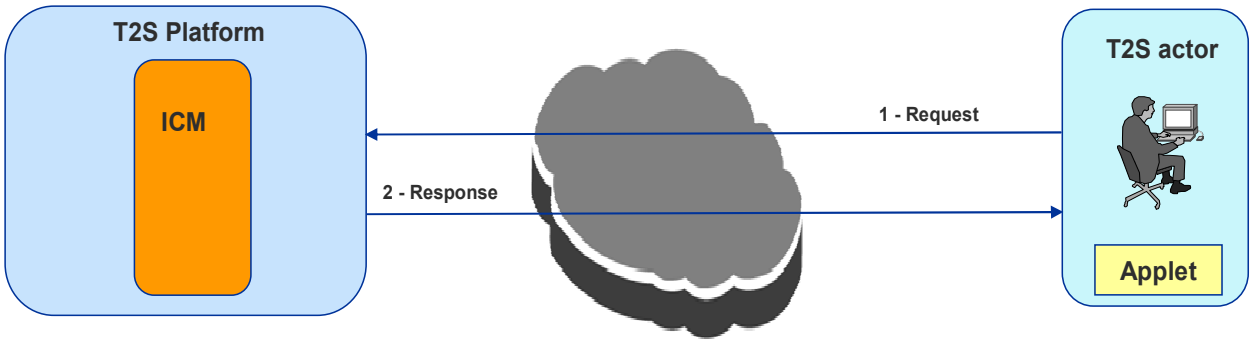

Figure 8 – User to application

Using this communication mode, the Directly Connected T2S Actor can perform both query and update operations.

U2A message flow

This paragraph describes the flow performed in the U2A interactions:

At end user site:

- The NSP performs a check whether the gateway used by the end user is authorised to access the requested URL: the check will be based on a "closed group of users" at network level principle;
- If the check is successful, the end user is able to establish an HTTPs session with the T2S U2A application;
- The T2S Platform will perform the identification and authentication of the end user based on client certificate provided in the HTTPs request;
- In the case of an update operation, an applet will be downloaded on the end user's workstation to sign (and time-stamp) the XML message for the purpose of non-repudiation;
- The end user sends signed data via a HTTPs session to the T2S web application server.

At the T2S Site:

- The web application server receives the signed data and invokes a T2S Platform service to validate certificate and signature, and stores NRO evidence after successful validation;
- The T2S Platform is connected to the NSP's PKI for certificate validation (CRL, CSL), which shall be completed each time;
- Signature validation (included time-stamping provided by the T2S Platform) will be completed by the T2S Platform based on the Directly Connected T2S Actor's 'public key included in the HTTPs message;
- The web Application sends a (business) acknowledgement via HTTPs session.

U2A Interface with the platform

Reference ID	T2S.UC.TC.30230

The NSP interface at the T2S Site shall be based on HTTPs protocol.

U2A security

Reference ID	T2S.UC.TC.30235

The NSP shall support U2A connectivity enabling HTTPs traffic between the users' workstations and the T2S Platform using a browser and assuring confidentiality and integrity of the exchanged data.

U2A user authentication

Reference ID	T2S.UC.TC.30245

The NSP shall distribute to the end users the credential to access the interface to the T2S. The NSP shall deliver the certificates for U2A to the end users (with a smart-card).

U2A closed group of user authorization

Reference ID	T2S.UC.TC.30250

The NSP shall check the authorization of the end users to access the T2S Platform based on the Network level. The IP of the end user access point is checked by the NSP to authorize the access to the requested T2S URL. The end user is requested to open a VPN connection (performing identification and authentication) with the NSP to be able to establish a HTTPs session with the T2S Platform.

3.4 NSP Interface with the Directly Connected T2S Actors

NSP shall provide an interface to the Directly Connected T2S Actor which allows the usage of U2A and A2A services.

A2A Interface with the users

Reference ID	T2S.UC.TC.30255

The NSP shall offer an interface to the users which are able to manage A2A flows described in the previous paragraph, section 3.2.3.

U2A Interface with the users

Reference ID	T2S.UC.TC.30260

The NSP interface with end users shall be based on HTTPs protocol.

U2A Interface with the users – minimal requirement

Reference ID	T2S.UC.TC.30265

The protocol at the interface between the NSP and the end users and its physical implementation are not specified in these Technical Requirements. This shall be defined bilaterally between the Directly Connected T2S Actors and the NSP.

However, the interface must comply with the minimal requirements listed in the current document for Web browsing access.

4 Security services

Security is of paramount importance for T2S, as very sensitive information will be exchanged between the T2S Platform and its users. The NSP plays a fundamental role in maintaining high protection levels of such information. The following paragraphs describe the security requirements of the security services to be provided by the NSP in order to guarantee:

- a high-quality managed security service;
- the integrity and confidentiality of the information exchanged;
- the end user accountability;
- the implementation of the need-to-do principle in access control mechanisms;
- the non-repudiation of the messages;
- the auditable of the security components and processes;
- the monitoring of the security components and processes;
- the availability of PKI services, such as the issuing of the end user certificates, the CRL/OCSP interface and the interface to the T2S Identity Manager.

4.1 General requirements

Technology and organisational processes

Reference ID	T2S.UC.TC.41010

The NSP shall offer state-of-the-art technology and organisational processes to support in an effective and efficient way the security of the T2S infrastructure and information.

In this context, the NSP shall comply with the SAS 70 best practices and/or the ISO27001 standard.

