

T2S User Connectivity

- Technical Dialogue -

Silvio Orsini – Pietro Tarquinio

Banca d'Italia

Amsterdam, 26 October 2010

Disclaimer

The following slides summarise the main aspects of the current considerations of the Eurosystem with respect to the envisaged implementation of the T2S External Network solution.

Although some of the issues presented can be considered fairly stable and will most likely be part of the final decision, others are not, and might therefore be dropped or substantially altered. Consequently, these slides should by no means be used by any T2S Actor or potential T2S Network Service Provider to make any decisions or investments with respect to connectivity in T2S.

Summary



1. T2S communication interface
2. Various modes of communication
3. Security characteristics
4. Location and management of communication equipment
5. Service level and performance expectations

1. T2S communication interface

Introduction



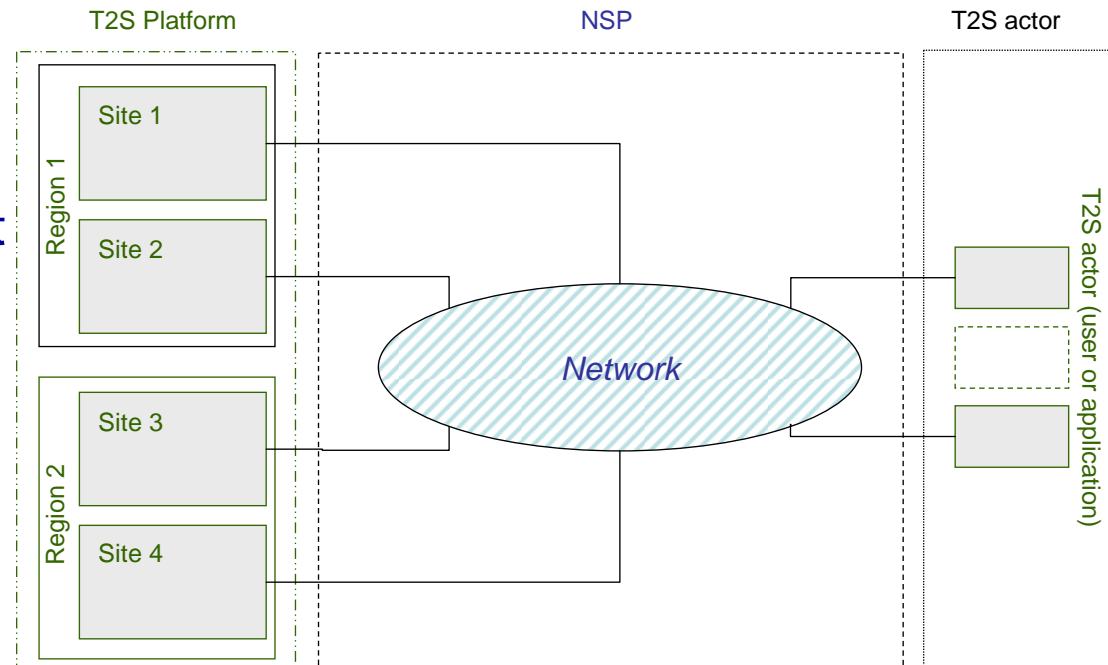
- The T2S platform widens over three Regions:
 - Region 1 Italy
 - Region 2 Germany
 - Region 3 France
- The remote access to the platform is enabled by Network Service Providers (NSPs)
 - Region 1 and region 2 are directly connected to the NSPs
 - Region 3 relies on the accesses to NSPs at region 1 & 2 (using the internal 4CB network)

1. T2S communication interface

General connectivity architecture



- The NSPs (up to three) are connected to the 4 sites avoiding any single point of failure
- The NSPs take into account T2S workload management and periodic swaps (i.e. rotation, recovery)
 - Users do not perceive in which Region a module is running
 - Rotation/recovery is transparent (no changes in user configuration is requested)



1. T2S communication interface

A2A communication protocol T2S - NSP



- Interface between T2S and the NSP is based on a T2S's protocol named DEP (Data Exchange Protocol)
- DEP is based on WebSphere MQ transport
- “Technical Ack” are exchanged between T2S and the NSP
- “Technical Ack” is based on the different types of WebSphere MQ report messages

1. T2S communication interface

A2A – sample message/file structure



<TechnicalEnvelope>

Technical header managed by the NSP GTW and by the T2S middleware (Sender, Receiver, Service Name,....)

