TARGET Instant Payment Settlement

NSP Compliance Check Procedure

Appendix 2 to the TIPS Connectivity - Technical Requirements

1.0

Author	4CB
Version	1.0
Date	23/03/2018

TABLE OF CONTENTS

1. Introduction

The "Connectivity - technical requirements" describe the technical requirements that the NSP has to fulfil. Each of these requirements is mapped into a test case and presented in this "Compliance Check Procedure". Acceptance tests are a series of tests on the different components delivered by the NSP (network, gateways, applications, etc) with a special focus on messaging services and security.

The TIPS project foresees the delivery of four different environments – TST, EAT, CRT, PRD – delivered progressively according to a specific planning and timing. Acceptance tests are run on the environment available at the time of testing and the availability of the testing environment is agreed bilaterally between the NSP and the TIPS Operator.

The entire compliance check process should be (successfully) completed by the end of July 2018 by those sponsored NSPs who apply as candidates to offer their connectivity services for the TIPS Go-Live (November 2018).

2. Scope of the document

This document describes the steps to access the compliance check process and drives the compliance checking assessment.

The acceptance test cases described in the document reflect the "Connectivity - technical requirements" comprehensively: 120 technical requirements are mapped into 120 acceptance test cases. Test cases are classified and grouped into six different sections based on their content:

- *Technical and operational* test cases
- *Network connectivity* test cases
- *Messaging services* test cases
- *Security services* test cases
- *Operational services* test cases
- *Implementation* test cases

3. Intended audience

Test cases are run by the TIPS Operator and the NSPs' technical staff under the coordination of the TIPS Operator itself.

4. The compliance check workflow

The criteria for accessing the compliance check are defined in the *TIPS Connectivity Guide*. For the reader's convenience, this section recalls the three most relevant steps:

- STEP 1 – Sponsorship
- STEP 2 – Project quality check
- STEP 3 – Running through the test cases

It is mandatory to pass Step 1 in order access Step 2 and it is mandatory to pass Step 2 in order to access Step 3.

4.1. STEP 1 – Sponsorship

The compliance check is initiated with the NSP receiving a sponsorship, either from a National Central Bank or from a TIPS Participant. In the latter case, this sponsorship should be communicated to the TIPS Operator by the relevant Central Bank. This is the very first step to trigger the start of the compliance assessment.

4.2. STEP 2 – Project quality check (evaluation of the Technical Offer)

In the Technical Offer, the NSP describes the overall architecture by analysing the solution (including technological implementation details from the physical layer to the application layer), the integration among the different components involved in the solution and how the various systems are managed through their respective element managers. The Technical Offer is expected to describe the Connectivity Services and an outline of the Technical Solution. A well written Technical Offer also illustrates how all the requirements are matched, i.e. correlating the implementation details of the solution to all of the Requirement IDs.
The Technical Offer will be evaluated by the TIPS Operator according to qualitative criteria: the simplicity and ease of management of the architecture as well as the ability to maximize the overall architectural performance with no impact on overall reliability. Poor quality of the Technical Offer and not matching all of the requirements are both considered clauses of immediate exclusion. The outcome of the evaluation of the Technical Offer by the TIPS Operator is not disputable. However, sponsored NSPs who fail to pass this step, but are still interested in offering their connectivity services, may apply with a revised Technical Offer for the second wave, six months after the TIPS Go-Live (June 2019).

4.3. STEP 3 – Running through the test cases

All tests will be conducted on site in cooperation between the TIPS Operator and the NSP. If no TIPS Actors are ready at the time of testing, they will be emulated by a TIPS Actor emulator (installed on the NSP and/or TIPS Operator sites). Test cases are uniquely identified, and numbered, using the "Reference ID" field, corresponding to the related Technical Requirement.

Every test case has six components:

1. *Description*: this section reflects the requirement (taken as-is from the "Connectivity - technical requirements");
2. *Expected result*: what is the test about, what functionality/environment is under test;
3. *Detailed test procedure*: how to perform the test;

4. *Outcome*: defines the test's expected outcome and the expected conclusion reached through a successful testing process;
5. *Result*: a test can either fail or pass, if it fails then a follow up action is triggered, if it passes then no follow up action is needed and it is possible to proceed straight to the next test;
6. *Formal acceptance*: contains the signatures of the TIPS Operator testing team staff and the NSP testing team staff that performed the test, formally accepting the test result.

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

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

If the NSP foresees an entire or partial reuse of an existing infrastructure – which may be already in place for other purposes (i.e. T2 or T2S) – then all tests have to be run entirely from scratch in order to ensure a level playing field.

4.3.1. Acceptance Test Criteria

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

4.3.2. Entrance criteria

As an entrance criterion, the NSP passes Step 1 and Step 2 and then communicates to the TIPS Operator that its Network is ready for acceptance testing. The NSP provides to the TIPS Operator confirmation of the successful completion of the NSP's internal tests. After the TIPS Operator confirms the Compliance Check Procedure can be started, an acceptance entrance meeting is held where the TIPS Operator and the NSP agree to start acceptance testing activities.

4.3.3. Acceptance criteria

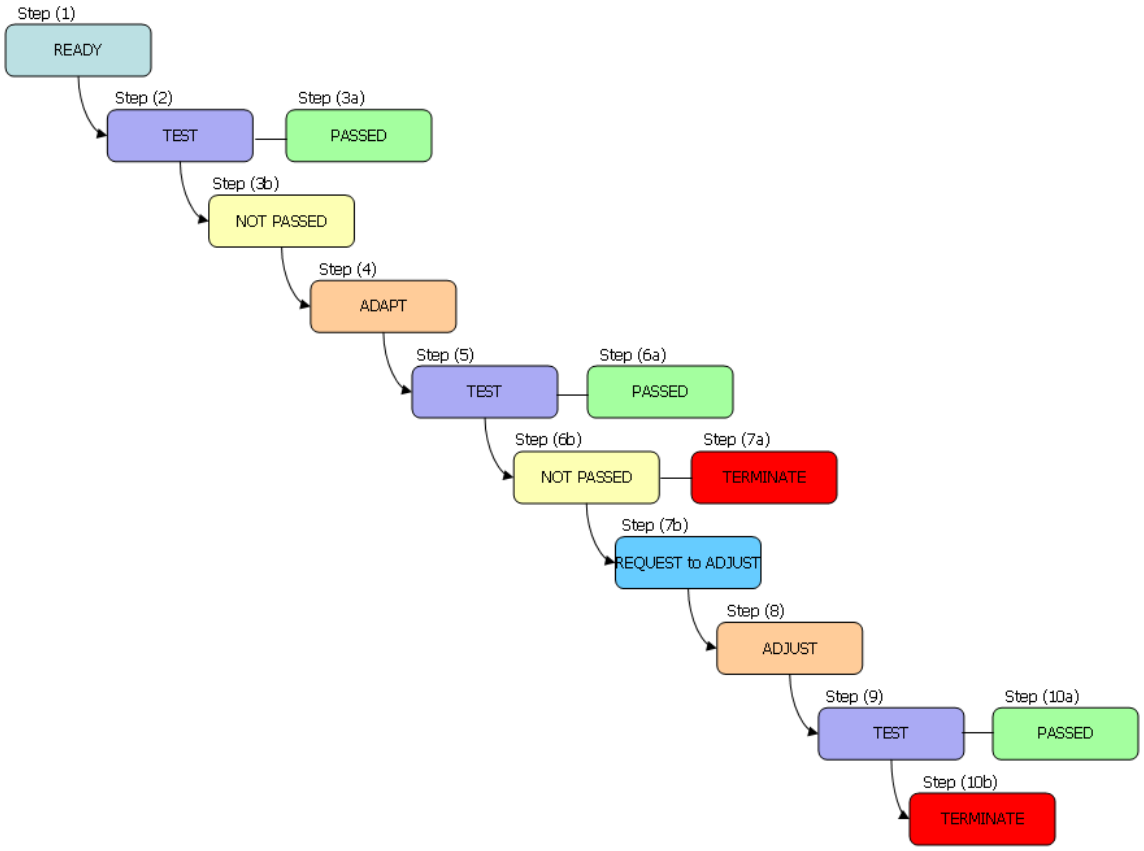
The acceptance testing phase is completed when the flow described in the "Connectivity - technical requirements" is completed and when all of the following conditions are matched:

- all acceptance test cases have been executed;

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

The Compliance Check Procedures acceptance criteria are defined in a flow described in the "Connectivity - technical requirements".

The following picture gives a visual representation :



The acceptance flow can be split into 10 different steps: (step 1) ready for acceptance, (step 2) performing the tests, (step 3a) all tests are passed, or (step 3b) some tests are not passed, (step 4) adapt[1], (step 5) tests are repeated, (step 6) some tests are not passed, (step 7a) terminate (i.e. test case is failed), or (step 7b) request to adjust, (step 8) adjust, (step 9) tests are repeated, (step 10a) all tests are passed, or (step 10b) terminate (i.e. test case is failed).

4.3.4. Termination criteria

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

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

5. Common definitions

- Desk Check: some tests are run on the field, while other tests are run as a desk check. A desk check in the Compliance Check Procedure focuses on the formal availability of the documentation. The evaluation is usually done as a paper-based proofreading. It aims at identifying errors and gaps at an early stage of the evaluation. A desk check assumes the testing engineers make sure to have traversed through all possible paths and make use of every scenario that has been assessed.
- Eurosystem: The European System of Central Banks (ESCB) consists of the European Central Bank (ECB) and the national central banks (NCBs) of all 28 member states of the European Union (EU).
- Region 1 includes TIPS site A and B.
- Site A is Banca d'Italia's main data centre: Centro Donato Menichella, Largo Guido Carli, 00044 Frascati (RM)
- Site B is Banca d'Italia's secondary data centre: Largo Bastia, 35, 00181 Roma (RM)
- TIPS Actor Emulator: message routing software emulating a real TIPS Actor
- TIPS Operator: Banca d'Italia is the TIPS Operator
- TIPS Platform is the TIPS infrastructure run by the TIPS Operator and hosted in sites A and B.

6. Test cases

6.1. SECTION I - General Service Description - Test Cases

Technical infrastructure

Reference ID	TIPS.UC.TC.11010

Description:	The Network Services Provider (NSP) has delivered 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 hosted in two datacentres (TIPS site A and TIPS site B) in Rome – Italy (Region 1).
Expected result:	Technical infrastructure (HW) and software (SW) components have been delivered by the NSP and are in place. All equipment and applications have been delivered.
Detailed test procedure:	Define a part list containing all of the NSP components necessary to support the test phase or reuse a part list from an existing detailed technical design, ie. testing team is aware of all of the components part of the technical infrastructure (desk check). Check against the list and verify jointly that all HW and SW has been installed and configured (on field). The NSP is then allowed to deliver additional HW and SW at a later stage.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Delivery point for Connectivity Services

Reference ID	TIPS.UC.TC.11050

Description:	The NSP has delivered Connectivity Services to each of the TIPS sites.
Expected result:	Connectivity Services have been delivered to each of the TIPS sites (site A and B). All Wide Area Network (WAN) links are installed, all Virtual Private Networks (VPN) have been deployed and so are messaging services gateways (ie. Network Gateways).
Detailed test procedure:	Verify that Connectivity Services are in place (the Connectivity Services could include routers for the WAN links, IPSec VPNs appliances, and Network Gateways). The test focuses on the Connectivity Services availability on the TIPS Platform, rather than what is present on the NSP site or the TIPS Actor site.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Location of equipment

Reference ID	TIPS.UC.TC.11060

Description:	The NSP has installed all the necessary devices to ensure the connectivity to the TIPS Platform (e.g. routers, VPN devices and Network Gateways) inside the TIPS Operator premises (i.e. inside each TIPS Site). The NSP has connected its equipment to the respective TIPS communication endpoints at each TIPS Site.
Expected result:	The TIPS Platform is connected to the Network Service Provider. NSP's equipment is connected to the TIPS communication endpoints. All equipment has been deployed at all TIPS Sites.
Detailed test procedure:	Verify that TIPS Platform is equipped with the all equipment necessary to connect the TIPS Platform to the NSP, such as link termination devices, routers, VPNs appliances and TIPS Actor Emulator (if any).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Hosting agreement

Reference ID	TIPS.UC.TC.11065

Description:	Terms and Conditions for hosting provisioning are detailed in attachment to the Harmonised Conditions for TIPS.
Expected result:	A hosting agreement – between TIPS Operator and the NSP – is formally (ie. contractually) finalized.
Detailed test procedure:	Verify both TIPS Operator and the NSP adhered to the hosting terms and conditions.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