Security Platform as a service

Reference ID	T2S.UC.TC.41020

The NSP shall deliver the necessary technical infrastructure and software components to its Directly Connected T2S Actors and to the T2S Platform which allows the management of the T2S security. The NSP shall operate a T2S Security Platform assuring compliance with the T2S security requirements set out in following sections.

Operational readiness

Reference ID	T2S.UC.TC.41030

The NSP guarantees the operational readiness of all relevant security devices and components of its security platform (such as network encryption device, signing software, PKI services) according to the relevant service levels.

4.2 Confidentiality

Encryption of all incoming and outgoing traffic

Reference ID	T2S.UC.TC.42040

The NSP shall ensure confidentiality of all T2S traffic over its Network. The NSP's gateway shall encrypt or decrypt all incoming and outgoing traffic accordingly.

The NSP shall ensure that its staff and other parties cannot access or copy unencrypted data exchanged over its network except when subject to access controls, secure logging and reporting to T2S.

Segregation of data

Reference ID	T2S.UC.TC.42050

The NSP shall ensure that the each of its Directly Connected T2S Actors can access only its own incoming and outgoing traffic. No other party (including the NSP and its Subcontractors) shall be able to access unencrypted data without such access being under access control, secure logging and reported to the Eurosystem.

4.3 Integrity

Digest algorithms

Reference ID	T2S.UC.TC.43060

The NSP shall use only strong and not deprecated digest (hash) algorithms for its Solution. If weak algorithms (SHA-1 and MD5) are used to generate digests, the NSP shall provide a risk analysis of non-compliance and an action plan for risk mitigation.

Integrity of traffic

Reference ID	T2S.UC.TC.43070

The NSP shall ensure the integrity of all traffic exchanged between its Directly Connected T2S Actors and the T2S Platform.

Integrity of software components

Reference ID	T2S.UC.TC.43090

The NSP shall ensure the integrity of its software components providing Connectivity Services and the security features for T2S (such as signing, encryption, key management). The NSP shall digitally sign all relevant software components. The Eurosystem shall manage the digital keys used for signing.

The NSP shall automatically detect every planned and unplanned (intentional and accidental) modification and immediately alert the Eurosystem.

The NSP shall ensure the protection against malicious codes.

Integrity of audit logs

Reference ID	T2S.UC.TC.43100

The NSP shall ensure and control the integrity of all T2S audit logs.

4.4 User identification and authentication

The T2S applications will authorise each connection of a remote end user or application based on an identity provided by the NSP. Subsequently, the T2S authorisation procedure will assign the privileges to the end user in accordance with the information in the T2S database, and grant access to data/functions based on that information.

Infrastructure

Reference ID	T2S.UC.TC.44110

The NSP shall deliver a technical infrastructure and necessary software components to its Directly Connected T2S Actors and the T2S Platform, allowing the management of end users identity and end users credentials.

Unique identification of users

Reference ID	T2S.UC.TC.44120

The NSP shall identify all its Directly Connected T2S Actors and the T2S Platform in a unique way. The NSP shall guarantee the identification via digital certificates.

Multi-identification of a user

Reference ID	T2S.UC.TC.44130

The NSP shall allow multi-identification of a Directly Connected T2S Actor for several user accounts and shall accommodate these consistently in its solution.

Decentralised management of users

Reference ID	T2S.UC.TC.44140

The NSP shall allow local security administrators of its Directly Connected T2S Actors and the T2S Platform to manage the end users' identity and credentials required to access the T2S Platform (such as end user provisioning, service provisioning). However, only the T2S / Eurosystem security administrator shall be able to grant the access privilege to the T2S Platform.

Identification

Reference ID	T2S.UC.TC.44150

The NSP shall identify its Directly Connected T2S Actors and the T2S Platform every time they open a new session with the NSP's gateway. There is no end-to-end session (U2A is an exception to this default behaviour).

The NSP shall transfer to the receiver the identity of the sender. The NSP shall include this information in the message and file envelope for the A2A.

Authentication

Reference ID	T2S.UC.TC.44160

The NSP shall authenticate its Directly Connected T2S Actors and the T2S Platform every time they open a new session with the NSP's gateway. The NSP shall use digital keys stored in Hardware Security Modules ("**HSM**") accessible by the NSP's gateways for this purpose.

The NSP shall always check validity of digital certificates issued for keys used to authenticate Directly Connected T2S Actors accessing the T2S Platform. The digital keys used for authentication purpose shall be different by the keys used for digital signature.

4.5 Access control

4.5.1 User access

Reference ID	T2S.UC.TC.45200

The NSP shall restrict access to its Connectivity Services only to identified and authorised end users in accordance with the specification described below.

4.5.2 Closed groups of users ("CGU")

Logically segregated groups of users

Reference ID	T2S.UC.TC.45210

The NSP shall allow creation and removal of logically segregated groups of Directly Connected T2S Actor/ end users. The NSP shall manage all groups. In particular, the NSP shall create and manage the groups of Directly Connected T2S Actors or end users for the production environment and for the test & training environments, one group for each environment. At any point in time, the NSP shall be able to implement additional groups for specific needs of T2S upon a request from the Eurosystem.

The subscription to a group of users, and any subsequent modification to such subscription, shall be arranged through an electronic workflow on the Internet. All the electronic forms shall be authorised by the T2S operator. The subscription of Directly Connected Participants shall be approved by the relevant CSDs, NCBs or external RTGS operator.

The earliest activation date for the subscriptions shall be the Saturday of the week following the form's approval by the T2S operator.

Upon request from the T2S operator, the NSP shall withdraw from the CGU a Directly Connected T2S Actor or an end user within one hour.

