T2S Non Functional Tests

Report

Author	4CB
Version	1.0
Date	28/11/2014
Status	Final
Classification	

1. Business Continuity

1.1. Summary

This chapter describes the Business Continuity tests performed during the NFT test campaign, the general workflow of the tests and the related results.

The primary site failure test was successfully executed on 11th October, the regional recovery test was successfully executed on 25th October.

The primary site test for region 3 (intra-regional recovery) was successfully executed on 24th November.

1.2. Introduction

The objective of the Business Continuity tests is to prove the ability of T2S to meet the agreed service levels even in case of severe incidents, intra-region and inter-region failover.

Three types of service interruptions have been considered in designing the tests:

- **Short continuity failure** is understood as a short service interruption (e.g. due to component failures, a system reboot, or a line failure). These incidents may typically be solved at the primary site using redundant and reliable infrastructures. So no action is required for such kind of failure.
- **Primary site failure** is understood as a serious service interruption (e.g. disruptions caused by fire, flood, terrorist attack or major hardware/telecommunications faults) that makes the primary site unavailable. These events require the activation of an alternative regional site.
- **Regional disaster** is understood as a "wide-scale regional disruption" causing severe permanent interruption of transportation, telecommunication, power or other critical infrastructure components across a metropolitan or geographical area and its adjacent communities (resulting in a wide-scale evacuation or inaccessibility of the population within the normal commuting range of the disruption's origin). These events require the activation of an alternative region.

1.3. Overview

- **List of Non Functional Business Continuity tests**

The following table summarizes the Business Continuity test cases executed:

ID	Short description
BC_PSA_01	Primary Site A Failure test for region1/2
BC_RD_01	Regional disaster test for region1/2
BC_PSE_01	Primary Site A Failure test for region 3

All the tests involved the T2S production environment (with zOS, AIX and Open systems active) simulating normal operational condition before starting the test.

Disaster simulation was based on the unavailability of one core infrastructure (i.e. storage disk infrastructure).

- **Reporting**

No measurement tools were used for the RTO; the RPO was measured by storage infrastructure utilities.

1.4. BC_PSA-01: Primary Site Failure for Region 1/2

The test involved the T2S production environment (zOS, AIX and Open systems active) and referred to a fault in the storage disk infrastructure.

More in detail, the disaster was simulated by disabling the primary storage subsystem in the primary site while producing I/O on z/OS and open systems.

1.4.1. Expected Results

Primary Site A failure test was aimed at verifying that T2S infrastructure was able to restart on the secondary site after a disaster which had made the primary site unavailable.
The expected results for this test were to:

- Verify that the full procedure (including restart of T2S core services) would take a maximum of 1 hour (RTO=1hour);
- Verify that all processing systems were able to restart on the secondary site using consistent data and without data loss (RPO=0);
- Start incremental asynchronous resynchronization between site B and site C (with no need for a full copy);
- Restart all systems on site B without waiting for end of resynchronization between site B and site C;
- Restart all the auxiliary systems (STS …).

1.4.2. Test Execution

The test execution was divided into the following phases:

- **Disaster simulation:**
  - Primary Site Disk subsystem access was made unavailable
- **Failover phase execution:**
  - This phase included the following steps :
    - Verifying that no data was lost and checking where the most recent data was located (site B or site C);
    - Configuring volumes on site B as primary;
    - Starting incremental asynchronous resynchronization between site B and site C (if more recent data was located on site C, rescue data from site C without involving a full copy or a change in the session synchronization direction);
    - Restarting all systems on site B without waiting for the end of resynchronization between site B and site C.

    The target RTO and RPO were verified with respect to this phase (disaster simulation is outside RTO and RPO verification).
- **End to end tests execution**

  This phase was aimed at checking the regular behaviour of T2S in recovery conditions.