The boundaries of responsibility

Reference ID	TIPS.UC.TC.11070

Description:	The demarcation line defining the responsibilities between TIPS Operator and the TIPS Actor is the network interface between the NSP's gateways and the TIPS Platform's. For the avoidance of any doubt, such demarcation line defines the boundaries of the responsibilities of the TIPS Actor (the NSP's gateway is the physical boundary of responsibility). The latter is fully responsible and liable for all NSP's failures within this boundary.
Expected result:	A clear boundary of responsibilities has been defined. There are no striking issues between the two counterparts, all services and responsibilities have been clearly identified.
Detailed test procedure:	Verify in the contractual framework that the boundary of responsabilities between TIPS Actor and TIPS Operator are clearly identified, for both the service perspective and the physical perspective (Network Gateway interface). If during the tests no contract is already in place between the NSP and the TIPS Actor, then verify the contract template (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Chain of trust relationship

Reference ID	TIPS.UC.TC.11080

Description:	The TIPS Actor is responsible for ensuring that the requirements expressed in the "Connectivity - technical requirements" (e.g. performance, security) are satisfied also inside the NSP domain and in the relation with their NSP.
Expected result:	An end-to-end chain of trust relationship has been established - where on one end there is the TIPS Platform and on the other the TIPS Actor - with the NSP in between. All requirements in the "Connectivity - technical requirements" are met.
Detailed test procedure:	Look for a formal evidence that all the requirements (eg. performance and security) in place between the TIPS Platform and the NSP are also in place between NSP and the TIPS Actor. If during the tests no contract is already in place between the NSP and the TIPS Actor, then verify the contract template (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Independence of interfaces on TIPS and TIPS Actor's sites

Reference ID	TIPS.UC.TC.11090

Description:	The NSP ensures that the technical solutions it adopts for the interface with the TIPS Actor do not affect technical solution adopted for the interface with its TIPS Platform. The NSP and its TIPS Actors have agreed on and established a connectivity interface on their site(s). These two interfaces are technically decoupled by means of the NSP's services, so that technical choices on one interface does not affect the other.
Expected result:	There is a full independence between the connection of the TIPS Platform to the NSP's interface on one hand and the NSP's interface to the TIPS Actors' interfaces on the other. The NSP technical solution adopted for the interface TIPS Platform / NSP did not affect technical solutions adopted for the interface on the NSP / TIPS Actor. Any change on the TIPS Platform / NSP has no impact on the NSP / TIPS Actor interface and vice versa.
Detailed test procedure:	Part I: Apply a change on the TIPS Platform / NSP interface and verify that there is no impact on the TIPS Actor. Part II: Apply a change on the NSP interface / TIPS Actor and verify that there is no impact on TIPS Platform. Please note the change can be as simple as possible; during the actual running of the test, it is possible to negotiate between the TIPS Platform and the NSP a change simple enough to demostrate the interface independency, but quick enough to avoid requiring a new version of software to be released to the TIPS Actor (for example, add a new communication queue between NSP and TIPS Platform and between NSP and TIPS Actor).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED

	[] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Single interface on the TIPS Site

Reference ID	TIPS.UC.TC.11100

Description:	The NSP is compliant with the TIPS interface as described in Chapter 3 of "Connectivity - technical requirements" document. The NSP has provided connectivity between the TIPS Platform's application and the TIPS Actor's application.
Expected result:	Middleware and/or gateway functions link the TIPS application to the NSP's Connectivity Services through the usage of the MEPT (Message Exchange Processing for TIPS).
Detailed test procedure:	From an application point of view, the test cases specified in "SECTION III - Messaging Services", if passed, will implicitly verify this requirement. From an infrastructure point of view, the previous test cases in this section, if passed, will implicitly verify this requirement.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Interface on the TIPS Actor's site

Reference ID	TIPS.UC.TC.11110

Description:	The interface on the TIPS Actor's site does not lower the overall level of compliance of the Connectivity Solution with the TIPS security requirements, and it does not affect by any means the interface on the TIPS Platform site (i.e. does not require any special handling on the TIPS site).
Expected result:	The interface on the TIPS Actor does not lower the TIPS Platform compliance to the security requirements.
Detailed test procedure:	TIPS security requirements are defined in the Market Infrastructure Security Requirements and Controls (MISRC) and the Market Infrastructure Cyber Resilience Requirements (MICRR). MISRC is the ISO 27002:2013 where every "should" was changed into a "must", plus few customizations related to the Market Infrastructures (T2, T2S, TIPS and ECMS). MICRR is a set of controls derived from the Committee on Payments and Market Infrastructures (CPMI) / Board of the International Organization of Securities Commissions (IOSCO) "Recovery of financial market infrastructures", removing all controls already overlapping with the MISRC. The ISO 27002:2013 is available here and the CPMI/IOSCO "Recovery of financial market infrastructures" is available here. Option I: In case two conditions occur: (i) the NSP has a Security Programme containing security controls derived from both the ISO 27002 and the CPMI/IOSCO and (ii) the TIPS Actor is legally binded to have a full compliancy to the NSP Security Programme, then the test team (TIPS Operator and the NSP) will assess only the security controls not already included/covered in their Security Programme. Option II: In case either the NSP has either no Security Programme or the TIPS Actor are not legally binded to have a full compliancy to the NSP Security Programme, then the test team will assess the TIPS Actor compliance against the security requirements contained in the two deliverables (ie. ISO 27002:2013 and CPMI/IOSCO "Recovery of financial market infrastructures").
Outcome:	_____

	_____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Security of interface at TIPS Actor's site

Reference ID	TIPS.UC.TC.11115

Description:	The NSP has delivered 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 has ensured that the security measures implemented on the TIPS Actor interface are at the same level as the ones implemented for the TIPS Platform interface.
Expected result:	TIPS Actor interface complies with the TIPS security requirements delivered from the NSP to the TIPS Actor. The documentation proves that the security measures implemented on the TIPS Actor interface are compliant with the TIPS security requirements, and are at the same level of the TIPS Platform interface.
Detailed test procedure:	Verify the NSP has delivered to the TIPS Actor the security requirements related to the local interface. Testing teams jointly check the documentation supplied by the NSP addressing the security aspect of the interface on the TIPS Actor's site. Both parts of the test are a desk check. Part I The security requirements in the NSP's documentation must be compliant with the TIPS security requirements. Part II Check that the security measures on the TIPS Actor interface are at the same level of the security measure implemented on the TIPS Platform interface.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Monitoring facilities

Reference ID	TIPS.UC.TC.11130

Description:	The NSP has provided 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.
Expected result:	TIPS operator is able to monitor the NSP's technical operations, because TIPS Operator has received facilities allowing this monitoring. All failure events between the NSP and the TIPS Platform are visible on the monitoring facility and an alarm is triggered.
Detailed test procedure:	The technical operations monitoring facility records and shows recent events. Simulate a Connectivity Services failure and check the relevant event reported on the monitoring facility. Restore to normal operation and verify the event is cleared. For example : 1. Simulate a WAN failure and check the relevant indication on the monitoring facility. Restore to normal operation. 2. Simulate a VPN failure and check the relevant indication on the monitoring facility. Restore to normal operation. 3. Simulate a Network Gateway failure and check the relevant indication on the monitoring facility. Restore to normal operation.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Time synchronisation

Reference ID	TIPS.UC.TC.11140

Description:	In order to make the data exchange time consistent the NSP has synchronised 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 is at least every one minute. The official time of TIPS system is the ECB time, i.e. the local time at the seat of the ECB. NSP has provided time information using Coordinated Universal Time (UTC) format.
Expected result:	NSP's devices are date and time synchronised with the TIPS Platform, using either TIPS Platform's time source or Stratum 2 or 3 time source. Time information comes in UTC format and the synchronisation occurs at least every minute. NSP's devices are date and time synchronised with the expected time sources. Time format and synchronisation interval are compliant with the requirements. Reference terminology is described in Request for Comments 5905 "Network Time Protocol Version 4: Protocol and Algorithms Specification".
Detailed test procedure:	Verify that all the NSP devices adopt a Network Time Protocol (NTP) synchronized with a time source. Check the compliance of the time source with the ones approved by the TIPS Operator. Check the synchronisation interval, the time format and the Stratum level.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.2. SECTION II - Network Connectivity - test cases

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

Reference ID	TIPS.UC.TC.20100

Description:	The NSP has delivered to all 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.
Expected result:	It is possible to identify a demarcation line between the NSP and the TIPS Platform. The Ethernet interface of the Gateway toward the TIPS platform is clearly marked.
Detailed test procedure:	The NSP delivered at the both TIPS Sites A and B one or more network devices. Identify the NSP's Gateway interface setting the demarcation line between the NSP and TIPS.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

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

Reference ID	TIPS.UC.TC.20102

Description:	The NSP has ensured 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 can handle the whole traffic.
Expected result:	The NSP has to ensure that the link bandwidth to each single TIPS site (A or B) is able to handle the whole traffic. In the case of a site failure the link to the remaining TIPS site is expected to handle the whole traffic.
Detailed test procedure:	During part I and part II A2A message traffic is coming simultaneously from the TIPS Actor to the TIPS Plaform and from the TIPS Platform to the TIPS Actor. Part I: The NSP disables the Ethernet interface(s) at TIPS site A that are part of the demarcation line between the NSP and TIPS (cfr. TIPS.UC.TC.20100). The whole traffic is handled by the remaining link connected to the TIPS site B. When test outcome is recorded please restore the initial condition. Part II: The NSP disables the Ethernet interface(s) at TIPS site B that are part of the demarcation line between the NSP and TIPS (cfr. TIPS.UC.TC.20100). The whole traffic is handled by the remaining link connected to the TIPS site A. The test is initially run with a 10% capacity of the overall bandwidth and the NSP gives evidence of being able to achieve the 100%.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED

	If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Service requirements - **Monitoring**

Reference ID	TIPS.UC.TC.20105

Description:	The proposed infrastructure is monitored and maintained by NSP.
Expected result:	The NSP gives evidence that all his components are monitored both by the NSP itself and the TIPS Platform.
Detailed test procedure:	1. List NSP's components; 2. Jointly assess how the NSP monitors the infrastructure (ie. provides evidence of the monitoring operational procedures), it is allowed to run this test as a desk check; 3. SNMP traps from the NSP's components are sent to the TIPS Platform monitoring systems; 4. Check on the TIPS Platform monitoring systems for evidence of received SNMP traps.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

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

Reference ID	TIPS.UC.TC.20107

Description:	All the TIPS Sites are served by the WAN links of the NSP. The NSP has insured 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 are 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 specified where each regional/local PoPs are located.
Expected result:	Sites A and B are both served by the NSP. The TIPS Sites are served and interconnected to the NSP's PoPs with redundant and direct links with physical diversification. All TIPS Sites are connected to all NSP's sites; both TIPS Sites are connected to the NSP's PoP with redundant and direct links with physical diversification.
Detailed test procedure:	Part I: Conduct a site survey to the two TIPS Sites (A and B) and verify the WAN services links are available to interconnect to the NSP. Part II: The NSP is expected to provide maps describing the local metro connectivity. Verify – desk check – that the links between NSP PoPs and each TIPS Site are provided with redundant and direct links with physical diversification.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 1 requirement - **Link bandwidth**

Reference ID	TIPS.UC.TC.20108

Description:	Each link is initially delivered with a minimum bandwidth of 1Gbps. It is possible to reuse existing interfaces (if any).
Expected result:	Each link has an available minimum bandwidth of 1Gbps. The test is initially run with a 10% capacity of the overall bandwidth and the NSP gives evidence of being able to achieve the 100%.
Detailed test procedure:	During the test the NSP temporarily delivers an IP packet generator. Install the IP packet generator on the TIPS Site under test and install either a packet receiver at the corresponding NSP site or a loop, generate a sustained traffic flow of 100Mbps at one end and verify all traffic is received at the other end. IP traffic profile is IMIX. Continue the test for an hour. Repeat the procedure for each of the available WAN links and each of the TIPS Site. The IP packet generator is removed when tests are completed.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 1 requirement - **Link latency**