Segregation of traffic

Reference ID	T2S.UC.TC.45220

The NSP shall ensure segregation of data traffic between different groups of users. End users belonging to different groups cannot exchange data with each other. In particular, the test & training end users shall not be able to send messages or files to or receive messages or files from the production environment. The NSP shall install gateway(s) dedicated to the Production environment and gateway(s) dedicated to the various test and training environments.

4.5.3 Physical and logical access control of the NSP's infrastructure

Reference ID	T2S.UC.TC.45230

The NSP shall protect essential network components used for its Solution with physical and logical access controls. In particular, the NSP shall protect access to its administration interfaces (such as encryption devices, NSP's gateways, other network devices).

The NSP shall adopt a "need to work" principle to allow access to its infrastructure components.

4.6 Auditable

Audit log

Reference ID	T2S.UC.TC.46240

All encryption devices and all other network devices provided by the NSP shall use logging functionality. The NSP shall agree with the Eurosystem which audit logs have to be stored on the T2S storage devices and which may remain on the NSP's devices.

Audit logging

Reference ID	T2S.UC.TC.46250

The NSP shall log each data session established between its Directly Connected T2S Actors and the T2S Platform.

The NSP shall securely log all network component changes, access attempts and security attacks/breaches on the network components.

4.7 Security monitoring

Monitoring facilities

Reference ID	T2S.UC.TC.47260

The NSP shall deliver to the Eurosystem the necessary facilities to monitor NSP's network components which provide security features (such as signing, encryption, key management) from an operational and a configuration point of view. In particular, the NSP shall deliver features to monitor the configuration of the security providing components.

The NSP shall implement mechanisms to monitor its infrastructure for security vulnerabilities, breaches and attacks and shall ensure quick updates of all devices whenever security patches are available. The NSP shall report immediately all issues to the Eurosystem using collaboration tools (such as e-mail, instant messages).

Automated alerts

Reference ID	T2S.UC.TC.47270

The NSP shall install alerts which are automatically triggered in the event of a device failure, breach or attempted breach. The alerts shall be sent by the NSP immediately to the Eurosystem, using SNMP protocol (version 3 required).

Change management

Reference ID	T2S.UC.TC.47280

The NSP shall apply a strict change management procedure to its network components that provide security features for the T2S Platform. The Change Procedure is governed by Art. 9.3 LA and further refined in section 1.5.5.4 below. The simplification of the change procedure applicable to changes before the performance of the Eurosystem Network Acceptance test (cf. section 5.5.3, T2S.UC.TC.55410 below) shall not apply to changes to Network components that provide security features.

Network encryption failure

Reference ID	T2S.UC.TC.47290

The NSP shall design and implement procedures determining Network encryption failures which might not be identified by T2S. The NSP shall design and implement procedures resuming the encryption functionality in such circumstances. The NSP shall agree with Eurosystem upon these procedures.

4.8 Encryption specification

4.8.1 Encryption algorithms

Reference ID	T2S.UC.TC.48300

The NSP shall implement the 3DES or AES encryption algorithms with a minimum length of 128 bit for symmetric encryption keys and 1024 bit for asymmetric encryption keys.

4.8.2 Management of encryption devices

Encryption devices

Reference ID	T2S.UC.TC.48310

The NSP shall install encryption devices in all T2S Sites in Region 1 and Region 2. The NSP shall install encryption devices in all sites of its Directly Connected T2S Actors interconnected with the T2S Platform.

The encryption devices shall comply with security specifications stated in 4.8.1

Management of encryption devices

Reference ID	T2S.UC.TC.48320

The NSP shall manage all its encryption devices relevant to the T2S under its own responsibility. In case of failure or disaster, the NSP shall have a possibility to manage these devices in a highly secure remote way.

The management of the keys shall not fall under the responsibility of the NSP. Eurosystem will be responsible for the key management.

The NSP shall enable secure and resilient management of all encryption devices from the T2S Sites in Region 1 and Region 2. Management of these devices shall be possible from a second site of each region in case of component failure or disaster at the main site.

4.8.3 Key management

Key management is the process that manages the life cycle of all the digital keys used in the encryption devices, for the Directly Connected T2S Actor authentication mechanisms (i.e. digital certificates), in signing the messages at the NSP's gateways and in signing off the configuration of the software components. It involves the use of both symmetric and asymmetric algorithms and the set up of an infrastructure able to generate, store and revoke the digital keys (i.e. PKI).

Public Key Infrastructure

Reference ID	T2S.UC.TC.48330

The NSP shall deliver a Public Key Infrastructure ("**PKI**") that shall comply with X.509 version 3 standard for the digital certificates.

The provided infrastructure shall provide the following components:

- Certificate Authority,
- Hardware Security Modules,
- Directory services.

A Certificate Policy/ Certificate Practices Statement shall be agreed with Directly Connected T2S Actors.

Certification Authority compliance

Reference ID	T2S.UC.TC.48331

The NSP shall comply with the European legislation on eSignature. The NSP shall belong to the Trusted List of Certification Service Providers available at:

http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

Certification Authority

Reference ID	T2S.UC.TC.48340

The NSP shall deliver Certification Authority (CA) functions to its Directly Connected T2S Actors and the T2S Platform. The provided functions shall support the generation, management, storage, deployment and revocation of public key certificates. The NSP shall ensure that these functions work within the context of the Certificate Policy and function operationally in accordance with the Certificate Practices Statement.

Certificate Policy

Reference ID	T2S.UC.TC.48350

The NSP shall deliver to Eurosystem the Certification Policy for the CA functions it will perform. A certificate policy shall focus on certificates and the NSP (CA) responsibilities regarding these certificates. It shall define certificate characteristics such as usage, enrolment, issuance and revocation procedures, as well as liability issues.