</TechnicalEnvelope>

<BusinessEnvelope>

<BusinessApplicationHeader>

Signing information (e.g. signature of the sender) based on the MessagePayload section

</ BusinessApplicationHeader >

< BusinessArea>

Message or file payload

</ BusinessArea >

</ BusinessEnvelope >

- The Business Application Header contains the signature of the payload made with the end-user certificate
- Sender and Receiver information in the Technical Header are used by the NSP to perform “network addressing” and are based on the unique Distinguished Name (DN) of the digital certificate

1. T2S communication interface

A2A – sample message/file structure



- The NSP gateway shall validate the Technical Envelope of the message/file
- The (optional, according the sender's choice) compression of the payload is notified to the receiver by a flag in the envelope
- NSP services shall deliver the data once, and only once
- For each A2A service (message and file exchange), the NSP must adapt to the T2S' message envelope format

1. T2S communication interface

A2A communication protocol T2S – T2S actor



- End-To-End authentication and non-repudiation is based on the information from business application header (signature of the business content)
- End-To-End encryption on application layer is not foreseen (the NSP is trusted about the confidentiality)
- Identification is based on the unique Distinguished Name (DN) of the x509 certificate (the same DN is registered in the T2S static data)

1. T2S communication interface

A2A communication protocol T2S actor - NSP



- The network interface with the NSP at T2S platform and T2S actor side are technically decoupled
- How the interface between T2S actor and the NSP will be implemented is not specified by T2S
- It is up to the NSP and the T2S actor to decide if implement a non-repudiation protocol between them

1. T2S communication interface

U2A communication protocol



- The NSP shall support U2A connectivity enabling web traffic between T2S users' workstations and the T2S platform
- Transport protocol used to exchange data is HTTPs
- T2S user identification and authentication is based on the digital certificate used to establish the HTTPs session with the T2S platform

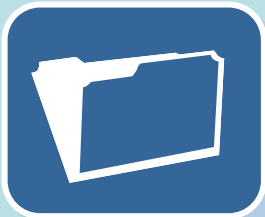
2. Various modes of communication

U2A and A2A services

Messages



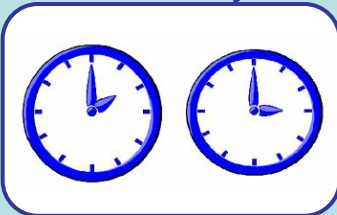
Files



Real Time



Guaranteed
Delivery



Push



Pull

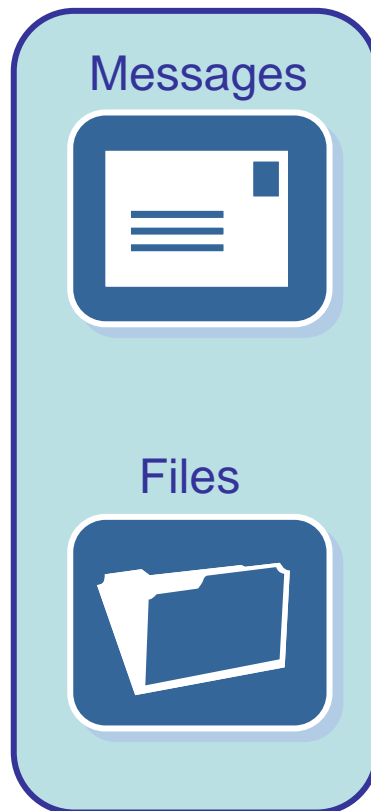


Browse



2. Various modes of communication

Message and file definition









- Data structure containing a financial instruction or information based on XML format (ISO20022 standard)
- Maximum length 32 KB