Reference ID	TIPS.UC.TC.20115

Description:	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.
Expected result:	Each link (ie. between the TIPS Sites and the TIPS Actor) has a one way delay of maximum 40 msec.
Detailed test procedure:	The test focuses on measuring the overall latency from the TIPS Actor to the TIPS Platform. If a TIPS Actor is available then: Part I (site A): Either deploy two GPS synchronised packet generators (one at the TIPS Actor and the other one at the TIPS Platform) or deploy one GPS synchronised packet generators at one link end (ie. at the TIPS Platform) and a loop at the other link end (ie. at the TIPS Actor), then generate IP packets at 100Mbps for 1 hour, then measure latency at the WAN link ends. IP packets have an IMIX profile. Measure the average round trip latency and divide it by two; this value should be less than or equal to 40msec. Part II: Repeat the test for site B If a TIPS Actor is not available then: Part I (site A): Same as above, but install the generator at the NSP site and expect a value less than or equal to 20msec. Part II: Repeat the test for site B
Outcome:	_____ _____ _____

Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

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

Reference ID	TIPS.UC.TC.20135

Description:	The NSP delivered to TIPS the connectivity service via network equipment having 1 Gigabit Ethernet ports.
Expected result:	WAN links are physically delivered via network equipment with 1Gbps Ethernet local interface.
Detailed test procedure:	Visually inspect the network terminating equipment and verify it has either a 1000Base-T interface or a 1000Base-SX one.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 1 requirement - **Path diversification**

Reference ID	TIPS.UC.TC.20140

Description:	Paths from the TIPS site to local NSP POPs are served by local loops. Each local loop has a diversified path from the site to the POPs. Paths are also diversified from the POP to the backbone and throughout the whole path across the backbone itself.
Expected result:	All local loops, POPs and backbone connections are diversified end-to-end (from the TIPS sites to the NSP sites) and share no common infrastructure. There is a full path diversification and this diversification is verified.
Detailed test procedure:	The NSP delivers detailed maps containing all the local loops physical paths from TIPS sites to NSP's POP (this part has already been covered with test TIPS.UC.TC.20107). Now the NSP describes with a high level map how paths are diversified across the backbone (ie. from NSP's POP on the TIPS metro area to NSP's POP in the NSP metro area).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 1 requirement - **Links responsibility**

Reference ID	TIPS.UC.TC.20145

Description:	The NSP maintains 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.
Expected result:	Links – from the TIPS Sites to the NSP Sites - are under the NSP responsibility, the NSP takes care of maintaining the links (ie. monitoring and servicing the links) and ensuring the agreed diversification is guaranteed in time.
Detailed test procedure:	The NSP documentation about physical paths, the underpinning contracts with the local carriers is jointly analysed and gaps are eventually flagged (if any). The NSP delivers detailed maps containing all the physical paths from TIPS sites to POP. The NSP describes with a high level map how paths are diversified across the backbone from POP to POP.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 3 requirement - **IPv4**

Reference ID	TIPS.UC.TC.20155

Description:	Internet Protocol (IP) version 4 (IPv4) protocol is used between the TIPS Platform and the TIPS Actor.
Expected result:	All traffic between the TIPS Platform and the NSP and between the NSP and the TIPS Actor is all IPV4.
Detailed test procedure:	Part I: Jointly inspect the documentation describing the Network, including network diagrams and verify only IPv4 addresses are transported on the service boundaries. Part II: Capture traffic at service bounadries with a network analyser and verify only IPv4 packets are transported across the network. Create a span port on the local 4CBNet DMZ switch and mirror incoming and outgoing traffic from the port where the Network Gateway is connected. Verify there is no IPv6 traffic, all traffic should be IPv4 only.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 3 requirement - **IP addressing schema**

Reference ID	TIPS.UC.TC.20160

Description:	The NSP used 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.
Expected result:	The NSP uses an IP address range which is "public" and agreed with the TIPS platform alternatively the NSP uses a private IP address range address (RFC1918).
Detailed test procedure:	Verify on the documentation provided by the NSP that the IP addressing schema relies on "public" addresses. Verify this address space was agreed with the TIPS Platform. Alternatively verify a private address allocation in terms of RFC1918 and again verify this address spave was agreed with the TIPS Platform.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

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

Reference ID	TIPS.UC.TC.20165

Description:	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 TIPS Actor's site and ends in TIPS Sites. All traffic must be encrypted and authenticated. Only authenticated parties are able to access the TIPS Platform. The links between the NSP and the TIPS Sites are closed to traffic from other sources or to other destinations than authenticated parties.
Expected result:	All traffic – between the TIPS Platform and the NSP and between the NSP and the TIPS actor – in encrypted and authenticated, confidentiality and integrity of data in transit across the public soil is ensured.
Detailed test procedure:	Part I: Verify that all data leaving the TIPS Platform to the NSP, and vice versa, is cryptographically protected (encrypted and authenticated). Part II: Verify that all data leaving the TIPS Actor to the NSP, and vice versa, is cryptographically protected (encrypted and authenticated). Part III: Verify that the links between the NSP and the TIPS Sites are closed to traffic from other sources or to other destinations than authenticated parties.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED

	If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Layer 3 requirement – **Static Routing**

Reference ID	TIPS.UC.TC.20175

Description:	Only static routes are used between the NSP and the TIPS Platform; no dynamic routing protocols are used.
Expected result:	No dynamic routing protocol is necessary between the NSP and the TIPS Platform, ie. only static routes are used. Between the NSP and the TIPS Platform all routing is static. The interface toward the NSP on the TIPS platform firewalls are in passive mode.
Detailed test procedure:	Check network equipment configuration and verify there is no dynamic routing protocol between the NSP and the TIPS Platform and vice versa.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.3. SECTION III - Messaging Services - test cases

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

Reference ID	TIPS.UC.TC.30010

Description:	The NSP offers the data transport services in the A2A and the U2A modes to the TIPS Actor and to the TIPS Platform.
Expected result:	The NSP offers both A2A and U2A data transport services to TIPS Platform and to all its TIPS Actors.
Detailed test procedure:	Part I: Inspect the available documentation describing the A2A mode (desk check), then use the application in A2A mode. Part II: Inspect the available documentation describing the U2A mode (desk check), then use the application in U2A mode.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

The "application to application" (A2A) mode

Reference ID	TIPS.UC.TC.30015

Description:	The NSP supports exchange of messages in A2A mode via "instant" transfer in the "push" mode only. The NSP supports exchange of files in A2A mode via "store-and-forward" transfer in the "push" mode only.
Expected result:	The NSP exchange messages in the A2A mode via the "instant" transfer and "store-and-forward" file transfer in the "push" mode only.
Detailed test procedure:	Part I: Send messages (A2A mode) via the "instant" transfer with "push" mode (no other modes are allowed, ie. push only). Part II: Send files (A2A mode) via the "store-and-forward" transfer with "push" mode (no other modes are allowed, ie. push only).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

The "user to application" (U2A) mode

TIPS.UC.TC.30220	TIPS.UC.TC.30220

Description:	The NSP supports the U2A connectivity enabling HTTPs traffic between the TIPS Actor and the TIPS Platform.
Expected result:	The NSP supports the U2A mode interactions through the web access using HTTPs protocol to the TIPS Platform.
Detailed test procedure:	Open an U2A HTTPs session from the TIPS Actor to TIPS Platform (via the NSP). The login prompt of the U2A application is presented to the TIPS actor. Verify that is not possible to establish a connection in plain HTTP.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP Interface

Reference ID	TIPS.UC.TC.30230

Description:	The NSP provides 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
Expected result:	The NSP has provided an A2A interface supporting the above mentioned operations.
Detailed test procedure:	This test is automatically passed when the following tests are passed: TIPS.UC.TC.30232/30233/30234/30235/30236/30245/30250
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP addressing model

Reference ID	TIPS.UC.TC.30231

Description:	The NSP supports 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)
Expected result:	NSP routes the messages based on the four addressing elements mentioned above.
Detailed test procedure:	Send a message from a TIPS Actor. Collect the message at the receiving interface at the TIPS platform and inspect the message itself. The four following addressing elements should be present: Sender Address, Receiver Address, business environment and the closed group of users, and Type of Message Flow.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP Interface High availability and resiliency

Reference ID	TIPS.UC.TC.30232

Description:	The NSP provides the Network Gateways (and network equipment) in high availability, to support the 24x7x365 requirement of the "instant" message exchange. The NSP supports Network Gateways in active-active configuration in the same site and also over multiple sites.
Expected result:	The Network Gateways and network devices provided by the NSP are configured in high availability, active-active mode, and can operate 24x7x365.
Detailed test procedure:	Check the architectural documentation provided by the NSP in order to verify that its solution is able to satisfy the required service level (desk check). Run some tests from a TIPS Actor: • Send continuously messages to the TIPS Platform for 24 hours and check that all messages are delivered to the receiver; • Send messages to the TIPS Platform during the week-end and check that they are always delivered to the receiver; • Check that it is possible to use all NSP's gateways.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP Interface scalability

Reference ID	TIPS.UC.TC.30233

Description:	The NSP supports horizontal scalability of the Network Gateway, to enable the addition of Network Gateways in case an additional traffic load is required. The deployment of a new Network Gateway does not impact the availability of the service in the involved infrastructure.
Expected result:	New Network Gateways can be added at runtime to the infrastructure without any impact to the service availability.
Detailed test procedure:	Send bunches of messages from a TIPS Actor to the TIPS Platform while the NSP adds a new Network Gateways. Check that there is no impact to the service availability. For example the NSP could consider to initially deliver two Network Gateways, then – while these two Network Gateways are being used – deploy two additional Network Gateways and verify this horizontal scaling does not impact the service availability.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP Load balancing

Reference ID	TIPS.UC.TC.30234

Description:	The NSP provides load-balancing features, by supporting the traffic exchange over multiple Network Gateways, with no requirement for any specific application logic to be implemented in the TIPS Platform.
Expected result:	The traffic is spread among all the available Network Gateways transparently to the TIPS Platform.
Detailed test procedure:	Send a bunch of messages from a test TIPS Actor and check that all the Network Gateways are used for the delivery to the Platform. Verify the NSP provides an effective way to check which gateway is sending each message. For example the Network Gateway ID which took care of the message is reported in the message itself.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP routing independency

Reference ID	TIPS.UC.TC.30235

Description:	The NSP provides 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 are required at the TIPS Platform.
Expected result:	The TIPS Platform is unaware of the physical location of the TIPS Actor.
Detailed test procedure:	Part I: Assuming the TIPS Actor has at least two sites, send a message to the TIPS Platform from a test TIPS Actor (site 1). Then, recover the TIPS Actor on another site (site 2) and send another message. Check that both messages are received by the TIPS Platform (please note the test is considered successful only if no configuration change is necessary). Part II: Send a message to the test TIPS Actor from a TIPS Platform (site A). Then, recover the TIPS Platform on another site (site B) and send another message. Check that both messages are received by the TIPS Actor (please note the test is considered successful only if no configuration change is necessary).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A NSP flooding control

Reference ID	TIPS.UC.TC.30236

Description:	The NSP implements an anti-flooding (throttling) mechanism to ensure that no single TIPS Actor can affect the availability of the solution at TIPS Platform or at another TIPS Actor.
Expected result:	The NSP has a throttling mechanism at both TIPS Actor and TIPS Platform interfaces.
Detailed test procedure:	Try to send from a TIPS Actors a set of messages with a rate higher than the threshold set by the NSP. The NSP should drop the messages above the predefined threshold rate. For example before starting the test set a very low threshold (ie. 5 msg/sec), then try to send messages at a higher rate, the messages above threshold should be dropped.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A message size limitations

Reference ID	TIPS.UC.TC.30237

Description:	The NSP supports the exchange of messages with 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.
Expected result:	The NSP offers A2A services in compliance with the size limitations described in the Technical Requirement document. It is possible to send messages up to 10 KB.
Detailed test procedure:	Send messages with business payload size equal and less than 10 KB. Send messages with business payload size larger than 10 KB.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A message size management

Reference ID	TIPS.UC.TC.30238

Description:	The NSP rejects as soon as possible any message that is not in the allowed size range. The NSP rejects the operation by sending back to the originator a negative acknowledgement message with the explanation of the error (e.g. "Message size out of allowed range.").
Expected result:	The NSP rejects any message that is not in the allowed size range. The originator receives a negative acknowledgement message. The NSP rejects the oversized message as close as possible to the source.
Detailed test procedure:	Generate from a TIPS Actor an oversized message and verify that the NSP rejects it and sends back to the TIPS Actor a negative acknowledgement message. The TIPS Platform does not receve the initial oversized message.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A message delivery approach