Certificate Practices Statement

Reference ID	T2S.UC.TC.48360

The NSP shall deliver to Eurosystem the Certificate Practices Statement for the CA functions it will perform. The Certificate Practice Statement shall concentrate on the operational procedures related to the certification authority functions.

Hardware Security Modules

Reference ID	T2S.UC.TC.48370

The NSP shall provide tamper-proof HSM for storing all digital keys used for its Solution (for both the U2A and A2A). The HSM(s) shall be compliant at minimum with FIPS 140-3 or Common Criteria EAL 4+ and they will be installed in the T2S Sites.

Smart Cards

Reference ID	T2S.UC.TC.48371

The smart cards, provided by the NSP, shall comply at least with FIPS 140 for the security level 3 or Common Criteria EAL4+.

Smart Card Readers

Reference ID	T2S.UC.TC.48372

The smart card readers, provided by the NSP, shall 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;
- contact definition according to ISO7816/2;
- electronic signals according to ISO 7816/3;
- T=0 and T=1 protocols;
- PC/SC for Microsoft driver;
- Microsoft Windows Hardware Quality Labs (WHQL) compliance;
- Operating Systems:
    - Windows XP/Vista/7/Server 2003/Server 2008;
    - Linux;

- Mac OS X.

Public Key Certificates

Reference ID	T2S.UC.TC.48380

The NSP shall deliver to Eurosystem a description of the format for the public key certificates it is going to use. The certificates format shall be based on the X.509 standard and shall include detail semantic profile of its public key certificates.

Public Key Certificates Directory Service

Reference ID	T2S.UC.TC.48381

The NSP shall deliver to Eurosystem a LDAP Directory Service accessible from the T2S infrastructure. The Directory shall provide, for each end user, a single entry containing surname, name, Social Security Number (SSN) (or equivalent) and public key certificates.

Certificate Extensions

Reference ID	T2S.UC.TC.48390

The NSP shall deliver to Eurosystem a description of the certificates extensions it is going to use, if any.

Digital signature certificates must have the Non-Repudiation bit set in the "Key usage" extension.

Certificate revocation list

Reference ID	T2S.UC.TC.48395

The NSP shall provide to Eurosystem the CRL in the HTTP, LDAP and OCSP formats. The T2S Platform will choose the protocol the most appropriate for the intended performance).

Digital Signature management

Reference ID	T2S.UC.TC.48396

The sender of a message/file will use the certificate provided to him by the NSP to digitally sign the message/file. The receiver of the message/file shall be able to check the validity of the signature by using the associated certificate (public key) of the sender.

Responsibilities for management of cryptographic keys

Reference ID	T2S.UC.TC.48398

The management of cryptographic keys dedicated to the T2S Platform shall remain under the sole responsibility of Eurosystem, which shall be the only institution having operational and physical access to its key storage devices (HSM) delivered by the NSP.

Administration of symmetric and asymmetric cryptographic keys

Reference ID	T2S.UC.TC.48410

The NSP shall ensure the following administration functions for symmetric and asymmetric cryptographic keys.

- *Generation*: The NSP shall ensure secure generation of keys/key pairs.
- *Distribution*: The NSP shall ensure secure electronic distribution of keys/public keys, i.e. encrypted.
- *Renewal*: The NSP shall ensure automatic renewal of the keys on a Directly Connected T2S Actor definable basis. However, only the Eurosystem shall define the frequency of exchange and the minimum length of keys used.
- *Renewal:* The NSP shall ensure that keys renewal does not interfere with its services.
- *Storage*: The NSP shall ensure that keys/private keys are stored securely.
- *Revocation*: The NSP shall ensure immediate revocation of the key/public key certificate if it is considered compromised.

Certificate independence

Reference ID	T2S.UC.TC.48420

The certificates issued by the PKI shall be distributed and used without any constraint or reference about the physical location which will host the T2S production environment.

4.9 Other security requirements

Back up

Reference ID	T2S.UC.TC.49422

The NSP shall create daily back-up copies of information exchanged (e.g. messages or files) and shall store them for a period of six months. A restore action using one back-up copy provided by the NSP will be tested by Eurosystem's staff at least twice a year.

Security framework (adopted or proposed)

Reference ID	T2S.UC.TC.49430

The NSP shall provide to Eurosystem the security framework adopted for as the security assessment (security threats & risk analysis, improvement guidelines), security strategy (adaptive security process), deployment, management, audit (external and internal health check analysis).

The Eurosystem will have the right to request or execute any security assessment on the security of the NSP services, and NSP should commit to apply the recommendations issued by the Eurosystem or by the external company acting on behalf of Eurosystem.

The action plan would have to be agreed either with the Eurosystem or the external company, within the context of a third party assessment (i.e. for receiving a SAS 70 certification) on the basis of the criticality of the highlighted risks.

5 Operational services

5.1 Service Catalogue and manuals

Connectivity service catalogue

Reference ID	T2S.UC.TC.51010

Each NSP shall develop a catalogue of Connectivity Services for its customers as part of the T2S overall service catalogue. The content of the Connectivity Services catalogue, at the least, shall include description of detailed services and service levels (such as detailing performance, availability, support commitments).