- Data structure containing two or more messages or data in a XML format (not only ISO20022)
- Minimum length 32 KB
- Maximum length 32 MB

NSPs shall give messages priority over files to better exploit the system throughput

2. Proposed modes of communication

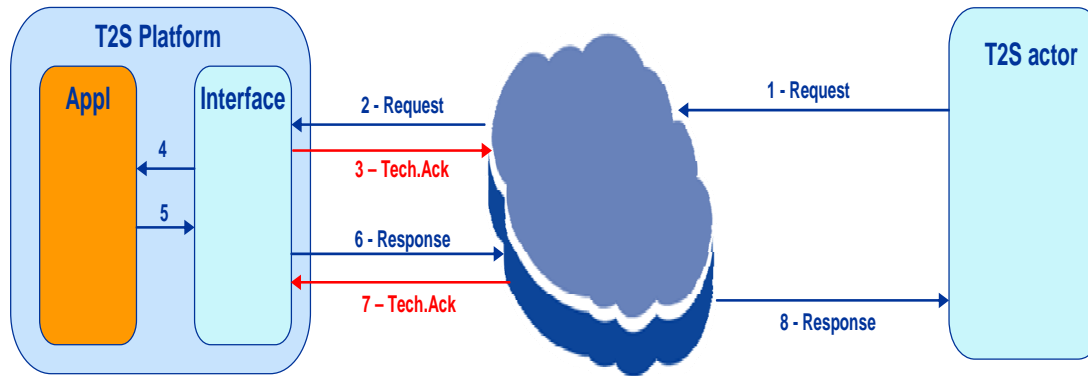
Mapping matrix

Messaging Services T2S Data Flows	A2A message Real Time	A2A message Guaranteed Delivery	A2A file Guaranteed Delivery	A2A file Real Time (pull) (to be checked)	U2A
Instructing (single) and event-based feedback					
Instructing (multiple)					
Query and response (U2A)					
Query and response (A2A)					
Report					

2. Various modes of communication

A2A Real-time message/file transfer only for query/response

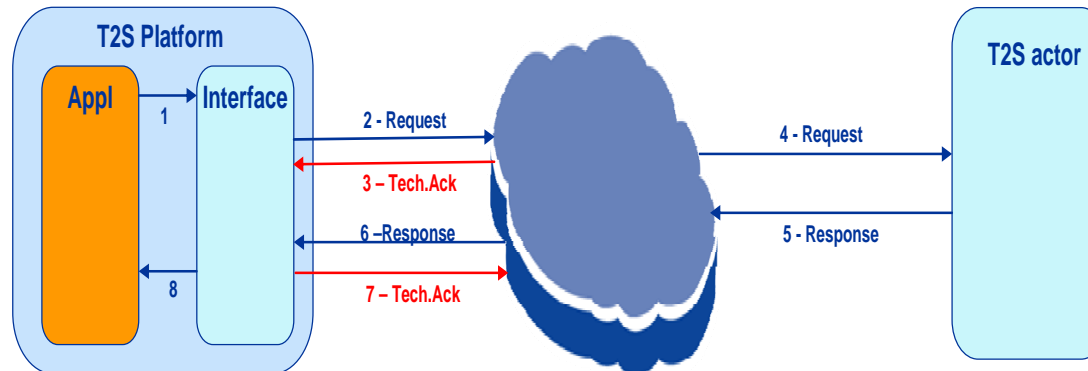
Incoming flow



- The sender and the receiver are available at the same time to exchange a message/file

- A real-time message/file exchange (request-response) shall be completed within NN seconds