Reference ID	TIPS.UC.TC.30239

Description:	The NSP delivers messages at most once. In case of error or doubt conditions, no retry mechanism are implemented to avoid any risk of message duplication.
Expected result:	Messages are sent by the NSP to the TIPS Platform only once; no duplicates and no retry mechanism are carried out.
Detailed test procedure:	Part I: 1. Send a message from a test TIPS Actor 2. Check that the message is correctly delivered to the TIPS Platform. Part II: 1. On the MQ Server deputed to the communication between the NSP Network Gateways and the TIPS Platform, to simulate a communication error either disable the MQ PUT for the queues used for the incoming traffic or disable the MQ at channel level. 2. Send a message from a test TIPS Actor. 3. After a few minutes enable the MQ PUT on the queues and check that the message is not delivered to the TIPS Platform.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A messages independency

Reference ID	TIPS.UC.TC.30241

Description:	The NSP manages 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.
Expected result:	A2A messages can be routed through any of the available NSP network access points regardless the content of the message.
Detailed test procedure:	Send from a TIPS Actor the same business message several times and verify that each one is handled independently (for example that different gateways are used): send from a TIPS Actor several business transactions and verify that the "instant" messages belonging to the same transaction are handled by different Network Gateways, (e.g. by checking the Network Gateway ID put in the messages).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A user authentication

Reference ID	TIPS.UC.TC.30245

Description:	The NSP provides 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).
Expected result:	The devices and deployment procedures provided by the NSP to the customers (ie. TIPS Actor) are in line with the security requirement. Check that the solution provided by the NSP to the TIPS Actors complies with the above requirement.
Detailed test procedure:	Part I: The NSP's certificates are available to the TIPS actor in order to access TIPS A2A. Part II: Verify certificates' private keys are secured by means of FIPS 140-2 Level 3 HSM. Part III: Verify protocols (and key length) are in line with the security recommendation.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A closed group of user authorization

Reference ID	TIPS.UC.TC.30250

Description:	The NSP checks 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.
Expected result:	The NSP checks that the TIPS Actor belongs to the TIPS Closed Group of Users and guarantees the traffic segregation among different users.
Detailed test procedure:	1. Send a message to the TIPS Platform from an authorized TIPS Actor, and another message from another TIPS Actor not present in the CGU. First one should pass, while the second one should fail. 2. Add the second TIPS Actor to the CGU and send messages from the Platform to both the Actors. Check that each message is delivered only to the intended addressee.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ product version

Reference ID	TIPS.UC.TC.30300

Description:	The NSP connects to the TIPS sites using the IBM Message Queuing ("WMQ") transport protocol. The NSP uses a WMQ product version compliant with the WMQ version adopted by TIPS Platform.
Expected result:	The NSP adopts an WMQ product version compliant with the WMQ version adopted by the TIPS Platform. WMQ versions are either the same or compliant.
Detailed test procedure:	Check the WMQ product version on all NSP's systems. Check the WMQ version on all TIPS Platform' systems, ensure a bilateral compatibility.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ channels

Reference ID	TIPS.UC.TC.30305

Description:	The NSP supports the use of multiple channels to connect to the TIPS WMQ infrastructure.
Expected result:	Each kind of flow (1. Instant messages, 2. Files store-and-forward) has at least one WMQ channel. At least one WMQ channel is available for the above mentioned categories.
Detailed test procedure:	1. Count the number of WMQ channels available for Instant messages; 2. Count the number of WMQ channels available for files store-and- forward; 3. Verify NSP is able to manage all available WMQ channels simultaneously.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ channels TLS connection

Reference ID	TIPS.UC.TC.30310

Description:	WMQ channel connections are 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 are provided by the TIPS Operator to the NSP.
Expected result:	WMQ channels are secured with TLS certificates provided by the TIPS Operator.
Detailed test procedure:	Check that WMQ channels are secured with TLS certificates. Make sure that the TLS certificates are signed by a TIPS Operator's compliant CA.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ channels type

Reference ID	TIPS.UC.TC.30315

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

WMQ message queues

Reference ID	TIPS.UC.TC.30320

Description:	The following type of queues are 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 are set up for each specific flow in the transport protocol between the TIPS Platform and the NSP. *[Please ref. to the flows described in the "Connectivity - technical requirements".]*
Expected result:	There is a set of queues containing *SendRequest*, a set of queues containing *ReceiveIndication*, a set of queues containing *SendFile* and a set of queues containing *Notify* and *TechnicalAck*. It is possible to configure the same queue used for *ReceiveIndication* to be used for *Notify* and *TechnicalAck*. Inbond and Outbound flow use a different set of queues. Command queues are used to control Network Gateway, if needed. Set of queues are used as requested.
Detailed test procedure:	Check if the set of queues are grouped as requested. Send a message and verify if each primitive is contained in the correct queue. Send a file and verify if each primitive is contained in the correct queue.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ messages management - load balancing

Reference ID	TIPS.UC.TC.30325

Description:	The NSP manages 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 is 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 is based on a random choice (e.g. round robin mechanism) across the queues dedicated to each kind of flow.
Expected result:	Check that there is a messages load balancing mechanism across WMQ queues for both incoming and outgoing messages. Check load balancing mechanism. Repeat the test for files.
Detailed test procedure:	The TIPS platform load balancer (for example F5) performs the load balancing across WMQ instance, while the NSP gateway performs load balancing on traffic queues for incoming messages (sent by the TIPS Actors). For outgoing messages (sent by TIPS platform), the load balancing mechanism is based on a load balancing mechanism for the message producer (TIPS), this means the message consumer should be able to read messages from all the MQ/queue instances.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ message description section – CCSID

Reference ID	TIPS.UC.TC.30330

Description:	The NSP handles the WMQ message description section field CCSID based on the one used by TIPS Platform (character set name: UTF-8, CCSID: 1208).
Expected result:	WMQ message description section field CCSID 1208 is populated with a significant and meaningful value.
Detailed test procedure:	Inspect the message description section field CCSID 1208. Take note of field value.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ additional headers

Reference ID	TIPS.UC.TC.30335

Description:	The NSP supports additional WMQ standard header RFH2 and JMS.
Expected result:	NSP manages the additional header structure RFH2 and JMS in WMQ. Additional header structure RFH2 and JMS in the WMQ messages are handled as described in the "Connectivity - technical requirements".
Detailed test procedure:	Check the additional header structure RFH2 and JMS in the WMQ messages.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

WMQ message structure

Reference ID	TIPS.UC.TC.30340

Description:	The NSP manages the exchange of message based on a WMQ message. A WMQ message is composed by a "Message Description" part (MQMD) and by a "Message Text" part. The WMQ message structure which is used is described in the annex "MEPT Message Exchange Processing for TIPS".
Expected result:	The NSP manages the message / file exchange based on a WMQ message. *Message Descriptions* and *Message Text* are correctly handled system wide.
Detailed test procedure:	Inspect the WMQ message and identify the two different parts a "Message Description" (MQMD) and a "Message Text" part. Verify the WMQ message structure is in line with the annex "MEPT Message Exchange Processing for TIPS".
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A traffic primitives management

Reference ID	TIPS.UC.TC.30345

Description:	The NSP manages 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".
Expected result:	The NSP manages the primitives to exchange messages in line with the TIPS Platform.
Detailed test procedure:	Generate a set of "SendRequest" primitive requests, from a test TIPS Actor emulator to the TIPS Platform and vice versa, varying different header properties (for example: notification option, technical ack option, message type, ...). Generate a set of "FileSend" primitive requests, from the TIPS platform to a test TIPS Actor, varying different header properties (for example: notification option, FileName, ...). Verify that the related notifications and technical ACKs are correctly generated, when expected. Verify that the NSP correctly delivers the message/file to the specified part, with the correct primitive type, or that a delivery error is generated when expected. Verify that the header properties of the received messages are the expected ones, according to the MEPT specifications.
Outcome:	_____

	_____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message end-to-end information transport

Reference ID	TIPS.UC.TC.30350

Description:	The NSP allows the exchange of end-to-end information from the sender application to the receiver application together with the "instant" message (i.e. from the 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
Expected result:	The NSP is able to exchange end-to-end information from the sender application to the receiver application together with the "instant" message.
Detailed test procedure:	Generate a set of "instant" messages (i.e. "SendRequest" primitive requests), from a test TIPS Actor emulator to the TIPS Platform and vice versa. Inspect the generated messages and check the exchange of end-to-end information from the sender application to the receiver application through with the "instant" message.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Message unique identification

Reference ID	TIPS.UC.TC.30355

Description:	The NSP identifies each exchanged "instant" message with a universally unique "network" message identifier. The unique "network" message identifier of every exchanged message is provided to the receiver, together with the "instant" message, for diagnose and non-repudiation purposes. The unique "network" message identifier is also notified to the sender, if needed.
Expected result:	The unique "network" message identifier of every exchanged message is provided to the receiver, together with the "instant" message, for diagnose and non-repudiation purposes. All "instant" message has a unique "network" message identifier.
Detailed test procedure:	Generate a set of "SendRequest" primitive requests, from a test TIPS Actor emulator to the TIPS platform. Inspect the generated messages. Verify that a unique "network" message identifier is provided to the receiver, together with the "instant" message. Verify that a unique "network" message identifier is provided to the sender through Technical ACK and/or Notify primitives, whenever applicable.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Protocol description

Reference ID	TIPS.UC.TC.30360

Description:	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 manages the exchange of instant messages with TIPS in accordance with the annex "MEPT Message Exchange Processing for TIPS".
Expected result:	The NSP manages the exchange of instant messages with TIPS in accordance with the annex "MEPT Message Exchange Processing for TIPS".
Detailed test procedure:	This test is automatically passed when the following tests are passed: TIPS.UC.TC.30239, TIPS.UC.TC.30355, TIPS.UC.TC.30350 and TIPS.UC.TC.30345.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A gateway control application

Reference ID	TIPS.UC.TC.30400

Description:	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 provides to TIPS Platform a "Gateway control application" with an "easy-to-use" interface implementing the A2A traffic control functionalities. The TIPS Platform implements directly only the sending/receiving traffic exchange primitives. All the security aspects must be managed through this Gateway control application. The NSP provides 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".
Expected result:	NSP provides a description of the "easy-to-use" interface, approved by the TIPS Operator. NSP provides the "Gateway control application".
Detailed test procedure:	Check the documentation provided by the NSP describing the interface, assess the usability and eventually approve it (desk check). Through the "Gateway control application" instruct control operations toward the NSP gateway (for example start/stop the gateway, renew the LAU symmetric keys, display gateway status, etc ...), as detailed in the annex "MEPT Message Exchange Processing for TIPS", and verify that the outcome is the expected one.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Store and forward file transfer

Reference ID	TIPS.UC.TC.30405

Description:	The NSP provides a description of the solution for store-and-forward file transfer, approved by TIPS Operator. The TIPS platform interacts with NSP following the set of rules described in the annex "MEPT Message Exchange Processing for TIPS".
Expected result:	The NSP store-and-forward file transfer interacts with TIPS Platform following the ruleset described in the annex "MEPT Message Exchange Processing for TIPS".
Detailed test procedure:	TIPS Platform sends a file to the TIPS Actor emulator (using the MEPT protocol), while the TIPS Actor emulator is online. The file is correctly delivered and received by the TIPS Actor emulator. TIPS Platform sends a file to the TIPS Actor emulator, while the TIPS Actor emulator is offline. After 60 minutes the TIPS Actor emulator returns online and the file is correctly delivered, without any TIPS Platform involvement. Both files are expected to be correctly received.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

U2A user authentication

Reference ID	TIPS.UC.TC.30545

Description:	The NSP distributes to the end users the credential to access the interface of the TIPS Platform. The NSP delivers the certificates for the U2A access to the end users (with a smart-card or a USB token).
Expected result:	The end user is able to access to the TIPS Platform using smart-card or USB token provided by the NSP. The end user receives a certificate in order to access to TIPS Platform for U2A.
Detailed test procedure:	Option I – a TIPS Actor is available: Verify that the TIPS Actor cooperating in the tests has received the credential - from the NSP - in form of a smart-card / USB token and the certificates stored in such device are valid for the authentication against the TIPS U2A interface. Option II – a TIPS Actor is not available: Verify that the TIPS Operator has received valid credential - from the NSP - in form of a smart-card / USB token and the certificates stored in such device are valid for the authentication of the TIPS Actor emulator against the TIPS U2A interface.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