The content of the Connectivity Services catalogue shall include the network providers the NSP uses to offer connectivity to T2S, and the services the NSP offers including:

- Detailed Services,
- Service Levels, detailing performances, availability and support commitments,
- Volume related services,
- Dedicated connectivity solutions,
- Backup/Alternative network access solutions,
- Procedures to assure the continuity of the business
- information about configuration and operation of the services

SLA, Operation and Escalation manual

Reference ID	T2S.UC.TC.51020

The NSP shall provide and maintain jointly with Eurosystem the Service Level Agreement, two reference manuals and several user guides:

1. The Service Level Agreement shall be drafted by the NSP in line with the selection criteria and the offer and in accordance with the indicators defined in this document. Then it shall be approved by Eurosystem;
2. the Operations Manual, which describes the network related components installed in the premises of the Service Provider and contains a complete list of monitored elements and the operational procedures specific to the Eurosystem – NSP relation;
3. the Escalation Manual, which formalises the escalation process in normal and abnormal situations;
4. the User Guides for all services dedicated for its Solution that shall include detailed technical information needed to install necessary software and hardware infrastructure and make use of provided services.

Each NSP will be the owner of its manuals and is responsible for any updates. Eurosystem will verify the accuracy of the manuals.

5.2 Support and Incident/Problem Management

5.2.1 Support Teams

The NSP shall offer to the Eurosystem and the Directly Connected T2S Actors a Service Desk service.

NSP Support Teams

Reference ID	T2S.UC.TC.52030

The Eurosystem and the Directly Connected T2S Actors shall be able to contact the NSP Support Teams 24 hours a day, seven days a week, all year around. The NSP Support Teams shall be able to trigger the procedure described in the Escalation Manual agreed on with the Eurosystem.

5.2.2 Trouble ticketing system

Trouble ticketing management

Reference ID	T2S.UC.TC.52040

The NSP shall record all actions, as well as the timestamp (time and date) at which the actions occur, in its central trouble ticketing system. Such system shall be accessible by the Directly Connected T2S Actors and by the Eurosystem via Internet.

Trouble ticketing report

Reference ID	T2S.UC.TC.52050

The NSP shall provide to the Eurosystem on a monthly basis a list of all severe, blocking and major incidents handled during the reporting period, including incidents where only Directly Connected T2S Actors are impaired. This table shall include at least the following information: case creation date/time, case closure date/time, impaired Directly Connected T2S Actors, severity of the incident and incident description and reason for closure. Further details are recorded and available to the Eurosystem upon request.

5.2.3 Operational incident management and escalation

The NSP maintains jointly with the Eurosystem the Escalation Manual. This document shall contain the management escalation process and the NSP's contact details.

Incident management and escalation

Reference ID	T2S.UC.TC.52060

The NSP shall start resolving each incident within 15 min after the incident has been reported and shall provide the first update to the Eurosystem within 30 min.

The NSP shall produce and deliver an incident report to the Eurosystem within 24 hours as of the incident time.

The NSP shall inform the Eurosystem in advance of known problems and any corrective measures to be taken.

5.2.4 Escalation of connectivity failures to NSP's Subcontractors

The NSP shall monitor the status of the T2S network connectivity of the T2S Platform. Upon detection of a connectivity failure by NSP or notification of a connectivity failure by the Eurosystem or Directly Connected T2S Actors, the NSP shall investigate the incident as set out below:

1. upon detection of a connectivity failure, the NSP shall immediately contact the Eurosystem and/or the Directly Connected T2S Actors and shall as soon as possible provide an initial analysis of the incident;
2. depending on the results of this analysis, the NSP may request the assistance of the Eurosystem / Directly Connected T2S Actors, provided the NSP and the T2S Actors have agreed on such assistance, in performing a number of basic checks of the connectivity equipment at the Eurosystem / the Directly Connected T2S Actors premises;
3. if the analysis shows that the incident is related to the NSP subcontractors, the NSP shall escalate the problem to the NSP's Subcontractors without any undue delay and notify Eurosystem/ Directly Connected T2S Actors of the time and date. Such a notification shall be recorded in the NSP's central trouble ticketing system;

4. The NSP shall record all actions, as well as the timestamp at which the actions occur, in its central trouble ticketing system. This information shall be made available to the Eurosystem upon request as part of the incident review activity.

Escalation of connectivity failures

Reference ID	T2S.UC.TC.52070

NSP shall have sound processes to detect, notify escalate and resolve connectivity failure.

5.3 Monitoring of the connection

Proactive monitoring

Reference ID	T2S.UC.TC.53080

The NSP shall proactively monitor all permanent connections.

The complete list of monitored elements and the details of their monitoring is documented in the Operation Manual.

Availability and bandwidth utilization report

Reference ID	T2S.UC.TC.53090

The NSP shall, on a monthly basis, report to the Eurosystem the availability of the monitored communication elements and the connections bandwidth utilization.

5.4 Business Continuity services

The NSP shall provide a reliable service, taking into account the T2S architecture and the rotation of the T2S Sites.

5.4.1 T2S Business Continuity and Rotation

Imperceptibility of the T2S Business Continuity towards the Directly Connected T2S Actors

Reference ID	T2S.UC.TC.54100

The NSP shall support the T2S Business Continuity imperceptibly to its Directly Connected T2S Actors i.e. without any necessary intervention or impact on their technical configuration.

Periodic rotations of the T2S Platform

Reference ID	T2S.UC.TC.54110

The NSP shall support the T2S Business Continuity in compliance with the T2S-specified service levels, the periodic rotations and backup procedures.

The NSP shall support traffic routing for periodic site rotations and backup procedures for the Business Continuity in imperceptibly for its Directly Connected T2S Actors. The end users shall not perceive in which site the T2S application is running. The rotation shall be fully invisible to CSDs, DCPs, NCBs and to the inter-connected market infrastructures, i.e. no configuration changes in the Directly Connected T2S Actor's systems shall be necessary.

