

TARGET Instant Payment Settlement

TIPS

Connectivity - Technical Requirements

Annex to the TIPS Harmonised Conditions

1.0

Author	4CB
Version	1.0
Date	08/01/2018

All rights reserved.

TABLE OF CONTENT

1. TECHNICAL AND OPERATIONAL CRITERIA	3
1.1. GENERAL SERVICE DESCRIPTION	3
2. NETWORK CONNECTIVITY	7
2.1. PHYSICAL CONNECTIVITY SERVICES	7
2.2. INTERFACE TO THE TIPS PLATFORM (BETWEEN TIPS AND NSP)	7
3. MESSAGING SERVICES	12
3.1. A2A REQUIREMENTS FOR "INSTANT" TRANSFER OF MESSAGES	14
3.2. A2A IBM MQ REQUIREMENTS	17
3.3. A2A MESSAGE SERVICE	20
3.3.1. A2A traffic protocol description	21
3.3.2. A2A gateway control application	21
3.3.3. A2A requirements for "store-and-forward" transfer of files..	22
3.4. U2A REQUIREMENTS	22
3.5. TIPS ACTOR EMULATOR	23
4. SECURITY SERVICES	23
4.1. CLOSED GROUPS OF USERS ("CGU")	29
4.2. KEY MANAGEMENT	29
5. OPERATIONAL SERVICES	33
5.1. SERVICE CATALOGUE AND MANUALS	33
5.2. SUPPORT AND INCIDENT/PROBLEM MANAGEMENT	34
5.2.1. Support Teams	34
5.2.2. Trouble ticketing system	34
5.2.3. Operational incident management and escalation	35
5.2.4. Escalation of connectivity failures to NSP's subcontractors ..	35
5.3. MONITORING OF THE CONNECTION	36
5.4. BUSINESS CONTINUITY SERVICES	36
5.4.1. TIPS Business Continuity and Rotation	36
5.5. OPERATION, ADMINISTRATION AND MANAGEMENT	38
5.5.1. Availability indicators	38
5.5.2. Service Compliance Meeting	40
6. IMPLEMENTATION	40
6.1. PROJECT MANAGEMENT	40

1. Technical and operational criteria

The general architecture of the TIPS Platform is set out in the High Level Technical Design document. It describes the platform and defines very high-level requirements for the Connectivity Services required for the remote access to the TIPS Platform.

This document presents detailed technical criteria for the Connectivity Solution - as defined in the Harmonised Conditions for TIPS - describing network connectivity, messaging services, security services, operational services and implementation. The Solution focuses on the interconnection between TIPS Service Provider (operating the TIPS Platform, hereinafter "the TIPS Operator") and the TIPS Actor.

Thus, the requirements listed below focus on such an interconnection and refer either to the TIPS Actor or to the NSP selected by the former, which remains responsible for the compliance of the latter.

Indeed, according to what was established in the Harmonised Conditions for TIPS, the TIPS Actor shall ensure that their NSP's Connectivity Solution fulfils the following technical and operational requirements, at the time of the TIPS Operator compliance check and afterwards throughout the whole period of participation of the TIPS Actor to the TIPS Platform.

1.1. General service description

The TIPS infrastructure is deployed over one geographical Region (Italy) with two Sites which are defined as the TIPS Platform and host the TIPS business applications. To allow continuous operations without service interruptions, the Region consists of a primary and a secondary site which run independently from each other.

An optional extension to a second geographical Region (Germany) with two additional Sites, configured as above, would be possible at a later stage, if deemed necessary by the Eurosystem.

The NSP interconnects the TIPS Actor to the TIPS Platform.

The following pictures represent a model with two NSPs. Nevertheless the total number of NSPs is not limited *a priori*, two NSPs are just an example.

Technical infrastructure

Reference ID	TIPS.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 between the TIPS Actor and the TIPS Platform.

Delivery point for Connectivity Services

Reference ID	TIPS.UC.TC.11050
--------------	------------------

The NSP shall deliver Connectivity Services to each of the TIPS sites. Region 1 and Region 2 (if the latter is implemented) are interconnected through the internal network (4CBNet) which is not in the scope of these requirements.

Location of equipment

Reference ID	TIPS.UC.TC.11060
--------------	------------------

The NSP shall install all the necessary devices to ensure the connectivity to the TIPS Platform (e.g. routers, VPN devices and Network Gateways as illustrated on the Figure 1¹) inside the TIPS Operator premises (i.e. inside each TIPS Site).

The NSP shall connect its equipment to the respective TIPS communication endpoints at each TIPS Site.

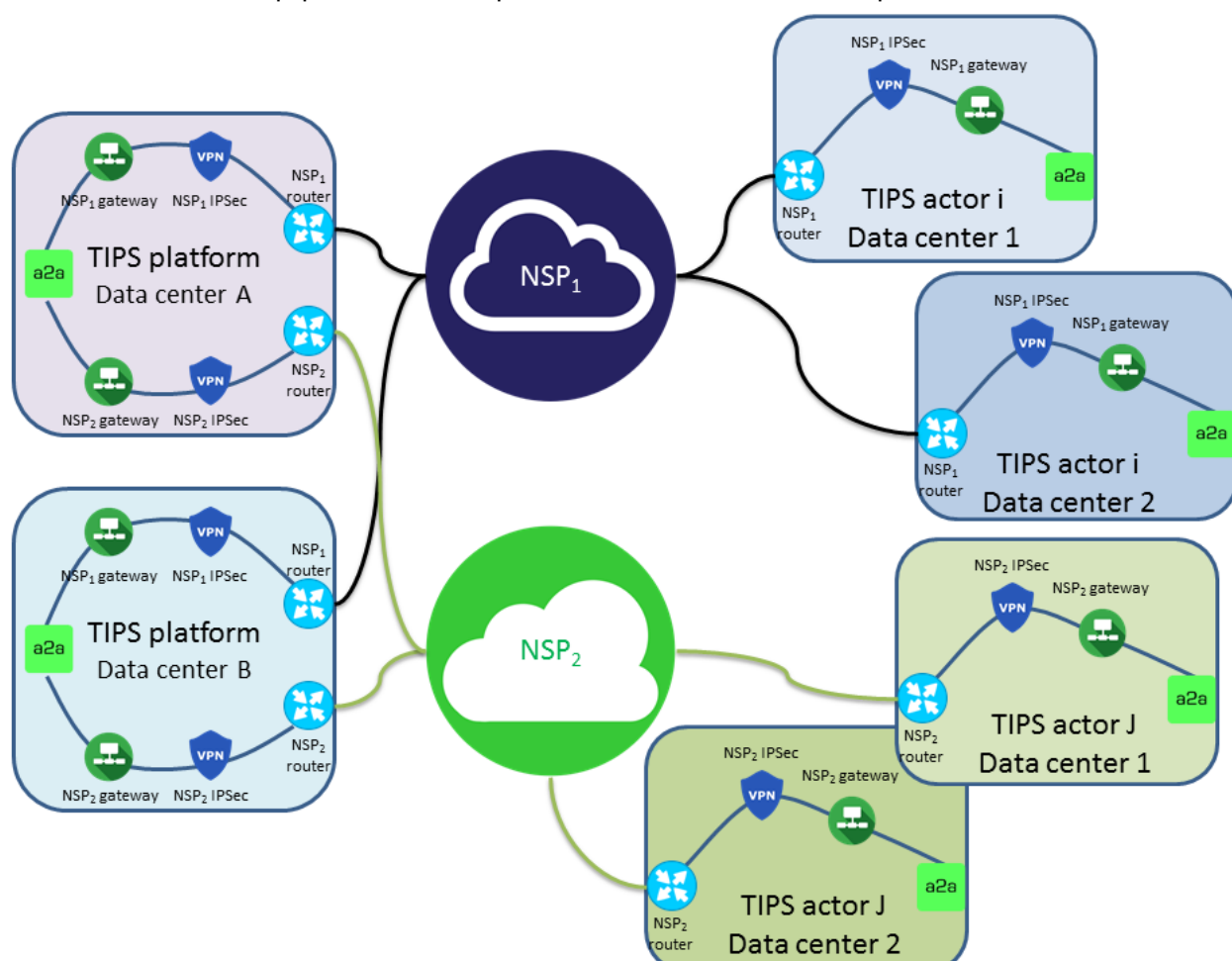


Figure 1 – Location of equipment and NSP demarcation point at the TIPS Platform sites
(on this Figure only one Region is shown, the same configuration shall be implemented on the second one)

¹ Location of equipment shown on the Figure 1 has to be considered only as an example.