1.4.3. General workflow

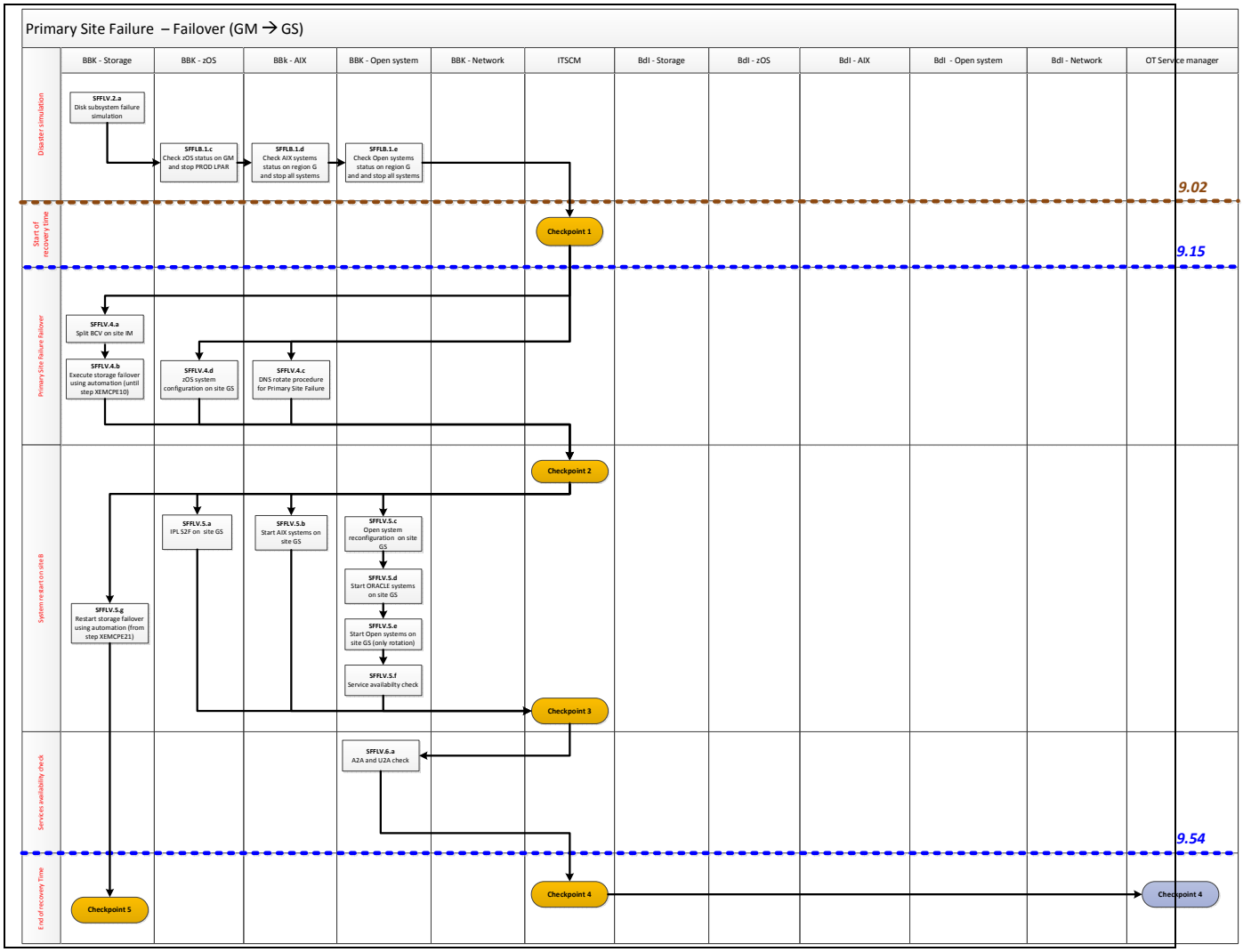

Figure: BC_PSA-01 General workflow

1.4.4. Test results

	Test result	SLA requirement	Status	Note
RTO	34 minutes	< 60 minutes	OK	Disaster simulation : **09:02** Failover starting time : **09.15** End-to-end test and communication to OT : **9.54** OT confirmation : **10:03**
RPO	0	0	OK	Volume status check on the other sites (B,C,D) report that no invalid tracks are present.
Incremental asynchronous resynch between site B and site C	YES	YES	OK	Incremental resynch started at 9.31 Incremental resynch finished at 10.01
Are systems able to restart B without waiting for end of resynchronization between site B and site C ?	YES	YES	OK	Authorization to systems restart was communicated to TT at 9.29 before starting incremental resynch.

Table: BC_PSA-01 Test Results

1.5. BC_RD-01: Regional Disaster for Region 1/2

The test involved the T2S production environment (zOS, AIX and Open systems active) and referred to a fault in the storage disk infrastructure.

More in detail, the disaster was simulated making storage connectivity between the two Regions unavailable while producing I/O on z/OS and open systems.