T2S Business Continuity time objectives

Reference ID	T2S.UC.TC.54120

The NSP shall support the T2S Business Continuity with the following time objectives:

- in the case of an intra-region recovery, between primary and secondary Site in the same region, on request of the Eurosystem, the NSP shall switch the traffic between the sites in less than 15 minutes;
- in the case of an inter-region recovery between two Regions, on request of the Eurosystem, the NSP shall switch the traffic between the Regions in less than 30 minutes;
- on periodic rotation occurrence (almost every six months), the NSP shall switch the traffic between the Regions, on request of the Eurosystem during a week-end in less than 30 minutes (planned operation);

No single point of failure

Reference ID	T2S.UC.TC.54130

The NSP shall design and implement the technical infrastructure of its Solution for the T2S Platform and shall configure its network components (such as gateways) on each of the T2S Sites in Region 1 and Region 2 in a way that avoids a single point of failure (SPOF).Any additional software or hardware components shall be redundant.

DNS functionalities for Business Continuity

Reference ID	T2S.UC.TC.54140

The NSP shall connect to the T2S Platform Domain Name System to obtain in automatic mode the current location of the services for A2A and of the URL for U2A. The T2S Platform will communicate 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.

5.4.2 The NSP's Business Continuity

Reference ID	T2S.UC.TC.54150

The NSP shall manage its disaster recovery solution, which affects the T2S Connectivity Services, with the following objectives.

- In the case of the NSP intra-region recovery, the NSP shall switch the traffic to its back-up site automatically within 15 minutes. The T2S active site will not switch over to the T2S back-up site.
- In the case of a NSP regional disaster, the T2S active Region will not switch to the second Region. The Directly Connected T2S Actors served by the NSP will loose access to T2S until the NSP restores the Connectivity Services in the active T2S Region.

5.5 Operation, administration and management

5.5.1 Service Availability

The Connectivity Services shall be available 24 hours per day, seven day per week, excluding a maintenance window during the weekend from 17:00 CET of Saturday to 08:00 CET on Sunday.

5.5.2 Availability indicators

Two types of indicators shall be used to measure the availability of the Connectivity Services:

1. the Connection Availability, measuring the availability of the connection of the Directly Connected T2S Actor to the T2S system independently of the type of messaging services used (A2A, U2A);
2. Service availability measuring the availability of the services A2A and U2A.

The **Connection Availability** is the percentage of time that the connection for the Directly Connected T2S Actors is considered to be operational. It is calculated using the following formula.

$$Connection\ availabili\ ty = 100 - \frac{TotalOutag\ eTime}{TotaleServ\ iceTime} \cdot 100$$

Where:

1. Total Outage time is the product of the outage time in minutes in the reporting period and the number of affected Directly Connected T2S Actor; in the case that the outage impacts the

connection with the T2S backend application all the Directly Connected T2S Actor are considered to be affected by the outage;

2. Total Service Time is the product of the total number of the Directly Connected T2S Actor and the Service time in minutes in the reporting period as defined above.

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

The **Service Availability** is the percentage of the time that the A2A and U2A services are available to the Directly Connected T2S Actor to send and receive messages/files. It is calculated with the following formula:

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

Where:

3. Outage time is the sum of the outage time in minutes in the reporting period;
4. Service Time is the expected availability time in minutes in the reporting period.

The **Service Availability** shall not be less then 99,98 calculated on a monthly basis.

For both indicators the NSP shall describe in detail how the measurements of the outage times are calculated.

Service requirements - **Service Level specification**

Reference ID	T2S.UC.TC.55020

NSP guarantees a fault clearance within the times defined in the following table:

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

Table 1 – Service level specification

The three metrics MxTTI, MxTTR and SNI are defined as follows:

- Status Notification Interval (SNI): The Eurosystem is informed about fault status and 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[4].

The definition of priority levels is the following:

1. *high* (both T2S Sites in a single region are down, or a single sites is down – the region has a reduced bandwidth since a link is interrupted, or WAN service parameters are strongly degraded),
2. *medium* (a WAN component is faulty or a link has failed),
3. *low* (fault has only slight impact on operations or it is a requests for information).

5.5.3 Dedicated set of T2S NSP Services

The NSP shall offer the possibility to create dedicated set of NSP support services to the Eurosystem. In this respect the NSP shall develop forms to define specific service parameters regarding the configuration and operation of the NSP support services.

The Eurosystem will be the Administrator of these dedicated set of T2S NSP Services. The Administrator will:

1. be responsible for defining the support service parameters;
2. manage the subscription of the participants to the support service (see also 3.1.3.5.2);
3. be the primary contact with the NSP for the provision of the support service and the relevant documentation.

5.5.4 Change management

Any Change Request and the procedure of any Change are governed by Art. 9 Licence Agreement and the change management process described below.

[4] MxTTR is temporarily suspended by the following events: 1. T2S is not available to support or provision access to the faulty components, or 2. T2S refuses to permit contractor personnel to enter the site, or *force majeure* (a circumstance is 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).

Change management process

Reference ID	T2S.UC.TC.55410

The NSP shall, in good faith, cooperate in the change management process described below.

Until the notification of the Eurosystem that the Network and the Connectivity Services are ready for acceptance (Art. 5.4 of the Licence Agreement), any needed change with regard to the NSP's Solution will be implemented in a co-operative spirit aiming for an in-time delivery of stable Connectivity Services. The change implementation will be based on a common agreement of the Eurosystem and the NSP on the content and schedule which shall be achieved in a meeting or consultation. The result of such meeting or consultation will be documented by the Party requesting the Change and provided to the other Party through the Project Managers of the Parties (cf. section 6.4) within one (1) week after the meeting.