Outgoing flow

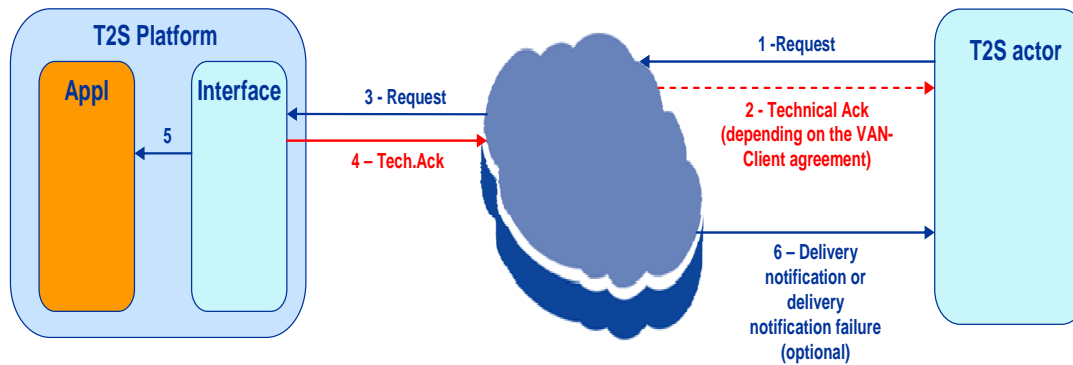


- If no response is received in this timeframe a “timeout” message shall be generated by the NSP and sent to the sender

2. Various modes of communication

A2A Guaranteed Delivery message/file transfer

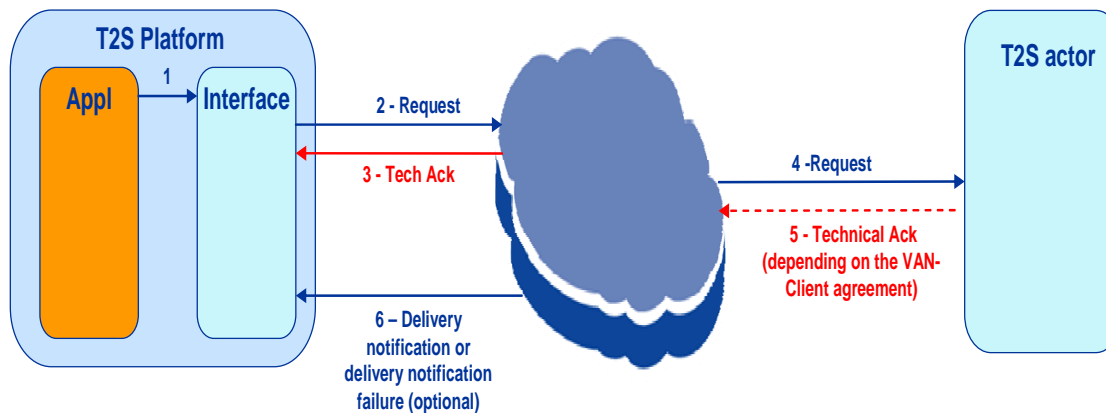
Incoming flow



- The sender can transmit file/message even when the receiver is not available

- The file/message is delivered by the NSP as soon as the receiver becomes available