Hosting agreement

Reference ID	TIPS.UC.TC.11065
--------------	------------------

Terms and Conditions for hosting provisioning are detailed in attachment to the Harmonised Conditions for TIPS.

The boundaries of responsibility

Reference ID	TIPS.UC.TC.11070
--------------	------------------

The demarcation line defining the responsibilities between the TIPS Operator and the TIPS Actor shall be the network interface between the NSP's gateways and the TIPS Platform's.

For the avoidance of any doubt, such demarcation line shall define the boundaries of the responsibilities of the TIPS Actor (the NSP's gateway is the physical boundary of responsibility). The latter shall be fully responsible and liable for all NSP's failures within this boundary.

Chain of trust relationship

Reference ID	TIPS.UC.TC.11080
--------------	------------------

The TIPS Actor shall be responsible for ensuring that the requirements expressed in this document (e.g. performance, security) are satisfied also inside the NSP domain and in the relation with their NSP.

Independence of interfaces on TIPS and TIPS Actor's sites

Reference ID	TIPS.UC.TC.11090
--------------	------------------

The NSP shall ensure that the technical solutions it adopts for the interface with the TIPS Actor do not affect the technical solution adopted for the interface with its TIPS Platform.

The NSP and its TIPS 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, so that technical choices on one interface shall not affect the other.

Single interface on the TIPS Site

Reference ID	TIPS.UC.TC.11100
--------------	------------------

The NSP shall comply with the TIPS interface as described in Chapter 3.

The NSP will provide connectivity between the TIPS Platform's application and the TIPS Actor's application.

Interface on the TIPS Actor's site

Reference ID	TIPS.UC.TC.11110
--------------	------------------

The interface on the TIPS Actor's site shall not lower the overall level of compliance of the Connectivity Solution with the TIPS security requirements, and it shall not affect by any means the interface on the TIPS Platform site (i.e. it shall not require any special handling on the TIPS site).

Security of the interface at the TIPS Actor's site

Reference ID	TIPS.UC.TC.11115
--------------	------------------

The NSP shall deliver to the TIPS Operator a detailed description of the security measures applied to the interface implemented on the TIPS Actor's site in order to allow the TIPS Operator to check their compliance with the TIPS security requirements.

The NSP shall ensure that the security measures implemented on the TIPS Actor interface are at the same level as the ones implemented for the TIPS Platform interface.

Monitoring facilities

Reference ID	TIPS.UC.TC.11130
--------------	------------------

The NSP shall provide to the TIPS Operator the facilities to continuously monitor the compliance of the NSP's technical operations with the requirements set out herein and in the "Operational manual", referred to in requirement TIPS.UC.TC.51020.

Time synchronisation

Reference ID	TIPS.UC.TC.11140
--------------	------------------

In order to make the data exchange time consistent the NSP shall synchronise the date-time of his devices either with the same date-time source adopted by the TIPS Platform or by using a Stratum 2 or 3 time source, approved by the TIPS Operator. The synchronisation interval shall be at least every one minute.

The official time of TIPS system will be the ECB time, i.e. the local time at the seat of the ECB.

NSP shall provide time information using Coordinated Universal Time (UTC) format.

2. Network Connectivity

2.1. Physical Connectivity Services

The TIPS Actor will request the NSP to offer a single logical service which can be basically seen as two different Wide Area Networks (WANs): the first between the TIPS Sites and the NSP's sites and the second between NSP's sites and TIPS Actor's sites.

The single logical service is provided as a link to a NSP managed Wide Area Network where also all the TIPS Actor sites are connected.

2.2. Interface to the TIPS Platform (between TIPS and NSP)

TIPS has two active Sites (the "TIPS Sites") which are hosted in Region 1 (in Rome, Italy). Two additional sites hosted in Region 2 (in Frankfurt am Main, Germany) could be implemented at a later stage, if deemed necessary by the Eurosystem. The NSP shall connect all active TIPS sites to its Network and provide the number of WAN links required to connect such TIPS Sites to its sites. The following requirements describe what each of the above links have to comply with.

The requirements are classified by layers according to 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 the two service demarcation lines.

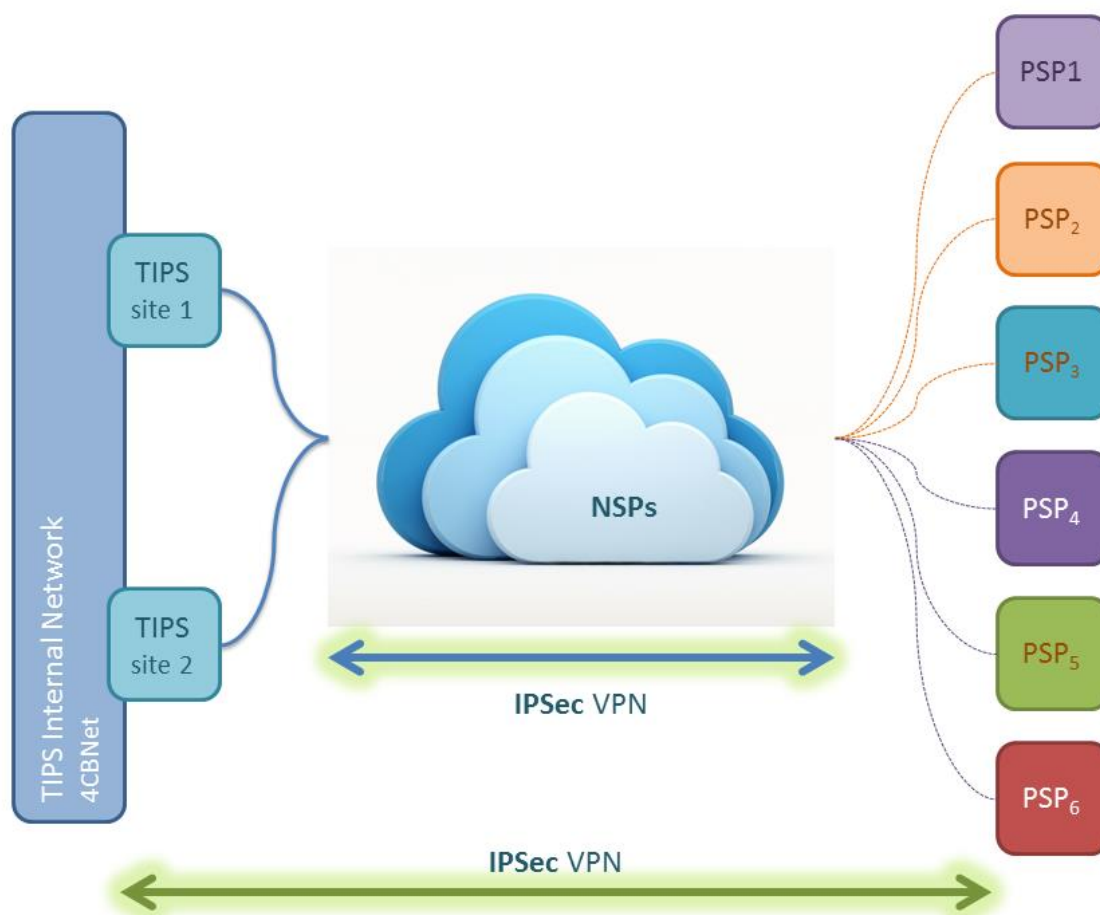


Figure 2 – Links between NSP and TIPS Platform sites

The simplified picture above describes the logical connections provided by the NSPs, assuming two network services providers are delivering connectivity services between the TIPS Platform and the TIPS actors (as previously stated, more than two providers are allowed)