Considering the unique interface at the T2S Site, which is connected to several network services providers, any change on the NSP's Solution should be avoided as of the performance of the Eurosystem Network Acceptance Test (Art. 5.4 of the Licence Agreement). If a change is nonetheless necessary or useful from the Eurosystem's or NSP's point of view, a formal change management process will be followed before the implementation of the Change.

The entity requesting the Change shall serve on the other party a written request, which shall contain

1. the content of the Change;
2. a justification for the Change considering the advantages and risks of its implementation,;
3. a schedule for the implementation and an acceptance test of the change;
4. an assessment of the potential impacts, including security impacts, of the change;
5. a description of fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

The Change Request will be exchanged through the designated members of the Steering Committee who will ensure, that all Changes are correctly identified and recorded. The Steering Committee will then initiate the preparation of a Feasibility Assessment which shall be provided by the NSP, if not already delivered with the Change Request under Article 9.3 of the Licence Agreement.

The Steering Committee will schedule a meeting of the NSP and the Eurosystem within [three (3)] months as of the submission of the Change Request at one of the T2S Sites to discuss the Change Request and possibly agree on its implementation. The result of such meeting will be documented by the Party who requested the Change and be served upon the other Party through the Steering Committee within one (1) week as of the meeting. If the other Party does not object to the protocol of the meeting within one (1) month as of its receipt, the protocol is deemed accepted.

A deviation from the change management process shall only be allowed upon the agreement of the Parties or if an emergency change must be implemented and no impact on the interface at the T2S Site will arise from its implementation. Even in this case a written Change Request has to be exchanged between the Steering Committee members.

5.5.5 Reverse Billing

The NSP shall charge the participants for the traffic sent by T2S and for all the other costs related to the service management for T2S.

5.5.6 Service Meeting

The reports related to the Service Level Agreement shall be discussed and reviewed in a monthly service Meeting hosted by the Eurosystem. For this purpose the NSP shall appoint a Service Manager that shall actas unique point of contact for all the Service Level Management related issue.

6 Implementation

6.1 Volumetric criteria

In "T2S General Technical Specifications - General Technical Design" version 2.2.0 document the following volumetric assumptions are estimated:

YEAR	ANNUAL VOLUME OF TRANSACTIONS	AVERAGE DAILY VOLUME[1]
2008	260 524 500	1 009 785
2009	227 868 000	883 209
2010	221 279 000	857 671
2011	232 342 950	900 554
2012	243 960 098	945 582
2013	256 158 102	992 861
2014	**268 966 007**	**1 042 504**
2015	282 414 308	1 094 629
2016	296 535 023	1 149 361
2017	311 361 774	1 206 829
2018	326 929 863	1 267 170
2019	343 276 356	1 330 529
2020	180 220 000	1 397 054

The following figures show the estimated volumes to be managed by T2S core system (the mainframe) and the archiving platform in 2014 which will be the first year of production.

DEFINITION,	VOLUME	COMMENTS
Annual volume of transactions	**268 966 007**	
Average daily volume	1 042 504	Average daily volume = Annual Volume of Transactions divided by 258 operating days in a year
Average night time volume	938 254	Night time volume is estimated to be 90% of the daily total (Average night time volume and average day time volume have an embedded margin of 20%)
Average day time volume	312 751	Day time volume is estimated to be 30% of the daily total. (Average night time volume and average day time volume have an embedded margin of 20%)
Peak day workload	4 326 391	Peak day workload is calculated as the average daily volume multiplied by a peak load factor which is provided in most markets by the CSDs.
Peak night time work load	3 893 752	
Peak day time work load	1 297 917	
Night time peak hour work load (10h/night)	389 375	
Day time peak hour work load (12h/day)	108 160	

The descriptions of all fields present on the previous figure are the following:

- Average daily volume = Annual Volume of Transactions divided by 258 operating days in a year.
- Average night-time volume and average day-time volume have an embedded margin of 20%.
- Night-time volume is estimated to be 90% of the daily total, while day-time volume is estimated to be 30% of the daily total.
- Peak-day workload is the average daily volume multiplied by a peak load factor provided in most markets by CSDs.
- The same multipliers have been used to determine the peak night-time workload and peak day-time workload.
- Day-time peak-hour workload is the day-time peak workload divided by the number of day-time operating hours.
- Night-time peak-hour workload is the day-time peak workload divided by the number of night-time operating hours.

For each business transaction six messages are necessary. Each NSP shall size its infrastructure based on its expected market share (theoretically it can also be equal to 100%). Capacity planning breakdown data and a capacity plan shall be provided to the T2S administrator one year after the signing of the Licence Agreement and shall be updated every year thereafter.

To assists the NSP in sizing its infrastructure according to the volumetric assumptions, the following assumptions could also be considered:

a. average number of xml messages (in and out) per settlement transaction [less than 6];

b. average length of xml instruction inside a message/file [less than 4KB];

c. more than 75% of the instructions should be received in big files [more than 200 instructions];

d. more than 75% of the transactions are expected to be settled during the night time;

e. maximum number of concurrent end users for U2A [less than 400 for the T2S main system, less than 100 for the Long Term Statistical System];

f. total number of U2A browsing requests per hour for the T2S main system [less than 25000];

g. total number of A2A requests/queries[5] per hour for the T2S main system [less than 10000];

h. day-time peak hour: 108 000 settlement transactions to be handled in real-time mode.

The volumes assumed herein are mere estimations. The actual volumes of messages and files might deviate significantly from these estimations.