1.5.1. Expected Results

The Regional disaster test focused on verifying that T2S was able to restart on the secondary site of the surviving Region after a disaster making the primary Region unavailable.

The expected results for this test were to:

- verify that the full procedure (including restart of T2S core services) would take a maximum of 2 hours (RTO<=2 hours);
- verify that all processing systems were able to restart using consistent data and with a maximum data loss of two minutes (RPO<=2 minutes);
- start incremental resynchronisation between the secondary site and the primary site (with no need for a full copy);
- restart all the auxiliary systems (STS, …).

1.5.2. Test Execution

The test execution was split into two phases:

- **Disaster simulation**
  - Storage connectivity between the two sites was made unavailable preventing real-time asynchronous replication between the two Regions.
- **Failover phase execution**
  - This phase included the following steps :
    - Verifying data consistency and time stamp at site C (timestamp was used to verify that RPO<=2 minutes);
    - Moving adaptive Replication from site C to site D in synchronous mode and waiting for complete alignment;
    - Changing the synchronous replication direction from site C to site D making primary the volumes on site D (as an alternative: deleting adaptive replication from site C to site D and defining a new synchronous replication session from site D to site C avoiding any resynchronization);
    - Starting applications on site D.

    The target RTO and RPO were verified with reference to this phase (disaster simulation is outside of RTO and RPO verification).
- **End to end tests execution**

  This phase was aimed at checking the regular behaviour of T2S in recovery conditions.