Service requirements – **Demarcation line between the NSP and TIPS**

Reference ID	TIPS.UC.TC.20100
--------------	------------------

The NSP shall deliver to all the TIPS sites one or more network devices (for example router + VPN device terminations and gateway or VPN device terminations and gateway), which present one or more Ethernet interfaces to the TIPS Platform. The NSP's Gateway is the physical boundary of responsibility which defines the network demarcation line between NSP and TIPS.

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

Reference ID	TIPS.UC.TC.20102
--------------	------------------

The NSP has to ensure that the link bandwidth to each single TIPS site is able to handle the whole traffic. In case of site failure within a region, then the link to the remaining TIPS site shall handle the whole traffic.

Service requirements - **Monitoring**

Reference ID	TIPS.UC.TC. 20105
--------------	-------------------

The proposed infrastructure shall be monitored and maintained by NSP.

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

Reference ID	TIPS.UC.TC.20107
--------------	------------------

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

The links between the NSP PoP (Point of Presence) and each TIPS Site shall be provided with redundant and direct links with physical diversification. For example, each NSP device installed into a PoP has one or more local links to the TIPS Site A and one or more local links to the TIPS Site B.

The NSP shall specify where each regional/local PoPs are located.

Layer 1 requirement - **Link bandwidth**

Reference ID	TIPS.UC.TC.20108
--------------	------------------

Each link is initially delivered with a minimum bandwidth of 1Gbps. It is possible to reuse existing interfaces (if any).

Layer 1 requirement - **Link latency**

Reference ID	TIPS.UC.TC.20115
--------------	------------------

Each link has a one way delay of maximum 40 msec. Each link for the connection between the TIPS Sites and the Actor can be separated in two physical connections: the first one between the Actor site and the NSP site and the second one between the NSP site and the TIPS Sites.

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

Reference ID	TIPS.UC.TC.20135
--------------	------------------

The NSP delivers to TIPS the connectivity services via network equipment having 1 Gigabit Ethernet ports.

Layer 1 requirement - Path diversification

Reference ID	TIPS.UC.TC.20140
--------------	------------------

Paths from the TIPS site to the local NSP 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 the backbone and throughout the whole path across the backbone itself.

Layer 1 requirement - Links responsibility

Reference ID	TIPS.UC.TC.20145
--------------	------------------

The NSP shall maintain all links and network equipment between all the TIPS 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 3 requirement - IPv4

Reference ID	TIPS.UC.TC.20155
--------------	------------------

Internet Protocol (IP) version 4 (IPv4) protocol is used between the TIPS Platform and the TIPS Actor.

Layer 3 requirement - IP addressing schema

Reference ID	TIPS.UC.TC.20160
--------------	------------------

The NSP has to use either an IP address range which is "public" and agreed with the TIPS platform or a private address allocation in terms of RFC1918 (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)) and agreed with the TIPS platform.

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

Reference ID	TIPS.UC.TC.20165
--------------	------------------

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

Only authenticated parties shall be able to access the TIPS Platform.

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

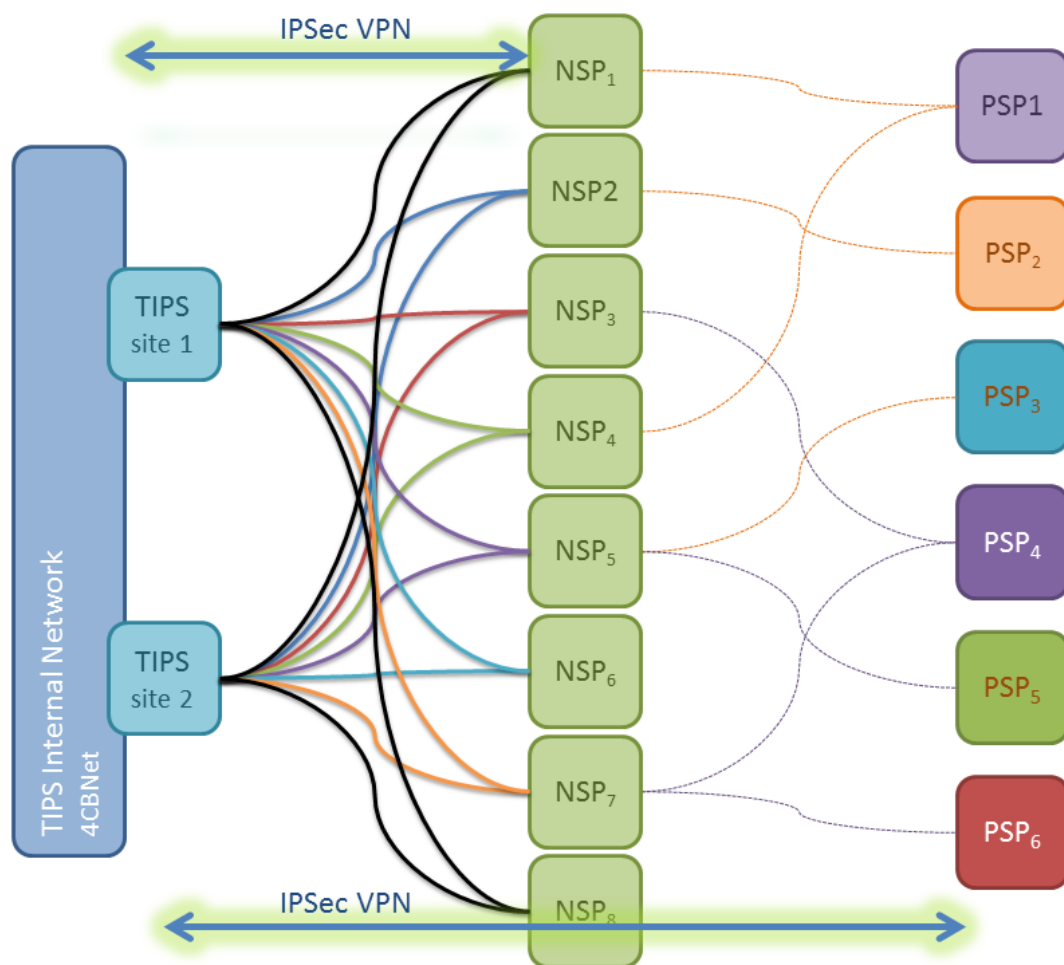
Layer 3 requirement – **Static Routing**

Reference ID	TIPS.UC.TC.20175
--------------	------------------

Only static routes will be used between the NSP and the TIPS Platform; no dynamic routing protocols are used.

3. Messaging services

This chapter details the requirements that the NSP has to fulfil to comply with the TIPS Platform in order to manage the "application to application" (A2A) and "user to application" (U2A) data flows.



The TIPS Platform can be accessed by the TIPS Actor in A2A mode and U2A mode.

In A2A mode, two categories of business data will be exchanged:

- "message" - a "message" is a data structure containing a financial instruction or information based on the XML format (ISO20022 standard)
- "file" - a "file" is a data structure containing one or more financial information, either for statistical or accounting or reporting purposes, based on different formats (e.g. flat text, ISO20022 standard, etc).