U2A closed group of user authorisation

Reference ID	TIPS.UC.TC.30550

Description:	The NSP checks 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.
Expected result:	The end user is able to establish a HTTPs session with the TIPS Platform only from a pre-authorized access point and by using an authorized U2A certificate.
Detailed test procedure:	1. Check that the end user connection to the TIPS Platform can be established via HTTPs from a valid IP agreed with the NSP and by using an authentication token whose certificate belongs to the TIPS U2A CGU; the connection should be successful. 2. Try to access the TIPS GUI from another IP not authorized by the NSP; the connection should fail. 3. Try to open an HTTPs tunnel from a valid IP, but with a certificate not belonging to the CGU; the connection should fail.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

TIPS Actor Emulator Access Point

Reference ID	TIPS.UC.TC.30655

Description:	The NSP provides to the TIPS Platform only a "TIPS Actor Emulator access point" to perform testing/monitoring (continuous and/or specific afterany 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 includes: • a connectivity infrastructure at one of the TIPS sites. The connectivity infrastructure is of the same type as the one provided to the TIPS Actor; • a minimal set of software components to manage simple message exchange, i.e. to trigger message sending and to support message receiving, emulating the basic configuration of a TIPS Actor. The TIPS Operator is able to use the TIPS Actor Emulator software without the need of any prior notice to the NSP.
Expected result:	The TIPS Operator is able to use the TIPS Actor Emulator software without the need of any prior notice to the NSP.
Detailed test procedure:	Verify that through the TIPS Actor Emulator software is possible to manage simple message exchanges between the TIPS platform and the emulated TIPS actors.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.4. SECTION IV - Security Services - test cases

Technology and organisational processes

Reference ID	TIPS.UC.TC.41010

Description:	The NSP offers 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 is compliant with the ISO27001:2013 standard.
Expected result:	NSP is compliant with the ISO27001:2013 standard and is able to formally demonstrate this compliancy toward the TIPS Operator.
Detailed test procedure:	Verify the NSP's conformity to the ISO27001:2013 standard. Acknowledge any assessment already achieved by the NSP in this area. Assess deviations of the implementation from the above mentioned standard. Produce a deviation analysis document and expect deviations (if any) trigger an action list. Measures recorded on this list have to be addressed before the user tests.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Security Platform as a service

Reference ID	TIPS.UC.TC.41020

Description:	The NSP delivers 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 ensures to be compliant with the TIPS security requirements.
Expected result:	The NSP delivers a technical infrastructure and software components - to both the TIPS Actor and to the TIPS Platform - allowing the security management and the compliancy to the security requirements listed in the present document.
Detailed test procedure:	The compliancy to the TIPS security requirements is achieved passing TIPS.UC.TC.11110, but additional security requirements are described in the "Connectivity - technical requirements". TIPS.UC.TC.41020 is passed when all of the tests listed below are passed: TIPS.UC.TC.41010 - Technology and organisational processes TIPS.UC.TC.41020 - Security Platform as a service TIPS.UC.TC.41030 - Operational readiness TIPS.UC.TC.42040 - Encryption of all incoming and outgoing traffic TIPS.UC.TC.42050 - Segregation of data TIPS.UC.TC.43060 - Digest algorithms TIPS.UC.TC.43070 - Integrity of traffic TIPS.UC.TC.43090 - Integrity of software components TIPS.UC.TC.43100 - Integrity of audit logs TIPS.UC.TC.46240 - Audit log TIPS.UC.TC.46250 - Audit logging TIPS.UC.TC.47260 - Monitoring facilities TIPS.UC.TC.47270 - Automated alerts TIPS.UC.TC.47280 - Change management TIPS.UC.TC.47290 - Network encryption failure TIPS.UC.TC.48300 - Encryption algorithms TIPS.UC.TC.48310 - Encryption devices

	TIPS.UC.TC.48320 - Management of NSP encryption devices TIPS.UC.TC.44120 - Unique identification of users TIPS.UC.TC.485100 - A2A Identification TIPS.UC.TC.485110 – A2A Local Authentication TIPS.UC.TC.485120 - A2A Network Authentication TIPS.UC.TC.485125 - A2A Non Repudiation support TIPS.UC.TC.45210 - Logically segregated groups of users TIPS.UC.TC.45220 - Segregation of traffic TIPS.UC.TC.45230 - Physical and logical access control of the NSP's infrastructure TIPS.UC.TC.48330 - Public Key Infrastructure TIPS.UC.TC.48340 - Certification Authority TIPS.UC.TC.48350 - Certificate Policy TIPS.UC.TC.48360 - Certificate Practices Statement TIPS.UC.TC.48370 - Hardware Security Modules TIPS.UC.TC.48371 - Smart Cards or USB token TIPS.UC.TC.48380 - Public Key Certificates TIPS.UC.TC.48390 - Certificate Extensions TIPS.UC.TC.48395 - Certificate revocation list TIPS.UC.TC.48396 - Digital Signature management TIPS.UC.TC.48398 - Responsibilities for management of cryptographic keys TIPS.UC.TC.48410 - Administration of symmetric and asymmetric cryptographic keys TIPS.UC.TC.48420 - Certificate independence TIPS.UC.TC.49430 - Security framework (adopted or proposed)
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Operational readiness

Reference ID	TIPS.UC.TC.41030

Description:	The NSP guarantees the operational readiness of all relevant security devices and components of its security platform according to the relevant service levels.
Expected result:	The NSP guarantees the operational readiness of all relevant security devices and components of its security platform according to the relevant service levels (ie. A2A message delivery time (§ TIPS.UC.TC.55010), A2A Service availability (§ TIPS.UC.TC.55020) and Fault clearance (§ TIPS.UC.TC.55030). Security devices and components are operationally ready.
Detailed test procedure:	List security devices and components, both HW and SW, e.g. network encryption device, signing software, PKI services, etc. Verify the operational readiness of each.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Encryption of all incoming and outgoing traffic

Reference ID	TIPS.UC.TC.42040

Description:	The NSP ensures confidentiality of all TIPS traffic over its Network. The NSP ensures 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.
Expected result:	All traffic is encrypted. NSP staff and other parties are not allowed to access or copy data except when the operation is subject to access controls, secure logging and reporting to TIPS Operator. All traffic is encrypted and the NSP ensures that its staff and other parties cannot access or copy unencrypted data exchanged over its network except in the way described in the requirements.
Detailed test procedure:	Jointly analyse end-to-end (from the TIPS Actor to the NSP, within the NSP Network, from the NSP to the TIPS Platform) if network all segments transport encrypted data. This analysis can be done inspecting existing documentation. If one (or more) network segments transport unencrypted data, then assess if it is possible for the NSP's staff (or third) parties to access the unencrypted data. Flag gaps (if any) and identify corrective measures to be addressed before the user tests.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Segregation of data

Reference ID	TIPS.UC.TC.42050

Description:	The NSP ensures that the TIPS Actor can only access its own incoming and outgoing traffic. No other parties (including the NSP and its subcontractors) are 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.
Expected result:	The NSP ensures TIPS Actor can access only their own incoming and outgoing traffic.
Detailed test procedure:	1. a TIPS Actor can access in A2A his own relevant data; 2. a TIPS Actor can access in U2A his own relevant data; 3. a TIPS Actor can not access in A2A data relevant to other TIPS Actors; 4. a TIPS Actor can not access in U2A data relevant to other TIPS Actors; 5. a TIPS Actor can get information about its traffic from the NSP (e.g. timestamps, message length, signature, etc.) [ie. not mandatory]; 6. check the procedure to be used by the NSP to access the data of a participant under the authorization of the TIPS Operator (if applicable, ie. the NSP could also not access at all to the TIPS Actor data) [desk check].
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Digest algorithms

Reference ID	TIPS.UC.TC.43060

Description:	The TIPS Actor uses only strong and not deprecated digest (hash) algorithms for its Solution. SHA-256 is the minimum required algorithm for the digest computation.
Expected result:	The TIPS Actor uses only strong and not deprecated digest (hash) algorithms. The TIPS Actor uses SHA-256 or more secure algorithms to generate digests.
Detailed test procedure:	The NSP has delivered to both the TIPS Actor and the TIPS Platform hardware and software. List which digest (hash) algorithms are used and where.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Integrity of traffic

Reference ID	TIPS.UC.TC.43070

Description:	The NSP does not interfere with the integrity of any traffic exchanged between its TIPS Actor and the TIPS Platform.
Expected result:	The NSP ensures the integrity of all traffic from the TIPS Actor to the TIPS Platform and back.
Detailed test procedure:	Verify that the NSP performs an integrity check on each message leaving its network. An hash must be calculated at both the sending and receiving side.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Integrity of software components

Reference ID	TIPS.UC.TC.43090

Description:	The NSP ensures the integrity of its software components providing Connectivity Services and security features for TIPS. The NSP automatically detects every planned and unplanned (intentional and accidental) modification and alert the TIPS Operator without undue delay. The NSP ensures the protection against malicious codes.
Expected result:	Software integrity can be proven for all components provided by the NSP's; all SW components are signed either by the NSP itself or by a NSP's vendor. The NSP assures software components integrity for the products delivered by the NSP itself (for example the NSP digitally signs his own software components and ensures that an external vendor has digitally signed the other software purchased by the NSP). The NSP manages digital keys used for signing. The NSP detects signature failures and promptly send alerts to the TIPS Platform. The NSP performs a malicious code detection on its systems.
Detailed test procedure:	Part I: List all SW used end-to-end (i.e. signing, encryption, key management) for both A2A and U2A solution. Verify if all SW is signed and by whom; please also verify the validity of the signature. Identify unsigned software. Part II: Obtain the NSP's malicious code prevention policies. Verify if and how these policies are implemented.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Integrity of audit logs

Reference ID	TIPS.UC.TC.43100

Description:	The NSP ensures and controls the integrity of all TIPS related audit logs.
Expected result:	The NSP ensures and controls the integrity of TIPS audit logs related to all equipments under his own management domain and responsibility. Audit logs integrity is ensured. NSP is able to determine when integrity is compromised.
Detailed test procedure:	List all NSP devices, list all audit logs produced by these devices, assess the procedures in place to identify if they have been manipulated (for example prove the compliancy with the ISO control 12.4.2 "Protection of log information" and give evidence of the anti-tampering measures in place). Verify integrity can be ensured for all audit logs, and if not, identify the gap, describe the corrective action and apply these action according to a plan agreed with the TIPS Operator. Please note this test is on field, ie. it is not a desk check.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Audit log

Reference ID	TIPS.UC.TC.46240

Description:	All network devices provided by the NSP uses a logging functionality. The NSP agreed 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 provides 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.
Expected result:	All provided NSP's network devices have a logging functionality enabled and these logs are either retained by the NSP or the TIPS Operator or both. TIPS Operator received from NSP the security policy applied to the audit logs. There is a procedure specifying what to log where, and these logs are actually available where they should be. NSP issues the logging security policy and provide it to TIPS Operator.
Detailed test procedure:	Part I Verify the logging security policy provided by the NSP. Also verify that an organisational procedure specifies which logs have to be available where. Part II Check that all network devices are logging according to the policy. Part III Identify which external logging servers are configured and verify they are actually receiving the expected logs.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____

Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Audit logging

Reference ID	TIPS.UC.TC.46250

Description:	The NSP logs each data session established between the TIPS Actor and the TIPS Platform.The NSP securely logs all network component changes, access attempts and security attacks/breaches on the network components.
Expected result:	NSP logs each data session established between its TIPS Actor and the TIPS Platform (for both A2A and U2A sessions). NSP securely logs all network component changes, access attempts and security attacks/breaches on the network components. Session audit logging is available and so is network components audit logging for the above mentioned significant events.
Detailed test procedure:	For each of the following events check if it is logged, then document how and where: 1. start a new session; 2. change a network component configuration on the NSP device; 3. successfully access a NSP network component; 4. fail the login to a NSP network component; 5. simulate an attack (if possible) on a NSP network component. Check logs are not only collected but also securely preserved (for example verifying the NSP' Security Logging policy).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Monitoring facilities

Reference ID	TIPS.UC.TC.47260

Description:	The NSP delivers 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 delivers features to monitor the configuration of the security providing components. The NSP implements mechanisms to monitor its infrastructure for security vulnerabilities, breaches and attacks and ensures quick updates of all devices whenever security patches are available. The NSP reports immediately any issues to the TIPS Operator using collaboration tools (such as e-mail, instant messages, smartphones).
Expected result:	TIPS Platform is monitoring the Connectivity Services. A reporting channel is in place. All the events mentioned in the requirement above are visible on the monitoring facility where specific alarms are triggered.
Detailed test procedure:	The technical operations monitoring facility records and shows recent events. 1. Simulate a WAN failure and check the relevant indication on the monitoring facility. Restore to normal operation. 2. Simulate a VPN failure and check the relevant indication on the monitoring facility. Restore to normal operation. 3. Simulate a Network Gateway failure and check the relevant indication on the monitoring facility. Restore to normal operation. 4. Describe how the NSP monitors its infrastructure for security vulnerabilities, breaches and attacks; 5. Describe how the NSP ensures quick updates of all devices (ie. inspect the NSP Vulnerability and Patch Management Policy or equivalent); 6. Describe how the NSP report any issues to the TIPS Operator and how.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Automated alerts