1.5.3. General workflow

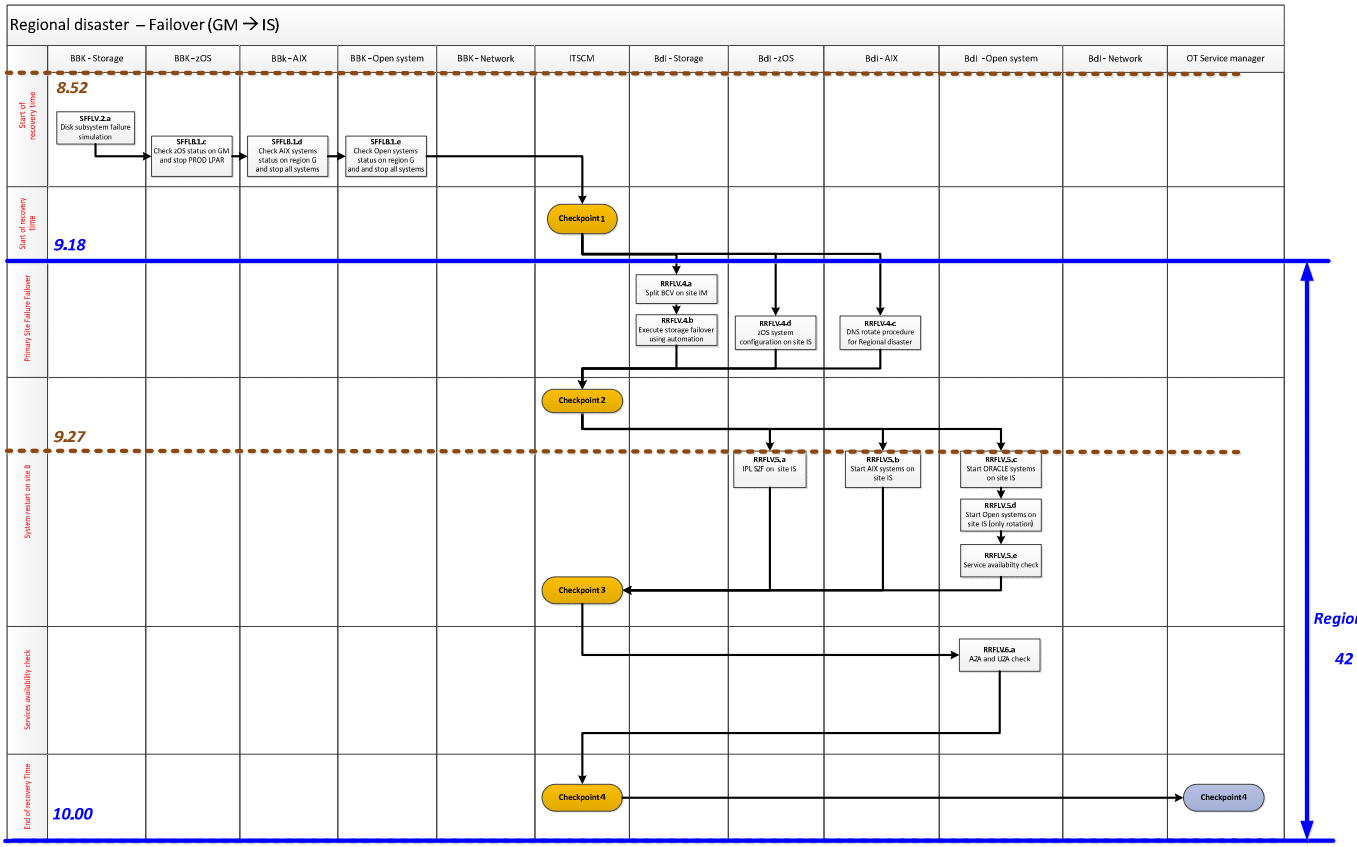

Figure: BC_RD-01 General workflow

1.5.4. Test results

	Test result	SLA requirement	Status	Note
RTO	42 minutes	<= 2 Hours	OK	Disaster simulation : **8.52** (out of critical path) Starting time for failover **: 9.18** Systems restart : **9.27** End-to-end test successfully completed : **10.00** Operational team check : **10:19** (out of critical path)
RPO	43 seconds	<= 2 minutes	OK	last update data on region I : 8.52.31 Network failure: 8.53.14
Incremental asynchronous resynch between site D and site C	YES	YES	OK	Incremental resynch automatically completed during storage failover phase
Auxiliary systems restart	YES	YES	OK	All open systems related to external DMZ were active at the end of the failover procedure.

Table : BC_RD-01 Test Results

1.6. BC_PSE-01: Primary Site Failure for Region 3

The test involved the T2S LTSI production environment (both Business Intelligence reporting and loading tools) and was mainly focused on the ability to restart all systems (UNIX/Linux and Windows systems) on the Region 3 recovery site.

More in detail, the disaster was simulated by disabling the Business Intelligence reporting servers of the LTSI production primary environment.

1.6.1. Expected results

The expected results for this test were to:

- Verify that the switch procedure would take a maximum of 24 hours (RTO=24hours).
- Verify that all systems were able to restart on the Region 3 recovery site using consistent data and without data loss (RPO=0).

- Verify that file transfer between Region 1-2 and Region 3 on the A2A channel was properly working after rotation to the second site;
- Verify that internal and external (U2A) connection to LTSI were properly working after rotation to the second site;
- Verify that loading and archiving of files was properly working after rotation to the second site;
- Verify the overall functioning of the LTSI and LEA applications;
- Verify that rotation back to the main site would meet the requirements listed above.

1.6.2. Test Execution

Test execution was split into the following phases:

- **Rotation phase execution 1**
  - Execution of the site rotation chain
  - Rotation to the secondary site

- **Connectivity phase execution**
  - Internal connection test from Development Team
  - Internal connection test from Functional Team
  - Internal connection test from Technical Team
  - Internal connection test through U2A channel

- **File transfer, loading and archiving phase execution**
  - File transfer test between Region 1-2 and Region 3
  - File loading test
  - File archiving test

- **Overall functioning check phase**
  - Verification of the regular behaviour of T2S LTSI and LEA applications

- **Rotation phase execution 2**
  - Execution of the site rotation chain
  - Rotation to the primary site

- **Connectivity, file transfer and overall functioning phases**

1.6.3. General workflow

The NFT Business Continuity consisted in performing a LTSI site recovery test and then in validating the following processes:

- EN2END File transfer from Region1-2 to Region3
- Simulation of an external users HTTP request to LTSI (wget)
- The business continuity model for Region 3:
    - Fault tolerance: RTO≤2h; RPO=0;
    - Intra-region recovery: RTO≤24h; RPO=0.

- **File transfer from Region1-2 to Region3**

The END2END was successfully sent from Region1-2 to Region 3 LTSI before and after the site recovery test:

- END2END file transfer from Region1-2 to Region LTSI before site recovery : OK
- END2END file transfer from Region1-2 to Region LTSI after site recovery : OK

- **External users connection to LTSI**

Since the SOPS-WP in the PROD environment hosted in Region1-2 will not be available before 02/2015, only connectivity tests from Region1-2 reverse proxies to LTSI have been performed.