Outgoing flow



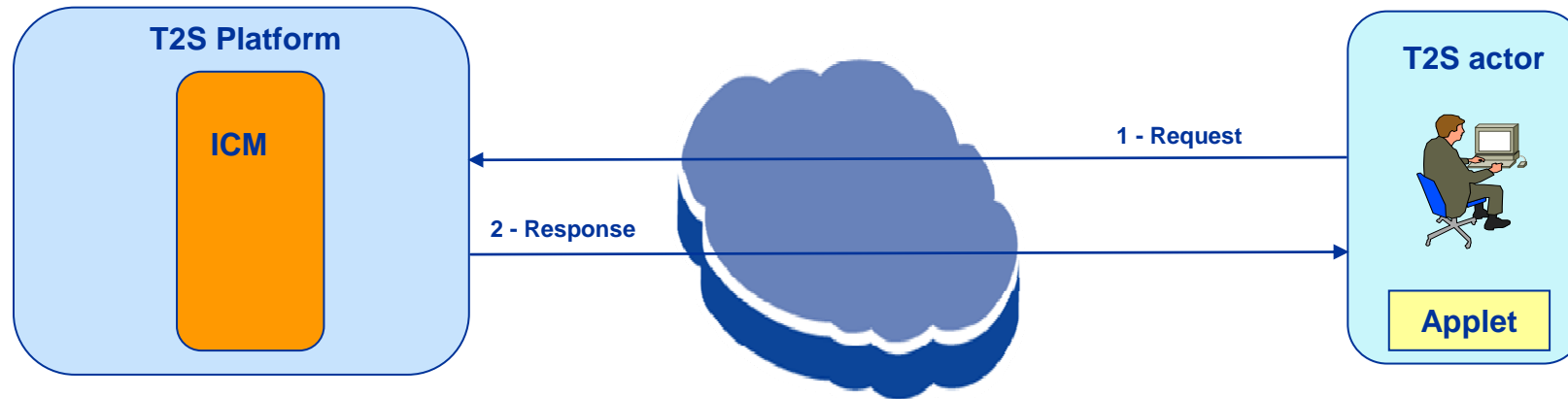
- NSP shall provide to the sender a delivery notification failure:

- after a maximum number of failed retries when the receiver is available (xx retries)

- after a number of days in case the receiver is not reachable (yy days)

2. Various modes of communication

U2A access to T2S platform



- NSP shall provide only the following services:
 - PKI (e.g. CRL, user certificates on token/smart card,...)
 - Connectivity
 - Closed group of users management (at network level)
- Update operations will be managed using an Applet (downloaded from T2S platform) on T2S actor side
- Update operations will be managed using ‘embedded’ signed XML over HTTPs POST

3. Security characteristics

Security features



- NSP shall provide the technical infrastructure to exchange messages in compliance with strict security requirements
 - Confidentiality
 - Integrity
 - User identification and access control
- 4CB staff shall
 - decide who is allowed to access the T2S logical domain
 - monitor the technical operations at the T2S interface of the NSP
 - manage all the encryption keys from T2S to the NSP

3. Security characteristics

Confidentiality



- End-To-End encryption on application layer is NOT foreseen (the NSP is trusted about the confidentiality)
- Each T2S actor shall be able to access its own traffic only
- No unauthorized party shall be able to access unencrypted data
- NSP shall assure the confidentiality of information on their internal network and in the communication with the T2S platform and T2S actor by means of traffic encryption

3. Security characteristics

Integrity



- The integrity of the data in transit shall be ensured
 - by the means of signing/encryption of network packets (TLS/SSL or IPsec) provided by the NSP
- The integrity of the network components and logs shall be ensured by appropriate access controls and audit logs (NSP to implement; 4CB staff to check)
- The NSP shall not use weak digest algorithms (e.g. SHA-1, MD5)
- The signing keys shall be different from the ones used for other purposes (e.g. encryption, authentication)

3. Security characteristics

User identification and authentication



- NSP shall identify the user in the institution by means of digital certificates
- The NSP shall handover to the T2S application
 - The sender/receiver unique name
 - The service name and service type
 - The relevant fields will be included in the Technical Envelope of the message/file

3. Security characteristics

Public Key Infrastructure (PKI)



- The NSP shall deliver the PKI
- Provided PKI shall be compliant with X.509 version 3 standard
- NSP shall deliver the following Certification Authority (CA) functions:
 - Generation
 - Management
 - Storage
 - Deployment
 - Revocation

of public key certificates to its T2S users and the T2S platform

- NSP shall provide interface to its PKI services to T2S platform and T2S actor

3. Security characteristics

Access restrictions



- NSP shall manage the access restrictions to different environments
 - test & training (INTEG, IAC, EAC, UTEST)
 - production
 - any additional
- NSP shall ensure logical message segregation between test & training and production environments
- NSP shall restrict the access to the A2A and U2A services to the authorised parties only
- NSP shall implement access restrictions on request of T2S