Reference ID	TIPS.UC.TC.47270

Description:	The NSP installs alerts which are automatically triggered in case of relevant events. The alerts are 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).
Expected result:	Assuming the "relevant events" are either a device failure or breach (or attempted breach), the NSP triggers automated alerts in case of a relevant event. These NSP alerts are sent to the TIPS Operator using SNMP. SNMP traps are sent from the NSP to the TIPS Operator in case of the following events takes place: device failure, attempted breach (or breach). This applies to all NSP's devices in the TIPS Platform sites, ie. all devices supplied by the NSP (for example routers, IPSec VPN, Network Gateways, …).
Detailed test procedure:	Power off (or shutdown) a device, verify a SNMP trap is sent from NSP to the TIPS Operator. Attempt to breach a device (for example multiple failure of login attempts), verify a SNMP trap is sent from the NSP to the TIPS Operator.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Change management

Reference ID	TIPS.UC.TC.47280

Description:	The NSP applies a strict change management procedure to its network components that provide security features to TIPS Platform.
Expected result:	The NSP applies a strict change management procedure to its network components that provide security features for the TIPS Platform. Change management process is described in the Operation Manual.
Detailed test procedure:	NSP has a change management document describing the workflow to be followed upon a change.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Network encryption failure

Reference ID	TIPS.UC.TC.47290

Description:	The NSP designs and implements procedures to identify Network encryption failures which might not be identified by TIPS. The NSP designs and implement procedures to resume the encryption functionality in such circumstances. The NSP notifies these procedures to the TIPS Operator and any subsequent change thereto, upon implementation.
Expected result:	The NSP has procedures to handle network encryption failures (ie. circumstances where traffic that should be encrypted actually is not). The NSP has procedures to resume the encryption functionality (to recover the circumstance described before, ie. encrypt all traffic that should be encrypted). The TIPS Operator agrees with the NSP on specific procedures under which unencrypted traffic is first detected, then restored back on an encrypted channel.
Detailed test procedure:	Check NSP's procedure to detect whether a channel that should be encrypted is not encrypted any more (for whatever reason) and verify the operational procedure to resume the normal encryption.For example under normal condition the traffic from the TIPS Actor to the TIPS Platform is encrypted in the IPSec VPN tunnel, then during the test the configuration on the Network Gateway is changed so to remove the traffic encapsulation configuration, then the receiver (either the TIPS Actor or the TIPS Platform) should not receive any traffic at all.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Encryption algorithms

Reference ID	TIPS.UC.TC.48300

Description:	The NSP implements the AES encryption algorithm with a minimum length of 128 bit for symmetric encryption keys and 2048 bit for asymmetric encryption keys.
Expected result:	The NSP uses AES key length in line with the minimum length foreseen. All equipment / systems using the AES encryption algorithms have the expected minimum key length (ie. 128 bit for symmetric keys and 2048 bit for asymmetric keys).
Detailed test procedure:	List equipment / systems using encryption algorithms; populate the list with the information of which encryption algorithms are used and corresponding key lengths.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Encryption devices

Reference ID	TIPS.UC.TC.48310

Description:	The NSP installs encryption devices in all TIPS Sites. The NSP installs encryption devices in all TIPS Actor's sites which are interconnected with the TIPS Platform. The encryption devices comply with the security specifications stated in the "Connectivity - technical requirements".
Expected result:	The NSP installs encryption devices in all TIPS Sites and TIPS Actor sites. The encryption devices comply with security specifications stated in the "Connectivity - technical requirements".
Detailed test procedure:	Check all TIPS Sites have encryption devices. Check all TIPS Actors' sites have encryption devices; for example the TIPS Actor (if any) could share with the TIPS Platform the installation reports of the NSP's devices at their sites (desk check). Check the encryption devices specifications and verify these are in line with the "Connectivity - technical requirements".
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Management of NSP encryption devices

Reference ID	TIPS.UC.TC.48320

Description:	The NSP manages all encryption devices relevant to the TIPS Actor under its own responsibility. In case of failure or disaster, the NSP has the possibility to manage these devices in a highly secure remote way. The NSP enables secure and resilient management of all encryption devices from all the TIPS Sites. The management of these devices is possible from a secondary site in case of component failure or disaster at the main site.
Expected result:	The NSP manages all encryption devices under its own responsibility. Even in case of failure or disaster, the NSP has the possibility to manage their devices remotely and in a highly secured way. Encryption devices are under the NSP's responsibility and the NSP has a way to manage them both under normal operations and during the event of a site failure / disaster.
Detailed test procedure:	Verify that the Operation Manual clearly states that the NSP is responsible for their devices. Collect information on the standard way the NSP manages devices. Gather information on the way the NSP manages their devices during a failure and during a disaster. Assess this main site failure scenario, identify possible improvement and record the agreed measures which shall be addressed before user tests.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Unique identification of users

Reference ID	TIPS.UC.TC.44120

Description:	The NSP identifies the TIPS Actor and the TIPS Platform in a unique way. The NSP guarantees the identification via digital certificates.
Expected result:	NSP uniquely identifies both the TIPS Actor and the TIPS Platform using digital certificates.
Detailed test procedure:	Verify NSP uniquely identifies TIPS Actor emulator via digital certificates. Verify NSP uniquely identifies TIPS Platform via digital certificates.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Identification

Reference ID	TIPS.UC.TC.485100

Description:	The NSP identifies 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 includes this information in the network envelope provided to the receiver together with the message.
Expected result:	Every time a new session is opened the NSP identifies both the TIPS Actor and the TIPS Platform (through the A2A NSP's Network Gateway). The identity of the sender is transfered to the receiver by the NSP and this information is included in the network envelope provided to the receiver together with the message.
Detailed test procedure:	Open several A2A sessions, each one with a different authentication certificate, from a TIPS Actor for sending messages. Verify that the NSP performs every time the authentication process and that the identity of the sender is always passed by the NSP to the receiver.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Local Authentication

Reference ID	TIPS.UC.TC.485110

Description:	The NSP authenticates 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 uses an appropriate mechanism for this purpose. An example of an "appropriate measure" is the use of HMAC algorithm. If the HMAC algorithm is used, the symmetric key should be periodically renewed.
Expected result:	Every time a new session is opened the NSP authenticates both the TIPS Actor and the TIPS Platform (through the A2A NSP's Network Gateway). The NSP has set up an appropriate measure, for example HMAC based (with a periodical keys renewal).NSP successfully completes the message partners authentication, for example using a Local AUthentication key (LAU).
Detailed test procedure:	Part I: A new session is opened from a TIPS Actor with no LAU or a wrong LAU and verify the NSP's Network Gateway rejects the session. Part II: A new session is opened from a TIPS Actor with the correct LAU and verify the NSP's Network Gateway accepts the session. Part III: When a message is exchanged, the NSP is in charge of verifying the integrity of the message checking the HMAC(s) field(s). Depending on the direction of the flow, HMAC(s) are either generated from the NSP itself or from the TIPS Actor or from the TIPS Platform. During the tests the teams will first inspect the message header and verify the HMAC(s) field(s) is(are) there; then the originator of the message will manipulate either the message or the HMAC(s) field(s) to ensure the NSP is rejecting the manipulated content.
Outcome:	_____ _____ _____

Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Network Authentication

Reference ID	TIPS.UC.TC.485120

Description:	The NSP authenticates 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 bases this mechanism on the availability of digital keys stored in a Secure Store accessible by the NSP's Network Gateways for this purpose. The NSP always checks 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 purpose are used for digital signature.
Expected result:	Every time a new session is opened the NSP authorizes both the TIPS Actor and the TIPS Platform (through the A2A NSP's Network Gateway) using digital keys stored in a Secure Store. The validity of digital certificate is periodically checked. The same keys are used for both authentication and digital signature. NSP successfully completes the message partners authorization, digital certificates are checked, same keys are used for authentication and digital signatures.
Detailed test procedure:	The possibility to open a new session on the NSP's Network Gateway mandates the presence of a valid digital certificate. Part I: A new session is opened from a TIPS Actor with no certificate or invalid certificate (ie. suspended certificate or expired certificate) and verify the NSP's Network Gateway rejects the session. Part II: A new session is opened from a TIPS Actor with a valid certificate and verify the NSP's Network Gateway accepts the session.
Outcome:	_____ _____ _____
Result:	Please describe the test result:

	[] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

A2A Non Repudiation support

Reference ID	TIPS.UC.TC.485125

Description:	The NSP manages 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 signs 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 includes the (digest of the) message payload provided by the sending application. The signature data is 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 stores all signature related information, as well as all signed data, for non-repudiation purposes. The NSP provides 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 provides 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 is able to retrieve the certificate and the certificate status at the time of the signature. The non-repudiation service is available up to three months after the traffic exchange took place.
Expected result:	The non repudiation mechanism is in place (signing is in line with the flow described above). [*Please notice it is not practical to test that "The non-repudiation service is available up to three months after the traffic exchange took place."*]
Detailed test procedure:	Send a message from a TIPS Actor and check that the business payload is signed by the Network Gateway on the sender. The signature includes the (digest of) message

	payload and is delivered to the receiver together with the "instant" message. Verify that the Network Gateway of the receiver: 1. checks the validity of the signing certificate (for example include its ID in the CRL and verify that the Gateways rejects the message) 2. verifies the signature. A non-repudiation support service is made available by the NSP.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Logically segregated groups of users

Reference ID	TIPS.UC.TC.45210

Description:	The NSP allows the creation and the removal of logically segregated groups of TIPS Actors or end users. The NSP creates and manages 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, is arranged through an electronic workflow on the Internet. All the electronic forms are authorised by the relevant National Central Bank. The activation date for the subscriptions is set at latest within two weeks after the form's approval by the TIPS Operator; the new subscription is scheduled and activated ensuring the availability of the service (e.g. adopting the "rolling update" approach). Upon request from the TIPS Operator, the NSP withdraws from the CGU a TIPS Actor or an end user within one hour.
Expected result:	The NSP allows creation and removal of logically segregated groups of users, manages all the user groups, and is able to segregate production environment from the test & training environment. The NSP shall demonstrate its ability to remove a user within an hour. In addition user and group creation are in line with the process described in the "Connectivity - technical requirements".
Detailed test procedure:	Subscribe some TIPS Actors to a test CGU already created by the NSP. Check any new Actor is able to operate. Request to remove a TIPS Actor assigned to the CGU. Check the removed Actor is not able to operate anymore. While performing these actions verify the Internet electronic workflow for Actors creation/deletion.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Segregation of traffic

Reference ID	TIPS.UC.TC.45220

Description:	The NSP ensures segregation of data traffic between different groups of user. 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 are not able to send or receive messages from the production environment.
Expected result:	The NSP ensures segregation of data traffic between different groups of users. The NSP ensures segregation of environments (production and test & training). Users belonging to different user groups can not exchange messages / files with each other. Environments (production and test & training) are segregated; ie. messages / files can not be swapped between two environments.
Detailed test procedure:	Send a message to a user belonging to a different user group. Repeat test for a file. Both attempts are expected to fail. Using a test & training user account, send messages to the production environment. Repeat test for a file. Both attempts are expected to fail. Using a production user account, send messages to the test & training environment. Repeat test for a file. Both attempts are expected to fail.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Physical and logical access control of the NSP's infrastructure

Reference ID	TIPS.UC.TC.45230

Description:	The NSP protects any essential network components used for its Solution with physical and logical access controls. In particular, the NSP protects access to its administration interfaces. The NSP adopts a "need to work" principle to allow access to its infrastructure components.
Expected result:	NSP protects his own network components through physical and logical access controls. The NSP protects access to network components (such as encryption devices, NSP gateways, other network devices) administration interfaces. The NSP describes – through operational procedures – how the "need to work" principle is implemented.
Detailed test procedure:	Assess the security posture of the NSP's network components, list and evaluate physical and logical access controls, inspect network diagrams and network components configurations. Repeat the same process for administration interfaces.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Public Key Infrastructure