- Technical tests (wget) from Region 1-2 Reverse Proxies to Region 3 LTSI before site Recovery (without DNS configuration) : OK
- Technical tests (wget) from Region 1-2 Reverse Proxies to Region 3 LTSI after site Recovery (without DNS configuration) : KO – The issue was investigated: a misconfiguration of the LTSI VIPA has been detected and is now fixed.
- Technical tests (wget) from Region 1-2 Reverse Proxies to Region 3 LTSI before site Recovery (with DNS configuration) : Not tested – The wrong URL was used during the test.
- Technical tests (wget) from Region 1-2 Reverse Proxies to Region 3 LTSI after site Recovery (with DNS configuration) : KO – The DNS alias lookup has failed. This issue is being investigated by both Region1-2 and Region3.

- **Business continuity model for Region 3**
    - The site recovery test (intra-regional recovery) has been performed in 45 minutes.
    - No data has been lost.

1.6.4. Test results

	Test result	SLA requirement	Status
RTO	45’	<= 24h	OK
RPO	0	0	OK

Table: BC_PSE-01 Test Results

2. Security

2.1. Summary

All information security tests were executed between June and October 2014, covering both application-level and infrastructure related tests.

4CB internal test reports were distributed on a regular basis throughout the testing phase to a minimum set of relevant experts in order to eliminate false positive, confirm findings (identified vulnerabilities) and identify mitigation actions. This close cooperation allowed to address all findings efficiently. As most of the actions were completed from July to November 2014, residual risk was thus lowered to a minimum level.

4CB information security experts have surveyed both the test reports and the status/schedule of mitigation actions in order to assess the residual risk situation considering the T2S go-live date as a reference point in time.

As a result, a single vulnerability present in certain categories of network equipment used for the internal T2S network, namely the 4CBNet, will need to be addressed thereafter (a technical version upgrade is already planned by end 2015). During the interim period, the resulting risk will have to be temporarily accepted.

2.2. Overview

2.2.1. Methodology Used

The T2S Security Requirements and Controls1 (T2S SRC) are derived from the high level security requirements expressed in Chapter 18 of the T2S URD and based directly on ISO standard 27002:2005.

The T2S SRC states that:

"As a general rule, the implementation of the security controls specified in this document is mandatory. However, it might be that due to specified technical and/or environmental circumstances (e.g. contradicting national legislation) the application of a particular security control is not feasible. If this was the case, it will have to be justified in the context of the security assessment, more specifically when the compliance of T2S with the T2S SRC is checked, why it is not possible to implement this particular security control. The associated residual risk must then be accepted."

"All security requirements and controls included in this document are specified from a business perspective and have to be implemented by the service provider (4CB) responsible for designing, building and operating T2S."

The compliance and risk assessment process[2] is used to assess the overall T2S Information Security risk situation. This includes as a first step to take the defined security requirements and controls as the reference

[1] See Framework Agreement Schedule 10 – Annex 2.

and perform a compliance check by validating the completeness and effectiveness of the actual implementation of these controls within the scope of T2S.

In order to assess whether the 4CB have implemented the T2S Information Security management framework, in particular by designing, developing and operating the T2S Platform in accordance with the T2S SRC, the following approach is adopted:

- A global compliance and risk assessment process is followed, resulting in the preparation of the T2S Pre-Production Security Assessment (PPSA), with 3 inter-related deliverables, namely:
    - Answers to the Security Compliance Check Questionnaire (SCCQ) covering all questions related to the T2S SRC controls;
    - The Risk Evaluation Table (RET). It provides the likelihood each threat (of the T2S Threat Catalogue) has to materialise into a risk, as well as its potential impact, taking into account the compliance level reached for all controls related to the threat;
    - The Risk Treatment Plan (RTP). This plan proposes a treatment (i.e. a mitigation measure or acceptance) for the risks listed in the RET.

  This process applied to the whole T2S scope is triggered every three years, firstly before the go-live of T2S (the "Pre-Production Security Assessment"). The PPSA will be delivered by the 4CB by end 2014. In turn, as described in the Framework Agreement[3], the Eurosystem will share information with the contracting CSD about the risk situation (in the form of the T2S Information Security Risk Evaluation Table or ISRET and, together with each ISRET entry, the proposed corresponding T2S Information Security Risk Treatment Plan or ISRTP).
- In addition, for one particular security control (T2S SRC 14.2.2 "Technical Compliance Checking"), specific non-functional tests were executed. The purpose of this document is to describe how these specific non-functional test cases were defined and executed. As a result, the 4CB will deliver prior to the go-live of T2S a risk assessment of the residual vulnerabilities (if any) considering mitigation measures implemented before T2S starts its operations. As a complement to the ISRET and ISRTP generated on the basis of the PPSA, the Level 2 will share the relevant information with the contracting CSD about the risk situation entailed by any residual vulnerability that may still be present at the go-live date.