For the A2A mode, the TIPS Platform communicates with the TIPS Actor with the "instant" transfer mode, where the primary objective is the lowest possible latency in the transfer of the message. The "instant" transfer mode:

- requires that both parties, the sender and the receiver, are available at the same time to exchange the message;
- adopts the "at most once" principle;
- does not envisage any message categorization/prioritization.

Therefore, if the receiver is unavailable or there is an error in transferring the message, no retry mechanism is foreseen.

During "instant" transfers, data will be exchanged only in "push" mode. The term "push" mode refers to when the originator of a message is pushing it to the final receiver.

For the A2A transmission of files, the TIPS Platform communicates with the TIPS Actors using the "store and forward" transfer mode, which enables a sender to transmit files even when a receiver is unavailable. If the receiver is temporarily unavailable, the NSP stores the files and delivers them as soon as the receiver becomes available again.

A2A services shall be provided by means of decoupling components, i.e. Network Gateways, allowing data exchange without any direct connections between the TIPS Actor's application and the TIPS Platform.

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

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

Reference ID	TIPS.UC.TC.30010
--------------	------------------

The NSP shall offer the data transport services in the A2A and the U2A modes to the TIPS Actor and to the TIPS Platform.

The "application to application" (A2A) mode

Reference ID	TIPS.UC.TC. 30015
--------------	-------------------

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

The "user to application" (U2A) mode

Reference ID	TIPS.UC.TC.30220
--------------	------------------

The NSP shall support the U2A connectivity enabling HTTPs traffic between the TIPS Actor and the TIPS Platform.

3.1. A2A requirements for "instant" transfer of messages

This paragraph describes the flow of the A2A interactions, in the scenario of a TIPS Actor sending an "instant" message to the TIPS Platform:

At the TIPS Actor's site:

- The Application of the TIPS Actor sends an "instant" message for the TIPS Platform to its Network Gateway;
- The Network Gateway of the TIPS Actor performs a check against the NSP on whether the TIPS Actor is authorised to exchange the requested traffic: the check will be based on a "closed group of users" defined at NSP level;
- If the check is successful, the Network Gateway of the TIPS Actor signs the message using the TIPS Actor digital certificate and forwards the "instant" message and related signature information to the Network Gateway of the TIPS Platform;

At the TIPS platform site:

- the Network Gateway of the TIPS Platform receives the signed data and validates the certificate and the signature, thus performing the identification and authentication of the sender (TIPS Actor);
- if the signature is verified, the Network Gateway of the TIPS Platform forwards the "instant" message and related signature information to the TIPS Platform;
- if the delivery of the message is successful, the Network Gateway of the TIPS Platform sends back a positive acknowledgment to the Network Gateway of the sender (TIPS Actor);
- the TIPS Platform receives the signed data and stores it as an NRO evidence;
- the TIPS Application sends the business response (positive or negative) for every message received.

This paragraph describes the flow of the A2A interactions, in the scenario of a TIPS Actor receiving an "instant" message from the TIPS Platform:

At the TIPS platform Site:

- the TIPS Application sends the request to send a message to the Network Gateway
- the Network Gateway of the TIPS Platform receives the message from the TIPS Application and, if required, it signs the message on behalf of the TIPS Platform
- the Network Gateway sends the message to the relevant TIPS actor
- the Network Gateway, if required, sends back to the TIPS Application a message indicating the successful/unsuccessful sending operation, it includes the signature added to the message
- the Network Gateway, if required, sends back to the TIPS Application a message indicating the successful/unsuccessful delivery of the message to the TIPS actor.

A2A NSP Interface

Reference ID	TIPS.UC.TC. 30230
--------------	-------------------

The NSP shall provide the A2A Interface by means of a Network Gateway supporting the network operations required for the solution, including:

- Identification, authentication and authorization of the NSP participant (TIPS Actor or TIPS Platform)
- Scalability
- High availability
- Load balancing
- Transparent routing
- Flood control

A2A NSP addressing model

Reference ID	TIPS.UC.TC. 30231
--------------	-------------------

The NSP shall support the message exchange based on the following addressing elements:

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

A2A NSP Interface High availability and resiliency

Reference ID	TIPS.UC.TC. 30232
--------------	-------------------

The NSP shall provide the Network Gateways (and network equipment) in high availability, to support the 24x7x365 requirement of the "instant" message exchange.

The NSP shall support Network Gateways in active-active configuration in the same site and also over multiple sites.

A2A NSP Interface scalability

Reference ID	TIPS.UC.TC. 30233
--------------	-------------------

The NSP shall support horizontal scalability of the Network Gateway, to enable the addition of Network Gateways in case an additional traffic load is required. The deployment of a new Network Gateway shall not impact the availability of the service in the involved infrastructure.

A2A NSP Load balancing

Reference ID	TIPS.UC.TC. 30234
--------------	-------------------

The NSP shall provide load-balancing features, by supporting the spreading of traffic exchange over multiple Network Gateways, with no requirement for any specific application logic to be implemented in the TIPS Platform.

A2A NSP routing independency

Reference ID	TIPS.UC.TC. 30235
--------------	-------------------

The NSP shall provide a location independent routing. The TIPS platform is unaware of the physical location of the TIPS Actor and viceversa. If the TIPS Actor configuration changes, for example due to disaster recovery procedures, no changes shall be required at the TIPS Platform.

A2A NSP flooding control

Reference ID	TIPS.UC.TC. 30236
--------------	-------------------

The NSP shall implement an anti-flooding (throttling) mechanism to ensure that no single TIPS Actor can affect the availability of the solution at the TIPS Platform or at another TIPS Actor.

A2A message size limitations

Reference ID	TIPS.UC.TC. 30237
--------------	-------------------

The NSP shall support the exchange of messages with a maximum length set to 10KiB (1 KiB = 1.024 bytes). The maximum length refers to the business content of the transferred message, without taking into account the communication protocol overheads.

A2A message size management

Reference ID	TIPS.UC.TC. 30238
--------------	-------------------

The NSP shall reject as soon as possible any message 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 size out of allowed range.").

A2A message delivery approach

Reference ID	TIPS.UC.TC. 30239
--------------	-------------------

The NSP shall deliver messages at most once. In case of error or doubt conditions, no retry mechanism shall be implemented to avoid any risk of message duplication.

A2A messages independency

Reference ID	TIPS.UC.TC. 30241
--------------	-------------------

The NSP shall manage each "instant" message as an individual message, with no correlation between messages (for example, messages belonging to the same business transaction), thus allowing the message "completing" a business transaction to be delivered through a network access point different from the access point used to send the message initiating the business transaction.

A2A user authentication

Reference ID	TIPS.UC.TC.30245
--------------	------------------

The NSP shall provide to the TIPS Actor the required certificates to access the A2A messaging services. The private keys of the PKI certificates must be secured by means of FIPS 140-2 Level 3 HSM – compliant equipment. The NSP must keep the cryptographic protocols and key length deployment in line with up-to-date security recommendation (e.g. NIST 800-57) .

A2A closed group of user authorization

Reference ID	TIPS.UC.TC.30250
--------------	------------------

The NSP shall check the authorization of the TIPS Actors to access the TIPS Platform based on enforced rules at NSP level, supporting segregation of traffic flows between participants.

3.2. A2A IBM MQ requirements

To provide A2A services to the TIPS Platform, the NSP shall connect to the IBM Messaging Queuing (formerly known as WebSphere MQ) infrastructure of TIPS Platform. The NSP shall comply with the following requirements.