Reference ID	TIPS.UC.TC.48330

Description:	The NSP delivers a Public Key be Infrastructure ("PKI") compliant with X.509 version 3 standard for the digital certificates. The provided infrastructure provides the following components:: • Certification Authority, • Hardware Security Modules.
Expected result:	NSP's PKI Infrastructure provides the following components: 1. Certificate Authority 2. Hardware Security Modules All components are compliant with X.509 V3 standard.
Detailed test procedure:	Check that the NSP has in place: 1. Certificate Authority 2. Hardware Security Modules Check both components and certificates signed by the NSP's Public Key Infrastructure (PKI) are X.509 ver.3 compliant.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certification Authority

Reference ID	TIPS.UC.TC.48340

Description:	The NSP delivers Certification Authority (CA) functions to the TIPS Actor and the TIPS Platform. The provided functions supports the generation, management, storage, deployment and revocation of public key certificates. The NSP ensures these functions work within the context of the Certificate Policy (CP) and function operationally in accordance with the Certificate Practices Statement (CPS).
Expected result:	The NSP delivers Certification Authority (CA) functions to TIPS Actor and the TIPS Platform, i.e. generation, management, storage, deployment, and revocation of public key certificates. The CA functions are compliant with the CP and function operationally in accordance with the CPS. The NSP provides CA functions to TIPS Operator and TIPS Actor, and ensures the above mentioned functions within the CP and CPS context.
Detailed test procedure:	A TIPS Actor generates a certificate using the NSP's CA. TheTIPS Actor is able to manage the certificate life cycle (store, deploy and eventually revoke certificates). TIPS Operator performs the same tests. Compare the life cycle with CP and CPS. In case no TIPS Actor is available during the testing phase, then please run the test only with the TIPS Operator and using the TIPS Actor emulator.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certificate Policy

Reference ID	TIPS.UC.TC.48350

Description:	The NSP delivers to the TIPS Operator the Certification Policy for the CA functions it performs. A certificate policy focuses on certificates and the NSP (CA) responsibilities regarding these certificates. It defines certificate characteristics such as usage, enrolment, issuance and revocation procedures, as well as liability issues.
Expected result:	The NSP delivers to the TIPS Platform the CP for the CA functions it performs. The CP addresses certificate responsabilities and characteristics. The certificate policy focuses on certificates and the NSP (CA) responsibilities regarding these certificates. It defines certificate characteristics such as usage, enrolment, issuance and revocation procedures, as well as liability issues.
Detailed test procedure:	Jointly analyse the NSP CP, in the analysis give a focus on NSP responsibilities and certificates usage, enrolment, issuance, revocation, and liability (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certificate Practices Statement

Reference ID	TIPS.UC.TC.48360

Description:	The NSP delivers to the TIPS Operator the Certificate Practices Statement for the CA functions it performs. The Certificate Practice Statement concentrates on the operational procedures related to the certification authority functions.
Expected result:	The NSP delivers to the TIPS Operator the CPS; the CPS contains the operational procedures for the CA functions NSP performs.
Detailed test procedure:	List the CA functions the NSP performs. Jointly inspect the CPS. Make sure all listed functions are covered within operational procedures.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Hardware Security Modules

Reference ID	TIPS.UC.TC.48370

Description:	The NSP provides tamper-proof HSM for storing all digital keys used for A2A. The HSM(s) are compliant at minimum with FIPS 140-2 Level 3 or Common Criteria EAL 4+ and they will be installed in the TIPS Sites.
Expected result:	The NSP have installed FIPS 140-2 Level 3 or Common Criteria EAL 4+ compliant tamper-proof Hardware Security Modules (HSM) in the TIPS Sites. HSM(s) contains digital keys used for A2A.
Detailed test procedure:	1. Check if the HSM(s) are installed in the TIPS Sites. 2. Check if the HSM(s) are FIPS 140-2 L3 compliant or Common Criteria EAL 4+; please note this part of the test is a desk check. 3. Check if all A2A keys used in the Network are stored in the HSM(s); the HSM containes a key pair for every certificate, during the test please list the available certificates.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Smart Cards or USB token

Reference ID	TIPS.UC.TC.48371

Description:	The smart cards or USB token, provided by the NSP, are compliant at least with FIPS 140 for the security level 3 or Common Criteria EAL4+. The smart card readers, provided by the NSP, are compliant 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.
Expected result:	The smart card /USB token provided by the NSP comply with FIPS 140 - L3 or Common Criteria EAL4+. The specifications of the smart card readers are verified and checked.
Detailed test procedure:	Check if smart card/USB token are compliant either with FIPS 140 - L3 or Common Criteria EAL4+. Verify the minimum requirements of the smart card readers : - 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.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Public Key Certificates

Reference ID	TIPS.UC.TC.48380

Description:	The NSP delivers to the TIPS Operator a description of the format for the public key certificates it is going to use. The certificates format is based on the X.509 standard and includes detail semantic profile of its public key certificates.
Expected result:	The NSP describes the X.509 based certificate's format. Certificates' format includes detailed semantic profile of its public key certificates.
Detailed test procedure:	Examine the certificates and check the details of the format and the semantic profile (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certificate Extensions

Reference ID	TIPS.UC.TC.48390

Description:	The NSP delivers 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.
Expected result:	Certificate extensions in use are documented. The Non-Repudiation bit of digital signature certificates are set in the "Key usage" extension.
Detailed test procedure:	Examine certificates to check and list which extensions NSP uses. Verify NSP documented all extensions listed. Verify Non-Repudiation bit is set in the "Key usage" extension of the digital signaturte certificates.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certificate revocation list

Reference ID	TIPS.UC.TC.48395

Description:	The NSP provides to the TIPS Operator a CRL in the HTTP, LDAP or OCSP formats. The TIPS Platform selects with the NSP the most appropriate protocol for the intended performance.
Expected result:	It is possible to read the CRL using any of the following protocols: HTTP, LDAP and OCSP. The TIPS Operator will choose the protocol it deems most appropriate from a performance point of view.
Detailed test procedure:	1. Query the NSP's CRL using HTTP (if applicable); 2. Query the NSP's CRL using LDAP (if applicable); 3. Query the NSP's CRL using OCSP (if applicable).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Digital Signature management

Reference ID	TIPS.UC.TC.48396

Description:	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 is 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.
Expected result:	The digital signature is created with the certificate provided to the sender by the NSP and the receiver of the message is able to check the validity of this signature.
Detailed test procedure:	Part I: The sender (TIPS Platform) digitally signs a message; the receiver (TIPS Actor) of the message is able to check the validity of the signature. Part II: Run the test with a TIPS Actor as sender and the TIPS Platform as a receiver; again check the receiver of the message is able to check the validity of the signature (please notice the control of the signature validity is performed by the NSP on behalf of the TIPS Platform).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Responsibilities for management of cryptographic keys

Reference ID	TIPS.UC.TC.48398

Description:	The management of cryptographic keys dedicated to the TIPS Platform remains under the sole responsibility of the TIPS Operator, which is 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.
Expected result:	The management of cryptographic keys is under the sole responsibility of the TIPS Operator, which is the only entity having operational and physical access to key storage devices (HSM) delivered by the NSP. Logical access is permitted to the NSP only for administrative and operational purposes, while physical access to the HSM is permitted to the NSP only to perform hardware replacement.
Detailed test procedure:	Verify that the TIPS Operator is able to manage crypto keys in the HSM; then verify whether the NSP is able to logically access the HSM (for example in order to perform a SW upgrade of the device), but is not authorized manage the key material in the HSM.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Administration of symmetric and asymmetric cryptographic keys

Reference ID	TIPS.UC.TC.48410

Description:	The NSP ensures the following administration functions for symmetric and asymmetric cryptographic keys. • *Generation*: The NSP ensures secure generation of keys/key pairs. • *Distribution*: The NSP ensures secure electronic distribution of keys/public keys, i.e. encrypted. • *Renewal*: The NSP ensures the renewal of the keys. However only the TIPS Operator defines the frequency of exchange and the minimum length of keys used. The NSP ensures that the keys renewal does not interfere with its services. • *Storage*: The NSP ensures that keys/private keys are stored securely. • *Revocation*: The NSP ensures immediate revocation of the key/public key certificate if it is considered compromised.
Expected result:	The NSP ensures the following administration functions for symmetric and asymmetric cryptographic keys: 1. Secure generation of the keys, 2. Secure distribution of the keys, 3. Renewal of the keys accordingly with the TIPS operator defined interval exchange and minimum key legth, 4. Secure storage of the keys, and 5. Immediate revocation of compromised keys.
Detailed test procedure:	Verify together with the NSP the procedure used to generate, distribute, renew, store and revoke symmetric/asymmetric cryptographic keys (desk check). Generate and distribute the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Renew the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Store the symmetric crypto keys, then repeat the test for the asymmetric crypto keys. Revoke the asymmetric crypto keys, then try to use it and verify it fails.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____

	_____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Certificate independence

Reference ID	TIPS.UC.TC.48420

Description:	The certificates issued by the PKI are distributed and used without any constraint or reference about the physical location which hosts the TIPS production environment.
Expected result:	Independently of where the TIPS services are running (either site A or site B), the TIPS Actor can successfully connect to the TIPS Platform; ie. all certificates are signed by the same CA.
Detailed test procedure:	Part I: Isolate site B (disabling the Ethernet interfaces on the 4CBNet switch), have the TIPS Actor to send successfully messages to the Network Gateways in site A. Restore site B and isolate site A, have the TIPS Actor to send successfully messages to the Network Gateways in site B. No changes of certificate on the TIPS Actor are expected. Part II: Isolate TIPS Actor site 2 (disabling the Ethernet interfaces on the 4CBNet switch), have the TIPS Platform to send successfully messages to the Network Gateways in site 1. Restore site 2 and isolate site 1, have the TIPS Platform to send successfully messages to the Network Gateways in site 2. No changes of certificate on the TIPS Platform are expected.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Security framework (adopted or proposed)

Reference ID	TIPS.UC.TC.49430

Description:	The NSP provides to 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 has the right to request or execute any security assessment on the security of the NSP services, and NSP commits to apply the recommendations issued by the Eurosystem. The action plan is 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.
Expected result:	The NSP provides the security framework adopted for the security assessment, security strategy, deployment, management, and audit (the framework can also be the NSP Security Programme, if available). The NSP's security framework addresses all the required topics (security assessment, security strategy, deployment, management, audit). The NSP is committed to perform security assessment on TIPS Operator request, and apply security recommendations issued by the TIPS Operator. Check on the available documention that the TIPS Operator can request or execute any security assessment and receive a commitment to apply the recommendations issued.
Detailed test procedure:	Ask to the NSP the security framework adopted and examine it (if the NSP has available a Security Programme, then use it). Check the compliancy is foreseen in the available documentation. Verify that the TIPS Operator has the right to request a security assessment. Verify that the NSP and the TIPS Operator have to agree on an action plan. Check that when the NSP's receives an action plan is then mandated to implement the recommendations issued.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED

	[] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.5. SECTION V - Operational Services - test cases

Connectivity service catalogue

Reference ID	TIPS.UC.TC.51010

Description:	The NSP has developed 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 least, includes a description of detailed services and service levels (such as detailing performance, availability, support commitments). The content of the Connectivity Services catalogue includes 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.
Expected result:	The NSP has a Connectivity Service catalogue with all the expected contents as described in the "Connectivity - technical requirements". Connectivity Service catalogue includes contents described in the detailed test procedure.
Detailed test procedure:	Jointly read the Connectivity Service catalogue, verify that it includes a description of detailed services and service levels. The Connectivity Service catalogue contains: detailed services, service levels, volume related services, dedicated connectivity solutions, backup/alternative network access solutions, procedures to assure the Business Continuity, and information about services configuration and operation.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED

	[] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Operation and Escalation manual

Reference ID	TIPS.UC.TC.51020

Description:	The NSP provides 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 include the detailed technical information needed to install necessary software and hardware infrastructure and make use of the provided services. The NSP is 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.
Expected result:	The NSP provides and maintains the Operations Manual, the Escalation Manual, and the User Guides. Above mentioned documents exist and responsibilities are clearly assigned (ie. the NSP is the owner of the manuals and is responsible for updates). To ensure the accuracy of the manuals the TIPS Operator may submit its observations to NSP and the NSP has to take them on board.
Detailed test procedure:	Jointly read the following documentation, written by the NSP, and check if it is in line with "Connectivity - technical requirements": 1. the Operations Manual 2. the Escalation Manual 3. the User Guides.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action:

	_____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

NSP Support Teams

Reference ID	TIPS.UC.TC.52030

Description:	The TIPS Operator and the TIPS Actor are able to contact the NSP Support Teams 24 hours a day, seven days a week, all year around. The NSP Support Teams are able to trigger the procedure agreed on with the TIPS Operator as described in the Escalation Manual.
Expected result:	The TIPS Operator can contact NSP Support Teams 7x24x365. The NSP's Support Teams are aware of the procedure described in the Escalation Manual.
Detailed test procedure:	Verify how it is possible to contact the NSP Support Teams. Verify in the available documentation the service level offered by the NSP to TIPS Operator, and check the service hours. Verify whether an escalation procedure is contained in the manual.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Trouble ticketing management

Reference ID	TIPS.UC.TC.52040

Description:	The NSP records all actions, as well as the timestamp (time and date) at which the actions occur, in its central trouble ticketing system. Such system is accessible by the TIPS Actor and by the TIPS Operator via Internet.
Expected result:	The NSP's Trouble Ticketing System (TTS) records all actions and time stamps at which a service request/update takes place. TTS is accessible via Internet to both the TIPS Actors and the TIPS Operator.
Detailed test procedure:	A TIPS Operator logs-in the NSP's TTS via the internet, opens a case for testing purposes, verifies case time stamp.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Trouble ticketing report

Reference ID	TIPS.UC.TC.52050

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

Incident management and escalation

Reference ID	TIPS.UC.TC.52060

Description:	The NSP starts resolving each incident within 15 min after the incident has been reported and provides the first update to the TIPS Operator within 30 min. The NSP produces and delivers an incident report to the TIPS Operator within 24 hours from the incident time. Such a report is 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 informs the TIPS Operator in advance of any known problems and any corrective measures to be taken.
Expected result:	A MxTTI is set and a SNI is set. The NSP starts resolving each incident within 15 min after the incident has been reported and provides the first update within 30 min. Incident reports are produced within a day, when the criticality of the fault may be classified as *high*. The NSP informs the TIPS Operator in advance about any known problems and any possible workarounds.
Detailed test procedure:	Verify in the available documentation that all the service metrics as described in the "Connectivity - technical requirements" are provided. Open a test incident and go through the process. Take note of the timing of updates and reports.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Escalation of connectivity failures

Reference ID	TIPS.UC.TC.52070

Description:	The NSP has sound processes to detect, notify escalate and resolve connectivity failure.
Expected result:	The NSP has developed an operational procedure to detect, notify, escalate and resolve connectivity failures. During the test a failure is simulated and the procedure is tested.
Detailed test procedure:	Vverify the NSP has an operational procedure to handle network connectivity failures. Review the section concerning these failures and the relevant process description. Simulate a failure disabling the corresponding Ethernet interface on the 4CBNet switch. Verify this event is perceived by the NSP's monitoring, check if it triggers an alarm, see how the alarm is handled, and follow it through the incident management process.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Proactive monitoring

Reference ID	TIPS.UC.TC.53080

Description:	The NSP proactively monitors 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.
Expected result:	In line with the Operation Manual, the NSP undertakes proactive monitoring of the TIPS Platform WAN links.
Detailed test procedure:	The NSP has prepared an Operation Manual. Jointly read the manual. List the elements monitored in the Operation Manual. List the WAN links. Compare the two lists in order to verify the completeness of the Manual.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Availability and bandwidth utilization report

Reference ID	TIPS.UC.TC.53090

Description:	The NSP, on a monthly basis, reports to the TIPS Operator the availability of the monitored communication elements and the connections bandwidth utilization.
Expected result:	The NSP prepares, on a monthly basis, reports on the availability of the monitored communication elements and on the bandwidth utilization of the WAN links.
Detailed test procedure:	Read the monthly report on monitored communication elements. Check that the bandwidth utilization charts/values are available.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Imperceptibility of the TIPS Business Continuity towards the TIPS Actors

Reference ID	TIPS.UC.TC.54100

Description:	The NSP supports the TIPS Business Continuity imperceptibly to the TIPS Actor i.e. without any necessary intervention or impact on their technical configuration.
Expected result:	The NSP supports the TIPS Business Continuity without any user intervention or impact on TIPS Actor's technical configuration.
Detailed test procedure:	Simulate a TIPS Business Continuity scenario: an active site isolation. Simulate a site A failure (disable the interface on the 4CBNet switch where the NSP VPNs are connected), check if the TIPS Actor Emulator is able to access the TIPS Platform seamlessly (without any impact or change to their configuration).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Periodic rotations of the TIPS Platform

Reference ID	TIPS.UC.TC.54110

Description:	The NSP supports the TIPS Business Continuity in compliance with the TIPS-specified service levels, the periodic rotations (if needed) and backup procedures. The NSP supports traffic routing for periodic site rotations and backup procedures for the Business Continuity imperceptibly for the TIPS Actor. The end users does not perceive in which site the TIPS application is running. The rotation is fully invisible to the TIPS Actor and to the inter-connected market infrastructures, i.e. no configuration changes in the TIPS Actor's systems is necessary.
Expected result:	TIPS Platform is active on one region (site A and site B) in active / active mode. The TIPS Actor runs his own services transparently and independently of where the TIPS Platform is run; ie. a TIPS Actor does not perceive in which site the TIPS application is running. The NSP is expected to support the site failure (from site A to B or from B to A) with no impact to the TIPS Actor. The NSP solution should scalable to support a regional rotation in case of adding a second region (if ever).
Detailed test procedure:	In case of TIPS Operator site failure verify the impact on TIPS Actors is null; no impact or configuration change is expected on TIPS Actor side. No configuration changes in the TIPS Actor's systems are required. The NSP solution should be scalable to a two region model (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

TIPS Business Continuity time objectives

Reference ID	TIPS.UC.TC.54120

Description:	The NSP supports 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 switches 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.
Expected result:	The NSP supports the TIPS Business Continuity with the time goals described in the "Connectivity - technical requirements". Intra-region recovery is completed in less than 15 minutes.
Detailed test procedure:	Test the business continuity scenario (intra-region recovery) and take note of how long it takes to recover the full service operation: disable the service on the primary site and clock the time elapsed for service recovery.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

No single point of failure

Reference ID	TIPS.UC.TC.54130

Description:	The NSP designs and implements the technical infrastructure of its Solution for the TIPS Platform and configures 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.
Expected result:	The NSP designs and implements the solution avoiding any single point of failure (SPoF). Additional software and hardware components are redundant.
Detailed test procedure:	Inspect detailed technical documentation whether the technical infrastructure is designed with full redundancy. Prove there is no single point of failure. Inspect the implementation and check whether it is in line with the "Connectivity - technical requirements". Identify deficiencies (if any) and agree on corrective measures to be taken before user testing.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

DNS functionalities for Business Continuity

Reference ID	TIPS.UC.TC.54140

Description:	The NSP connects 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 communicates to the NSP one IP address for each site where a DNS server system, able to provide IP address information to the NSP, will be activated. It is also possible to agree with the TIPS platform alternative non DNS based solutions.
Expected result:	The NSP interfaces the TIPS Platform Domain Name System (DNS) in order to obtain the current location of the services and URL for A2A and U2A services. TIPS Platform has communicated to the NSP two IP addresses (one per site) where a DNS server is activated. The NSP uses this information to "route" A2A and U2A to the active TIPS Platform Site.
Detailed test procedure:	Identify the TIPS Platform DNS servers. Check that they disclose to the NSP the IP addresses of the TIPS Platform Site for the A2A and U2A application services (ie. both sites in case of active / active). The NSP is able to "route" A2A and U2A requests to the TIPS Platform.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

The NSP's Business Continuity

Reference ID	TIPS.UC.TC.54150

Description:	The NSP manages its disaster recovery solution, which affects the TIPS Connectivity Services, with the following objectives. In case of NSP recovery, the NSP supports the traffic exchange through its back-up site automatically within 15 minutes.
Expected result:	The NSP has more than a single site, the NSP is able to lose a site and to recover its services within 15min.
Detailed test procedure:	Simulate a NSP site failure, take note of the time needed by the NSP to switch the traffic to the surviving site. Verify the impacts on the TIPS Platform (if any).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.6. SECTION VI - Operation, administration and management – test cases

Service requirements – A2A message delivery time

Reference ID	TIPS.UC.TC.55010

Description:	The NSP delivers 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 commits on a Service Level of 95% of deliveries within the required delivery time.
Expected result:	Sending a message from the TIPS Actor to the TIPS Platform takes no longer than 250 ms and only 5% of the overall number of messages take longer.
Detailed test procedure:	Send messages from the Actor to the Platform at a constat rate – close to the 90% of the overall maximum allowed rate (measured in messages/sec) – for at least 16 hours and record the delivery time for each of the messages. Record the overall number of messages, record the number of messages delivered in less than 250ms, record the number of messages which took longer than that to deliver. Calculate the percentage of the "lazy" ones and make sure they are less than 5%.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Service requirements – **A2A Service availability**

Reference ID	TIPS.UC.TC.55020

Description:	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: $$ServiceAvalability = \left(\frac{ServiceTime - OutageTime}{ServiceTime} \right) \cdot 100$$ Where: • Outage time is the sum of the outage time of each NSP connected Actor (in minutes) in the reporting period; • Service Time is the sum of the expected availability time of each NSP connected Actor (in minutes) in the reporting period. The Service Availability is not less than 99,98 calculated on a monthly basis. The NSP describes in detail how the above measurements of the outage times are calculated.
Expected result:	The NSP describes how Service Availability is measured and gives evidence of what has been put in place in order to achieve the expected monthly goal.
Detailed test procedure:	Inspect the documentation provided by the NSP [desk check], then inspect [on the field] the NSP Service Availability portal (from how the availability is calculated up to the impacts of availability on invoicing).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Service requirements – **Fault clearance**

Reference ID	TIPS.UC.TC.55030

Description:

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

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:

- *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),
- *medium* (a WAN component is faulty or a link has failed),
- *low* (fault has only 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 fault status and the fault clearance progress at recurring intervals;

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

- Maximum Time To Repair (MxTTR): maximum time between the acceptance of a trouble ticket and the end of the fault clearing process. (MxTTR is temporarily suspended by the following events: 1. 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).
Expected result:	The NSP has a customer handbook describing the incident management relationship with the TIPS Operator. This customer handbook describes the incident classification and MxTTI, MxTTR and SNI.
Detailed test procedure:	[desk check] NSP's customer handbook reports three different incident priorities and explains how these are mapped into the The NSP has a customer handbook describing the incident management relationship with the TIPS Operator. This customer handbook describes the incident classification and MxTTI, MxTTR and SNI. The handbook is expected to represent a sounding description of the operational process the NSP has put in place in order to keep up with the available documentation.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

6.7. SECTION VII - Implementation - test cases

NSP infrastructure sizing

Reference ID	TIPS.UC.TC.61030

Description:	The NSP sizes its infrastructure based on its expected market share and in order to ensure it meets performance and volume requirements. The NSP sizes 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.
Expected result:	The NSP sizes its infrastructure based on its expected market share and ensures it meets the performance and volume requirements. The NSP infrastructure can support full TIPS traffic load in a single TIPS site.
Detailed test procedure:	The NSP declares to the TIPS Operator the limit used to size the solution (ie. the sounding hypothesis on top of which market share assuptions were formulated). The testing team verifies the infrastructure has been sized accordingly (desk check).
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

Connectivity Managers

Reference ID	TIPS.UC.TC.64040

Description:	The NSP – presented by the TIPS Actor – has appointed a Connectivity Manager (CM) who is the responsible central contact person coordinating all 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").
Expected result:	The NSP has appointed their own CM and the TIPS Operator has been informed about the CMs contact details.
Detailed test procedure:	The NSP' CM is appointed, he/she is the central contact person coordinating all required project activities and central point for coordinating the communication with TIPS CM.
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED [] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____

NSP Connectivity Manager Duties

Reference ID	TIPS.UC.TC.64050

Description:	The CM has 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 need 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 implementation; • to monitor the deadlines of the implementation schedule; • to have regular meetings with the TIPS Operator.
Expected result:	The CM accomplishes the duties outlined in the "Connectivity - technical requirements".
Detailed test procedure:	Jointly review the relevant documentation provided by the NSP (desk check). List the CM's duties as outlined in the applicable NSP's documentation. Compare the list with the duties outlined in the "Connectivity - technical requirements".
Outcome:	_____ _____ _____
Result:	Please describe the test result: [] PASSED

	[] FAILED If failed, then description of the follow up action: _____ _____
Formal acceptance:	TIPS testing team _____ date ____/____/____ NSP testing team _____ date ____/____/____