3. Security characteristics

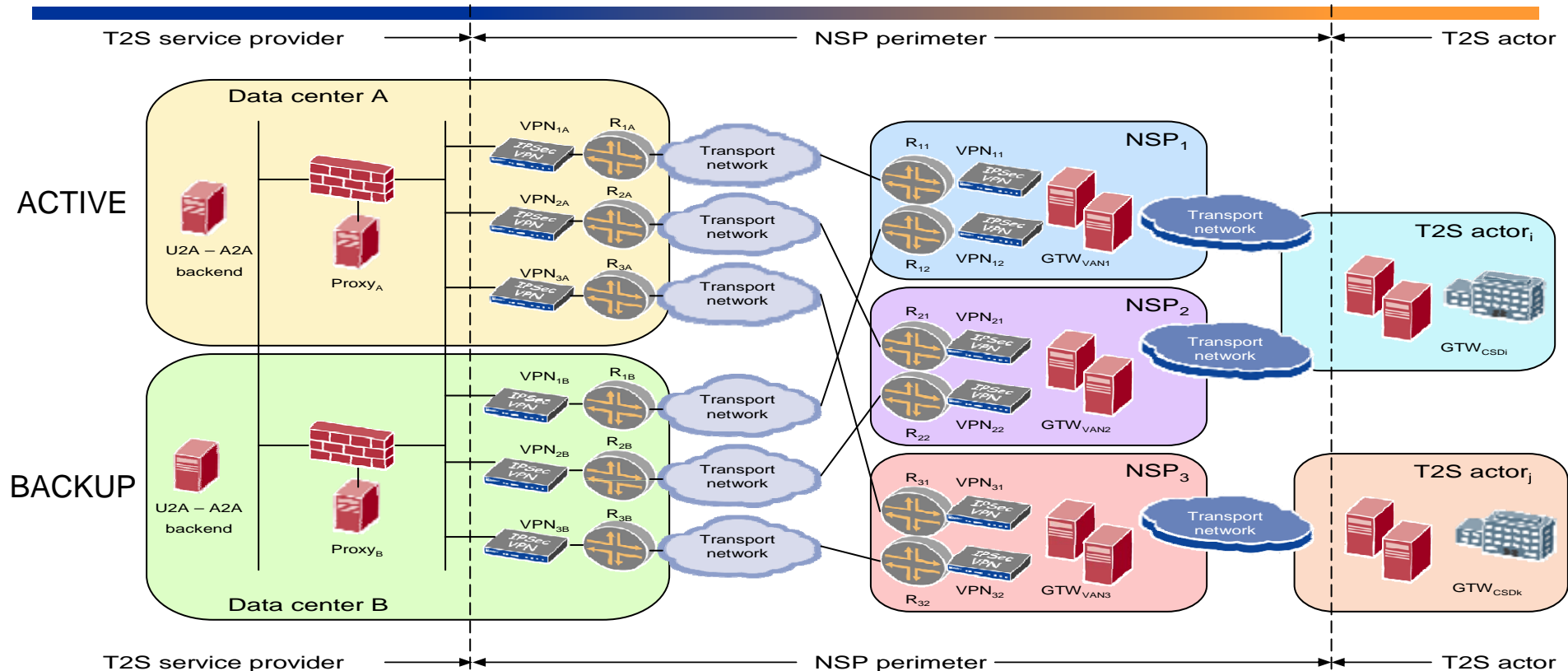
Management of encryption devices



- NSP shall install encryption devices in all the T2S platform site in Region1 and Region2
- NSP shall install encryption devices in all site of its T2S actor interconnected with the T2S platform
- NSP shall manage all its encryption devices under its responsibility
- In case of failure or disaster the NSP shall have a possibility to manage these devices in a highly secure remote way