WMQ product version

Reference ID	TIPS.UC.TC.30300
--------------	------------------

The NSP shall connect to the TIPS sites using the IBM Message Queuing ("WMQ") transport protocol. The NSP shall use a WMQ product version compliant with the WMQ version adopted by the TIPS Platform.

WMQ channels

Reference ID	TIPS.UC.TC.30305
--------------	------------------

The NSP shall support the use of multiple channels to connect to the TIPS WMQ infrastructure.

WMQ channels TLS connection

Reference ID	TIPS.UC.TC.30310
--------------	------------------

WMQ channel connections shall be secured by using the TLS protocol and digital certificates exchanged between the TIPS Platform and the NSP. Digital certificates for the WMQ channels TLS connection will be provided by the TIPS Operator to the NSP.

WMQ channels type

Reference ID	TIPS.UC.TC.30315
--------------	------------------

The NSP shall connect to the TIPS WMQ infrastructure using client-server mode (channels SVRCONN located at the TIPS sites). The name of the channels should follow the TIPS naming convention.

WMQ message queues

Reference ID	TIPS.UC.TC.30320
--------------	------------------

The following type of queues shall be supported:

- *command queues* to control Network Gateway (e.g. to establish communication sessions, if needed in the NSP solution);
- *file queue to exchange file send requests*;
- *traffic queues* to exchange messages within the established communication session.

A set of queues shall be set up for each specific flow in the transport protocol between the TIPS Platform and the NSP.

The following flows are envisaged:

Queue type	Flow	Flow direction	Description
Command	Request	TIPS Platform => NSP's NG	command request
	Response	NSP's NG => TIPS Platform	outcome of the command request
	Indication	NSP's NG => TIPS Platform	unsolicited notification
File	Send	TIPS Platform => NSP's NG	request to send a file to the receiver
	Result	NSP's NG => TIPS Platform	outcomes of the sending of a file

Traffic	Send	TIPS Platform => NSP's NG	request to send a message to the receiver
	Result	NSP's NG => TIPS Platform	outcomes of the sending of a message
	Receive	NSP's NG => TIPS Platform	delivery of a message to the receiver

Multiple *command queues* shall be supported for each flow.

Multiple *traffic queues* shall be supported for each flow (Send, ReceiveIndication).

The name of queues shall follow the TIPS naming convention.

WMQ messages management - load balancing

Reference ID	TIPS.UC.TC.30325
--------------	------------------

The NSP shall manage the load balancing across WMQ traffic queues for outgoing messages (sent by the TIPS Platform) and incoming messages (sent by TIPS Actors). For outgoing messages the load balancing mechanism shall be based on traffic queue sharing (i.e. the same traffic queue should be read by multiple Network Gateways). For incoming messages the load balancing mechanism shall be based on a random choice (e.g. round robin mechanism) across the queues dedicated to each kind of flow.

WMQ message description section – CCSID

Reference ID	TIPS.UC.TC.30330
--------------	------------------

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

WMQ additional headers

Reference ID	TIPS.UC.TC.30335
--------------	------------------

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

WMQ message structure

Reference ID	TIPS.UC.TC.30340
--------------	------------------

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

The WMQ message structure which is used is described in the annex "MEPT Message Exchange Processing for TIPS", which is part of these requirements.

3.3. A2A message service

A2A traffic primitives management

Reference ID	TIPS.UC.TC.30345
--------------	------------------

The NSP shall manage the following primitives to exchange messages with the TIPS Platform:

- **SendRequest:** the TIPS Platform uses this primitive to send a message to the TIPS Actor
- **Notify:** the NSP's Network Gateway uses this primitive to notify a positive/negative outcome of the initial processing of a SendRequest or FileSend operation to the TIPS Platform;
- **ReceiveIndication:** the NSP's Network Gateway uses this primitive to deliver a message sent from the TIPS Actor to the TIPS Platform;
- **Technical Ack:** the NSP's Network Gateway uses this primitive to notify a positive/negative completion of the exchange;
- **FileSend:** the TIPS Platform uses this primitive to send a file to the TIPS Actor.

The A2A traffic primitives are described in the annex "MEPT Message Exchange Processing for TIPS", which is part of these requirements.

Message end to end information transport

Reference ID	TIPS.UC.TC.30350
--------------	------------------

The NSP shall allow the exchange of end-to-end information from the sender application to the receiver application together with the "instant" message (i.e. from the TIPS Actor to the TIPS Platform and vice versa). The following end-to-end information is envisaged (the exhaustive set of information is detailed in the MEPT annex):

- the identifier of the "instant" message
- a timestamp of the creation/submission of the "instant" message
- a Possible Duplicate Message indication
- additional accompanying data

Message unique identification

Reference ID	TIPS.UC.TC.30355
--------------	------------------

The NSP shall identify each exchanged "instant" message with a universally unique "network" message identifier. The unique "network" message identifier of every exchanged message shall be provided to the

receiver, together with the "instant" message, for diagnose and non-repudiation purposes. The unique "network" message identifier should be also notified to the sender, if needed.

3.3.1. A2A traffic protocol description

The protocol is described in the annex "MEPT Message Exchange Processing for TIPS", which is part of these requirements. Below a description of the major features and characteristics of such rules.

A2A Protocol description

Reference ID	TIPS.UC.TC.30360
--------------	------------------

All messages must be exchanged in "instant" mode with at most once delivery, no retries and certainty of the outcome of the delivery, either positive or negative. In case of doubt regarding the outcome of the delivery, no notification is needed.

The NSP shall manage the exchange of instant messages with TIPS in accordance with the annex "MEPT Message Exchange Processing for TIPS".

3.3.2. A2A gateway control application

A2A gateway control application

Reference ID	TIPS.UC.TC.30400
--------------	------------------

The TIPS Operator is the service provider of the TIPS service to the TIPS community. To properly fulfil this role, the following TIPS Platform specific requirements are set.

In order to reduce the impact of managing the functionalities over multiples NSPs the NSP shall provide to TIPS Platform a "Gateway control application" with an "easy-to-use" interface implementing the A2A traffic control functionalities.

The TIPS Platform will implement directly only the sending/receiving traffic exchange primitives. All the security aspects must be managed through this Gateway control application.

The NSP shall provide a description of the "easy-to-use" interface, to be approved by the TIPS Operator.

This requirement applies to the TIPS Platform only and is detailed in the annex "MEPT Message Exchange Processing for TIPS".

3.3.3. A2A requirements for "store-and-forward" transfer of files

Based on the different business requirements between "instant" messages and "store-and-forward" file transfer, it is envisaged that the NSP could provide a different solution for this data exchange.

Store and forward file transfer

Reference ID	TIPS.UC.TC.30405
--------------	------------------

The NSP shall provide a description of the solution for store-and-forward file transfer, to be approved by the TIPS Operator. The TIPS platform shall interact with the NSP following the set of rules described in the annex "MEPT Message Exchange Processing for TIPS", which is part of these requirements.

3.4. U2A requirements

User to Application (U2A) is delivered through a HTTPs connection.

This paragraph describes the flow of the U2A interactions:

At the end user site:

- The NSP checks whether 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 TIPS Platform
- The TIPS Platform will perform the identification and authentication of the end user based on the client certificate provided in the HTTPs request;

At the TIPS Site the TIPS Platform sends a (business) acknowledgement via HTTPs session.

U2A user authentication

Reference ID	TIPS.UC.TC.30545
--------------	------------------

The NSP shall distribute to the end users the credential to access the interface of the TIPS Platform. The NSP shall deliver the certificates for the U2A access to the end users (with a smart-card or a USB token).

U2A closed group of user authorisation

Reference ID	TIPS.UC.TC.30550
--------------	------------------

The NSP shall check the authorisation of the end users to access the TIPS Platform at Network level. The IP of the end user access point is checked by the NSP in order to authorise the access to the requested TIPS URL.