NSP infrastructure sizing

Reference ID	T2S.UC.TC.61030

Each NSP shall size its infrastructure based on its expected market share and to ensure it meets performance and volume requirements.

6.2 Round trip/Transit time

The round-trip time is the time needed for the exchange of a request and response message pair between Directly Connected T2S Actor and the T2S Platform, excluding the processing time at the recipients' side, under steady state conditions. It is applicable to A2A message traffic only.

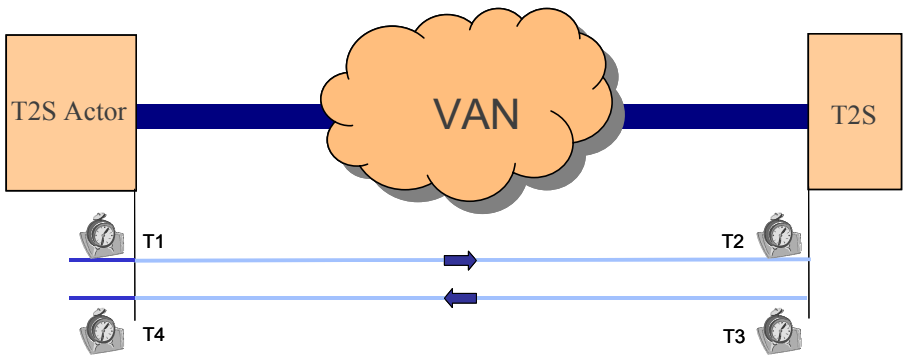

Figure 9 – Round trip time

Round Trip Time (excluding application time) is: (T2-T1) + (T4-T3)

[5] The number of instructions is not included in the number of requests/queries.

The transit time for incoming message transfer in Store-and-Forward (S&F) mode is defined as the sum of:

- the time elapsed between the time of receipt of the Directly Connected T2S Actor's message by the NSP and the NSP's first attempt to deliver the message to the T2S Platform, and
- the time elapsed between the time of receipt of the related Tech-Ack[6] from the T2S Platform and the NSP's first attempt to deliver this message to the Directly Connected T2S Actor.

Round trip time requirement for Message Transfer Real Time	< 2 sec. for the 95% of the messages < 40 sec. for the 100%
Transit time requirement for Message Transfer in S&F	< 10 sec. for the 95% of the messages < 60 sec. for the 100% of the message

The previous performance indicators shall be guaranteed for a message size of 4kB and inside the NSP domain.

6.3 Throughput

The throughput is defined as the amount of traffic (messages/files) that is exchanged per hour between the Directly Connected T2S Actors and the T2S Platform. It is applicable to both Real Time and Store-and-forward traffic.

Throughput requirement for Message Transfer	Up to 650.000 messages per hour between T2S and the NSP (in and out) up to 300.000 messages per hour for a single Directly Connected T2S Actors (in and out)
Throughput requirement for File Transfer	Up to 4,5 Gigabytes per hour between T2S system and the NSP (in and out) up to 2 Gigabytes per hour for a single Directly Connected T2S Actors (in and out).

Table 5 – Throughput

[6] T2S send an acknowledgement for a message it receives from a T2S Actor in A2A S&F mode.

6.4 Project management

Project Managers

Reference ID	T2S.UC.TC.64040

Within ten (10) days of contract award, the NSP must appoint a Project Manager (PM) who is the responsible central contact person coordinating all required activities and communicating with the Eurosystem / the 4CB over the entire term of the Licence Agreement.

The Eurosystem will also appoint a PM (the "**T2S PM**").

NSP Project Manager Duties

Reference ID	T2S.UC.TC.64050

The PM will have the following duties:

- Maintenance of the relations with the T2S PM;
- preparation of the "Implementation Plan" (Art. 5.1 of the Licence Agreement);
- Securing of the availability of all personnel and technical resources needed for the implementation, according to the plan;
- Coping with all the issues relating to the NSP service provisioning and optionally escalating the problem to the person(s) responsible in the NSP's organisation;
- identification of the NSP's personnel in charge of the performance of services with an impact on security and written notification of their identities (names, picture ID, reserved information accessed) to the Eurosystem immediately after their determination;
- identification of the NSP's personnel involved in the implementation who need access to restricted areas on the T2S Sites and written notification of their identities (names, picture ID, restricted areas to access, dates) to the Eurosystem the latest three (3) Business days before the installation-services are due to be performed;
- preparation of a monthly project progress report on the NSP installation schedule for the NSP service provisioning;
- submission of a final closure report at the end of implementation;
- monitoring and controlling the deadlines of the implementation schedule;
- regular meetings with the Eurosystem.

Implementation plan

Reference ID	T2S.UC.TC.64060

The "Implementation Plan" must be ready within thirty (30) calendar days of that PM appointment, but no later than thirty (30) Business Days after the successful completion of the Proof-of-Concept Test (Art. 5.1 of the Licence Agreement).

Implementation plan content

Reference ID	T2S.UC.TC.64070

This plan must contain the resources, the implementation dependencies, restrictions and risks, corresponding installation times and dates and necessary logistics.

The implementation schedule must consider at least the following activities:

- Proof Of Concept platform implementation;
- Local loop implementation;
- Services implementation;
- Eurosystem Network Acceptance tests.

The timing and priorities must be defined according to the T2S needs. The Eurosystem retains the right to change the priorities.

Project documents

Reference ID	T2S.UC.TC.64080

The NSP must supply the following documents:

No.	Project documents
1	Implementation plan
2	Project progress report

Table 6 – Project document list