4. Location and management of equipment

Overview



- In this figure only one Region is showed, the same configuration shall be implemented on the other one
- Location of equipment on the NSP providers and T2S actor side showed in this figure have to be considered only as an example

4. Location and management of equipment

Responsibility



- The NSP shall connect its equipment to the respective T2S communication endpoints at each T2S site in Region 1 and Region 2
- The demarcation line defining the responsibilities between T2S and the NSP shall be as described in previous slide figure
- It is up to the T2S actor to establish, with the network provider, the demarcation line defining the responsibilities between them, based on the gateway location and its management on T2S users side
- These two demarcation lines shall define the boundary of responsibility of the NSP provider. The NSP shall be fully responsible and liable for all services it offers to its T2S directly connected users and T2S within this boundary

5. Service level and performance expectations

Daily figures



Transactions		
Average day total	1.042.504	100%
Average night time	938.254	90%
Average daytime	312.751	30%

Average night-time volume and average day-time volume have an embedded margin of 20%.

- average number of xml messages (in and out) per settlement transaction [less than 6]
- more than 75% of the instructions should be received in big files [more than 200 instructions]
- more than 75% of the transactions are expected to be settled during the night time

5. Service level and performance expectations

Recovery of the NSP



- The NSP shall automatically manage its recovery, exploiting the redundancies, to assure the service continuity
- T2S is not going to rotate in case of the regional disaster of a single NSP (users of that NSP will not be able access T2S platform)
- Recovery from one NSP to another is a user responsibility

5. Service level and performance expectations

NSP sizing



- Each NSP shall size its infrastructure based on its expected market share (theoretically it can also be equal to 100%) and shall size the infrastructure to ensure it meets performance and volume requirements
- Capacity planning breakdown data shall be provided to T2S administrator every year (for sizing and monitoring purpose)

5. Service level and performance expectations

Service catalogue and manuals



- The NSP shall provide a catalogue of connectivity services for its customers as part of the T2S overall service catalogue
- Jointly with the 4CB staff, the NSP shall provide and maintain two reference manuals:
 - Operations manual, that describes the network related components installed in the premises of the Service Provider and contains the complete list of monitored elements
 - Escalation manual, that formalises the escalation process in normal and abnormal conditions

5. Service level and performance expectations

Support and Incident/Problem management



- Support Team:
 - the NSP providers shall offer to 4CB and the T2S actors a Service Desk service
 - the 4CB Teams shall be able to contact the NSP providers Support Teams 24 hours seven days a week during all year
- Trouble ticketing system:
 - the NSP providers shall record all actions, as well as the timestamp (time and date) at which the actions occur, in its central Trouble ticketing system
 - this information shall be made available to the 4CB upon request and as part of the periodic incident review activity
- The NSP providers shall provide:
 - initial response time for blocking problems: 15 min as a maximum
 - first status update time for blocking problems: 30 min as a maximum

5. Service level and performance expectations

Implementation requirements



- The NSP providers shall preliminary implement a proof of concept; the PoC infrastructure will remain as internal test environment for the 4CB (INTEG, IAC)
- The NSP providers shall support for implementing and executing integration and acceptance tests of the services
- Ad hoc training courses will be provided by the NSPs

5. Service level and performance expectations

T2S Business Continuity support



NSPs shall support T2S Business continuity without any user intervention or impact on user configuration

- in case of intra-region recovery, between primary and secondary site in the same region, on request of 4CB staff, NSPs are requested to switch the traffic in few minutes
- in case of inter-region recovery, between the two Regions, on request of 4CB staff, NSPs are requested to switch the traffic in few minutes
- on periodic rotation occurrence (e.g. almost every six months), the NSP must switch the traffic between the two Region, on request of 4CB staff, during a week-end, in few minutes (planned operation)

T2S User Connectivity - Technical Dialogue

Thank you for your attention

silvio.orsini@bancaditalia.it

(please specify in the mail subject "T2S TECHNICAL DIALOGUE")

Amsterdam, 26 October 2010