The end user is requested to open a VPN connection (performing identification and authentication) with the NSP in order to be able to establish a HTTPS session with the TIPS Platform.

3.5. TIPS Actor Emulator

TIPS Actor Emulator Access Point

Reference ID	TIPS.UC.TC.30655
--------------	------------------

The NSP shall provide to the TIPS Platform only a "TIPS Actor Emulator access point" to perform testing and monitoring (continuous and/or specific after any change implementation). This is needed in order to ensure a proper operational behaviour of the connectivity infrastructure of the TIPS Platform.

The TIPS Actor Emulator access point shall include:

- a connectivity infrastructure at one of the TIPS sites. The connectivity infrastructure shall be of the same type as the one provided to the TIPS Actor
- a minimal set of software components to manage simple message exchanges, i.e. to trigger message sending and to support message receiving, emulating the basic configuration of a TIPS Actor

The TIPS Operator should be able to use the TIPS Actor Emulator software without the need of any prior notice to the NSP.

4. Security services

Security is of paramount importance for TIPS, as very sensitive information will be exchanged between the TIPS 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 implementation of the need-to-do principle in access control mechanisms;
- the non-repudiation of the messages;
- the auditing 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 TIPS Identity Manager.

Technology and organisational processes

Reference ID	TIPS.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 TIPS infrastructure and information.

In this context, the NSP shall comply with the ISO27001:2013 standard.

Security Platform as a service

Reference ID	TIPS.UC.TC.41020
--------------	------------------

The NSP shall deliver the necessary technical infrastructure and software components to the TIPS Actor and to the TIPS Platform in order to allow the management of the TIPS security. The NSP shall ensure compliance with the TIPS security requirements set out in following sections.

Operational readiness

Reference ID	TIPS.UC.TC.41030
--------------	------------------

The NSP guarantees the operational readiness of all relevant security devices and components of its security platform according to the relevant service levels.

Encryption of all incoming and outgoing traffic

Reference ID	TIPS.UC.TC.42040
--------------	------------------

The NSP shall ensure confidentiality of all TIPS traffic over its Network.

The NSP shall ensure that its staff and other parties cannot access or copy data exchanged over its network except when subject to controlled access, under secure logging and reported to TIPS Operator.

Segregation of data

Reference ID	TIPS.UC.TC.42050
--------------	------------------

The NSP shall ensure that the TIPS Actor can only access its own incoming and outgoing traffic. No other party (including the NSP and its subcontractors) shall be able to access data without such access being subject to controlled access, secure logging and reported to the TIPS Operator. Nevertheless, the NSP can offer data analytics solutions to the Actors connected via the NSP, so that each Actor can have access to information related to their traffic sent or received.

Digest algorithms

Reference ID	TIPS.UC.TC.43060
--------------	------------------

The TIPS Actor shall use only strong and not deprecated digest (hash) algorithms for its Solution.
SHA-256 is the minimum required algorithm for the digest computation.

Integrity of traffic

Reference ID	TIPS.UC.TC.43070
--------------	------------------

The NSP shall not interfere with the integrity of any traffic exchanged between its TIPS Actor and the TIPS Platform.

Integrity of software components

Reference ID	TIPS.UC.TC.43090
--------------	------------------

The NSP shall ensure the integrity of its software components providing Connectivity Services and security features for TIPS.

The NSP shall automatically detect every planned and unplanned (intentional and accidental) modification and alert the TIPS Operator without undue delay. The NSP shall ensure its protection against malicious codes.

Integrity of audit logs

Reference ID	TIPS.UC.TC.43100
--------------	------------------

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

Audit log

Reference ID	TIPS.UC.TC.46240
--------------	------------------

All network devices provided by the NSP shall use a logging functionality. The NSP shall agree with the TIPS Operator which audit logs have to be stored on the TIPS storage devices and which may remain on the NSP's devices. The NSP shall provide to the TIPS Operator the security policy applied to these audit logs. Analogous documentation shall be provided whenever the NSP changes the mentioned policy, within one month after such changes are implemented.

Audit logging

Reference ID	TIPS.UC.TC.46250
--------------	------------------

The NSP shall log each data session established between the TIPS Actor and the TIPS Platform.

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

Monitoring facilities

Reference ID	TIPS.UC.TC.47260
--------------	------------------

The NSP shall deliver to the TIPS Operator the necessary facilities to monitor the NSP's network components which provide security features 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 any issues to the TIPS Operator using collaboration tools (such as e-mail, instant messages, smartphones).

Automated alerts

Reference ID	TIPS.UC.TC.47270
--------------	------------------

The NSP shall install alerts which are automatically triggered in case of relevant events. The alerts shall be immediately sent by the NSP to the TIPS Operator, using SNMP protocol (version 3 is required, however, the alerts that are logged locally on systems provided by the NSP and located at the TIPS Operator, can use SNMP version 1 or 3).

Change management

Reference ID	TIPS.UC.TC.47280
--------------	------------------

The NSP shall apply a strict change management procedure to its network components that provide security features for the TIPS Platform.

Network encryption failure

Reference ID	TIPS.UC.TC.47290
--------------	------------------

The NSP shall design and implement procedures to identify Network encryption failures which might not be identified by TIPS. The NSP shall design and implement procedures to resume the encryption functionality in such circumstances. The NSP shall notify these procedures to the TIPS Operator and any subsequent change thereto, upon implementation.

Encryption algorithms

Reference ID	TIPS.UC.TC.48300
--------------	------------------

The NSP shall implement the AES encryption algorithm with a minimum length of 128 bit for symmetric encryption keys and 2048 bit for asymmetric encryption keys.

Encryption devices

Reference ID	TIPS.UC.TC.48310
--------------	------------------

The NSP shall install encryption devices in all TIPS Sites. The NSP shall install encryption devices in all TIPS Actor's sites which are interconnected with the TIPS Platform.

The encryption devices shall comply with the security specifications stated herein.

Management of NSP encryption devices

Reference ID	TIPS.UC.TC.48320
--------------	------------------

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

The NSP shall enable a secure and resilient management of all encryption devices from all the TIPS Sites. The management of these devices shall be possible from a secondary site in case of component failure or disaster at the main site.

Unique identification of users

Reference ID	TIPS.UC.TC.44120
--------------	------------------

The NSP shall identify the TIPS Actor and the TIPS Platform in a unique way. The NSP shall guarantee the identification via digital certificates.

A2A Identification

Reference ID	TIPS.UC.TC.485100
--------------	-------------------

The NSP shall identify the TIPS Actor and the TIPS Platform every time they open a new session with the NSP's Network Gateway for A2A traffic. There is no end-to-end session. The NSP shall transfer the identity of the sender to the receiver. The NSP shall include this information in the network envelope provided to the receiver together with the message.

A2A Local Authentication

Reference ID	TIPS.UC.TC.485110
--------------	-------------------

The NSP shall authenticate the TIPS Actor and the TIPS Platform as local message partner every time they open a new session with the NSP's Network Gateway for A2A traffic exchange. The NSP shall use an appropriate mechanism for this purpose. An example of an "appropriate measure" is the use of the HMAC algorithm. If the HMAC algorithm is used, the symmetric key should be periodically renewed.

A2A Network Authentication

Reference ID	TIPS.UC.TC.485120
--------------	-------------------

The NSP shall authenticate the TIPS Actor and the TIPS Platform as network participant every time they open a new session with the NSP's Network Gateway for A2A traffic exchange. The NSP shall base this mechanism on the availability of the digital keys stored in a Secure Store accessible by the NSP's Network Gateways for this purpose.

The NSP shall always check the validity of the digital certificate issued for keys used to authenticate the TIPS Actor and the TIPS Platform. The digital keys used for authentication purposes shall be used for the digital signature.

A2A Non Repudiation support

Reference ID	TIPS.UC.TC.485125
--------------	-------------------

The NSP shall manage the non-repudiation of emission on instant messages sent by a sender to a receiver.

The Network Gateway (or the back-office application) of the sender party shall sign on behalf of the network participant (either TIPS Platform or TIPS Actor) using the appropriate private key stored in the HSM and referred to in a valid security context (established during the Network authentication phase).

The signature shall include the (digest of the) message payload provided by the sending application.

The signature data shall be delivered to the receiver together with the "instant" message. The Network Gateway of the receiver checks the validity of the certificate involved in the signature and verifies the signature by using the public key certificate of the signer.

The receiver should store all signature related information, as well as all signed data, for non-repudiation purposes.

The NSP shall provide a non-repudiation support service to verify the signature of a message. The service can be requested by network participants in order to help in case of dispute or claim.

The network participant shall provide all the necessary information required by the NSP to perform again the signature verification, such as the signature, all signature-related information and the traffic data to be validated.

The NSP shall be able to retrieve the certificate and the certificate status at the time of the signature.

The non-repudiation service shall be available up to three months after the traffic exchange took place.

4.1. Closed groups of users ("CGU")

Logically segregated groups of users

Reference ID	TIPS.UC.TC.45210
--------------	------------------

The NSP shall allow the creation and the removal of logically segregated groups of TIPS Actors or end users. The NSP shall manage all groups. In particular, the NSP shall create and manage the groups of TIPS Actors or end users for the production environment and for the test & training environments, one group for each environment.

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 relevant National Central Bank.

The activation date for the subscriptions shall be set at the latest within two weeks after the form's approval by the TIPS Operator; the new subscription shall be scheduled and activated ensuring the availability of the service (e.g. adopting the "rolling update" approach). Upon request from the TIPS Operator, the NSP shall withdraw from the CGU a TIPS Actor or an end user within one hour.

Segregation of traffic

Reference ID	TIPS.UC.TC.45220
--------------	------------------

The NSP shall ensure segregation of data traffic between different groups of users. TIPS Actors belonging to different groups cannot exchange data with each other. In particular, the end users and TIPS Actors belonging to the test & training groups shall not be able to send or receive messages from the production environment.

Physical and logical access control of the NSP's infrastructure

Reference ID	TIPS.UC.TC.45230
--------------	------------------

The NSP shall protect any essential network components used for its Solution with physical and logical access controls. In particular, the NSP shall protect the access to its administration interfaces.

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

4.2. Key management

The key management is the process that manages the life cycle of all the digital keys used in the encryption devices, for the TIPS Actor authentication mechanisms (i.e. digital certificates), and in signing off the configuration of the software components. It involves the use of both symmetric and asymmetric algorithms and the setup of an infrastructure able to store digital keys (i.e. PKI). TIPS Actors should use keys and certificates provided by the NSP.

Public Key Infrastructure

Reference ID	TIPS.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:

- Certification Authority,
- Hardware Security Modules.

Certification Authority

Reference ID	TIPS.UC.TC.48340
--------------	------------------

The NSP shall deliver Certification Authority (CA) functions to the TIPS Actor and the TIPS 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	TIPS.UC.TC.48350
--------------	------------------

The NSP shall deliver to the TIPS Operator 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	TIPS.UC.TC.48360
--------------	------------------

The NSP shall deliver to the TIPS Operator 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	TIPS.UC.TC.48370
--------------	------------------

The NSP shall provide tamper-proof HSM for storing all digital keys used for A2A. The HSM(s) shall be compliant at minimum with FIPS 140-2 Level 3 or Common Criteria EAL 4+ and they will be installed in the TIPS Sites.

Smart Cards or USB token

Reference ID	TIPS.UC.TC.48371
--------------	------------------

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

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;
- compatible with ISO 7816-1,2,3,4 specifications. T=0 and T=1 protocols;
- PC/SC for Microsoft driver;
- Microsoft Windows Hardware Quality Labs (WHQL) compliance;
- Operating Systems: Windows, Linux and Mac OS X.

Public Key Certificates

Reference ID	TIPS.UC.TC.48380
--------------	------------------

The NSP shall deliver to the TIPS Operator 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 a detail semantic profile of its public key certificates.

Certificate Extensions

Reference ID	TIPS.UC.TC.48390
--------------	------------------

The NSP shall deliver to the TIPS Operator 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	TIPS.UC.TC.48395
--------------	------------------

The NSP shall provide to the TIPS Operator a CRL in the HTTP, LDAP or OCSP formats. The TIPS Platform will select, together with the NSP, the most appropriate protocol for the intended performance.

Digital Signature management

Reference ID	TIPS.UC.TC.48396
--------------	------------------

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

Responsibilities for management of cryptographic keys

Reference ID	TIPS.UC.TC.48398
--------------	------------------

The management of cryptographic keys dedicated to the TIPS Platform shall remain under the sole responsibility of the TIPS Operator, which shall be the only institution having key management duties and physical access to the key storage devices (HSM) delivered by the NSP. The NSP may have logical access to the key storage devices only to perform administrative and operational tasks on the device (monitoring, initialization, software updates, etc). The NSP may have physical access to the key storage devices only to perform hardware replacement.

Administration of symmetric and asymmetric cryptographic keys

Reference ID	TIPS.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 the renewal of the keys. However, only the TIPS Operator shall define the frequency of exchange and the minimum length of keys used.
- *Renewal:* The NSP shall ensure that the 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	TIPS.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 TIPS production environment.

Security framework (adopted or proposed)

Reference ID	TIPS.UC.TC.49430
--------------	------------------

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

The TIPS Operator 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.

The action plan would have to be agreed either with the TIPS Operator, within the context of a third party assessment (i.e. for receiving a SSAE 16 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	TIPS.UC.TC.51010
--------------	------------------

The NSP has to develop a catalogue of Connectivity Services as part of the TIPS overall service catalogue to the TIPS Operator and the TIPS Actors. The content of the Connectivity Services catalogue, at the least, shall include a 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 TIPS, and the services the NSP offers including:

- Detailed Services,
- Service Levels, detailing performances, availability and support commitments,
- Volume related services,
- Support for dedicated connectivity solutions,
- Support for backup/Alternative network access solutions,
- Procedures to assure the continuity of the business Information about configuration and operation of the services

Operation and Escalation manual

Reference ID	TIPS.UC.TC.51020
--------------	------------------

The NSP shall provide the TIPS Operator with the following documents:

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

The NSP will be the owner of its manuals and is responsible for any updates. The TIPS Operator may submit its observations and comments to the NSP in order to ensure the accuracy of the manuals.

5.2. Support and Incident/Problem Management

5.2.1. Support Teams

The NSP shall offer to the TIPS Operator and the TIPS Actor a Service Desk service.

NSP Support Teams

Reference ID	TIPS.UC.TC.52030
--------------	------------------

The TIPS Operator and the TIPS Actor 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 procedures agreed on with the TIPS Operator as described in the Escalation Manual.

5.2.2. Trouble ticketing system

Trouble ticketing management

Reference ID	TIPS.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 TIPS Actor and by the TIPS Operator via the Internet.

Trouble ticketing report

Reference ID	TIPS.UC.TC.52050
--------------	------------------

The NSP shall provide to the TIPS Operator on a monthly basis a list of all severe, blocking and major incidents handled during the reporting period, including incidents where only TIPS Actors are impaired. This table shall

include at least the following information: case creation date/time, case closure date/time, impaired TIPS Actors, severity of the incident, incident description and reason for closure. Further details are recorded and available to the TIPS Operator upon request.

5.2.3. Operational incident management and escalation

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

Incident management and escalation

Reference ID	TIPS.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 TIPS Operator within 30 min.

The NSP shall produce and deliver an incident report to the TIPS Operator within 24 hours from the incident time. Such a report shall be produced also for violations of the service requirements set out in the Service level specification (TIPS.UC.TC.55020), when the criticality of the fault episode may be classified as *high*, according to the definition given therein.

The NSP shall inform the TIPS Operator in advance of any 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 TIPS network connectivity to the TIPS Platform. Upon detection of a connectivity failure by the NSP or notification of a connectivity failure by the TIPS Operator or the TIPS Actor, the NSP shall investigate the incident as set out below:

1. upon detection of a connectivity failure, the NSP shall immediately contact the TIPS Operator and/or the TIPS Actor 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 TIPS Operator/TIPS Actor, provided that the NSP and the TIPS Actor have agreed on such assistance, in order to perform a number of basic checks of the connectivity equipment at the TIPS Operator/TIPS Actor 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 TIPS Operator/TIPS 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 TIPS Operator upon request as part of the incident review activity.

Escalation of connectivity failures

Reference ID	TIPS.UC.TC.52070
--------------	------------------

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

5.3. Monitoring of the connection

Proactive monitoring

Reference ID	TIPS.UC.TC.53080
--------------	------------------

The NSP shall proactively monitor all permanent connections to the TIPS platform. 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	TIPS.UC.TC.53090
--------------	------------------

The NSP shall, on a monthly basis, report to the TIPS Operator 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 TIPS architecture and the rotation of the TIPS Sites.

5.4.1. TIPS Business Continuity and Rotation

Imperceptibility of the TIPS Business Continuity towards the TIPS Actors

Reference ID	TIPS.UC.TC.54100
--------------	------------------

The NSP shall support the TIPS Business Continuity imperceptibly to the TIPS Actor i.e. without any necessary intervention or impact on their technical configuration.

Periodic rotations of the TIPS Platform

Reference ID	TIPS.UC.TC.54110
--------------	------------------

The NSP shall support the TIPS Business Continuity in compliance with the TIPS-specified service levels, the periodic rotations (if needed) and backup procedures.

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

TIPS Business Continuity time objectives

Reference ID	TIPS.UC.TC.54120
--------------	------------------

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

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

No single point of failure

Reference ID	TIPS.UC.TC.54130
--------------	------------------

The NSP shall design and implement the technical infrastructure of its Solution for the TIPS Platform and shall configure its network components on each of the TIPS Sites 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	TIPS.UC.TC.54140
--------------	------------------

The NSP shall connect to the TIPS Platform Domain Name System to obtain automatically the current location of the services and URL for A2A and U2A. The TIPS 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.

It is also possible to agree with the TIPS platform alternative non DNS based solutions.

The NSP's Business Continuity

Reference ID	TIPS.UC.TC.54150
--------------	------------------

The NSP shall manage its disaster recovery solution, which affects the TIPS Connectivity Services, with the following objectives. In case of NSP recovery, the NSP shall support the traffic exchange through its back-up site automatically within 15 minutes.

5.5. Operation, administration and management

5.5.1. Availability indicators

Three types of indicators shall be used to measure the availability to the TIPS platform:

1. the **A2A message delivery time**, measuring the maximum time to deliver a message;
2. the **A2A Service Availability**, measuring the availability of the A2A services;
3. the **fault clearance**, measuring the Maximum Time to Recovery for a regional isolation, site isolation or WAN component failure recovery.

Separately from these availability indicators – and relevant to the TIPS platform only - the NSP shall be able to deliver to any TIPS Actor a SLA bilaterally agreed.

Service requirements – A2A message delivery time

Reference ID	TIPS.UC.TC.55010
--------------	------------------

The NSP shall deliver an “instant” message from the Sender to the Receiver in maximum 250 ms. The acknowledgment of the delivery sent back to the sender is not included in the delivery time.

The NSP shall commit on a Service Level of 95% of deliveries within the required delivery time.

Service requirements – A2A Service availability

Reference ID	TIPS.UC.TC.55020
--------------	------------------

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

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

Where:

1. Outage time is the sum of the outage time of each NSP connected Actor (in minutes) in the reporting period;
2. Service Time is the sum of the expected availability time of each NSP connected Actor (in minutes) in the reporting period.

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

The NSP shall describe in detail how the above measurements of the outage times are calculated.

Service requirements – **Fault clearance**

Reference ID	TIPS.UC.TC.55030
--------------	------------------

The NSP guarantees a fault clearance of the incidents affecting the connectivity between the NSP and the TIPS platform within the times defined in the following table, depending on the criticality of the identified fault:

	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

In order to establish its priority, the criticality of each fault episode may be classified as *high*, *medium* or *low*. The definition of the related levels is the following:

1. *high* (both TIPS 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* (the fault has only a slight impact on operations or it is a requests for information).

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

- Status Notification Interval (SNI): The TIPS Operator is informed about the fault status and the fault clearance progress at recurring intervals;

- Maximum Time To Intervene (MxTTI): maximum time elapsing between the acceptance of a trouble ticket and the start of the fault clearing process;
- Maximum Time To Repair (MxTTR): maximum time between the acceptance of a trouble ticket and the end of the fault clearing process².

5.5.2. Service Compliance Meeting

The TIPS Operator will continuously monitor the compliance of the NSP's Service with the requirements set by the Eurosystem.

Such compliance shall be discussed and reviewed in a monthly Service Compliance Meeting hosted by the TIPS Operator. For this purpose the NSP shall appoint a Service Manager that shall act as unique point of contact for all the Service Compliance related issue.

6. Implementation

NSP infrastructure sizing

Reference ID	TIPS.UC.TC.61030
--------------	------------------

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

The NSP shall size the infrastructure towards the TIPS platform in order to support the full traffic load (standard and peaks) managed by a single TIPS site, in case of maintenance or failure of one of the TIPS sites.

6.1. Project management

Connectivity Managers

Reference ID	TIPS.UC.TC.64040
--------------	------------------

The NSP presented by the TIPS Actor must appoint a Connectivity Manager (CM) who is the responsible central contact person coordinating all the required activities and who will communicate with the TIPS Operator over the entire term established by the Harmonised Conditions for TIPS.

The TIPS Operator will also appoint a CM (the "**TIPS CM**").

² MxTTR is temporarily suspended by the following events: 1. TIPS is not available to support or provision access to the faulty components, or 2. TIPS refuses to allow contractor personnel to enter the site, or *force majeure* (a circumstance due to an external, unpredictable event unrelated to computer operations and when that circumstance could not have been either foreseen or prevented with all due reasonable care).

NSP Connectivity Manager Duties

Reference ID	TIPS.UC.TC.64050
--------------	------------------

The CM will have the following duties:

- to maintain the relationship with the TIPS CM;
- to cope with all the issues relating to the NSP service provisioning and optionally escalating the problem to the responsible person(s) in the NSP's organisation;
- to identify the NSP's personnel in charge of the performance of services with an impact on security and to notify in written form their identities (names, picture ID, reserved information accessed) to the TIPS Operator immediately after their determination;
- to identify the NSP's personnel involved in the implementation who needs access to restricted areas within the TIPS Sites and to notify in written form their identities (names, picture ID, restricted areas to access, dates) to the TIPS Operator at the latest three (3) Business days before the installation of the necessary equipment at the TIPS premises;
- to prepare a monthly project progress report on the NSP installation schedule for the NSP service provisioning;
- to submit a final closure report at the end of the implementation;
- to monitor the deadlines of the implementation schedule;
- to have regular meetings with the TIPS Operator.