2.2.2. Non Functional requirements to be fulfilled through testing

Specific test cases were performed to address URD T2S.18.1300 / T2S SRC 14.2.2 "Technical Compliance Checking". These tests aimed at establishing the level of compliance obtained by the T2S Platform with technical security specifications. As any non-compliance could be identified as a potential cause for risks materialising, the finality of these tests was to assess to what extent (even partially) non-compliant implementation of security controls may lead to any residual risks.

[2] See Framework Agreement Schedule 10 – Section 4: The T2S Information Security Risk Management Process.

[3] See Framework Agreement Schedule 10 – Section 4.2: Deliverables to the Contracting CSD.

Vulnerability assessment and penetration test activities were executed, resulting in the production of finding reports which were used to define action plans aiming at mitigating the vulnerabilities.

2.2.3. List of Non Functional Security Tests Executed

The following table summarizes the test cases perfomed. For each test case the following information is provided:

ID	Short description
SEC_01	Application level vulnerability tests
SEC_02	Infrastructure vulnerability tests

It must be noted (in line with T2S SRC 14.2.2) that vulnerability tests and penetration tests were partially executed by third party security experts duly mandated to do so under the proper supervision of competent and authorised 4CB staff members. Other security tests were performed by specialised and authorised 4CB members of staff (who in this case were distinct from the security experts in charge of performing the risk assessment of test results).

2.2.4. High level planning

- The security-related Non Functional Tests were executed between June and October 2014.
- The analysis of findings was performed between July and November 2014.
- The assessment by 4CB security experts of the residual risk situation was made between September and November 2014, based on actions scheduled to tackle all findings (i.e. identified technical vulnerabilities), and considering the reference point in time as of the go-live date.

As a result, the residual risk situation is entailed by all findings which will not be properly addressed by 22 June 2015.

2.2.5. Reporting

As their contents may be used to harm the interests of the System Owner, neither the detailed documents describing test cases nor the detailed reports of findings will be published. In compliance with T2S SRC 14.2.2 and security best practices, only a restricted list of authorised 4CB security experts, relevant technical experts and managers will have access to these sensitive documents.

As explained in section 2.2.2, the deliverables shared with the Level 2 will be limited to **risk assessments of the residual vulnerabilities**. These assessments reflect the risk situation after the implementation of actions addressing the findings identified during the aforementioned tests.

Taking into account the findings documented in the test reports, the mitigating action plans and the actual implementation status of the actions as of the T2S go-live date, the Eurosystem is providing in the current report to the contracting CSD and Central Banks as per the T2S Information Security Risk Management process, the Risk Evaluation Table and the risk Treatment Plan with an indication of the residual risk situation after the implementation of the actions addressing all the findings identified during the tests. Each identified risk is scored in terms of likelihood and impact using the grading scales applicable in the T2S context.

2.3. SEC_01: Application level vulnerability tests

In December 2013, the 4CB Project Steering Committee approved the Letter of Authorisation (LOA) describing the test campaign, thus giving the green light to organise and execute the T2S application level vulnerability tests. The LOA addressed at once application-level and infrastructure-related tests.

2.3.1. Test objective

The objective of the application level vulnerability tests is to address URD T2S.18.1300 / T2S SRC 14.2.2 ("Technical Compliance Checking") by ensuring that the T2S applications are free of any relevant security threats and able to manage user interaction while avoiding the Open Web Application Security Project (OWASP) security top ten[4] vulnerabilities.

2.3.2. Test case description

The test activity was conducted executing the applications and checking the presence of vulnerabilities according to the OWASP testing criteria[5].

The components involved in the activity were all web based software modules of the applications connected to external networks.

The tests on the software modules were conducted in a "White Box" approach trying to identify the typical web vulnerabilities[6].

4 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

5 https://www.owasp.org/index.php/Category:OWASP_Testing_Project

6 The web vulnerabilities can be exploited, for example, with the following attacks: Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Cross-Site Request Forgery (CSRF), Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards, etc.

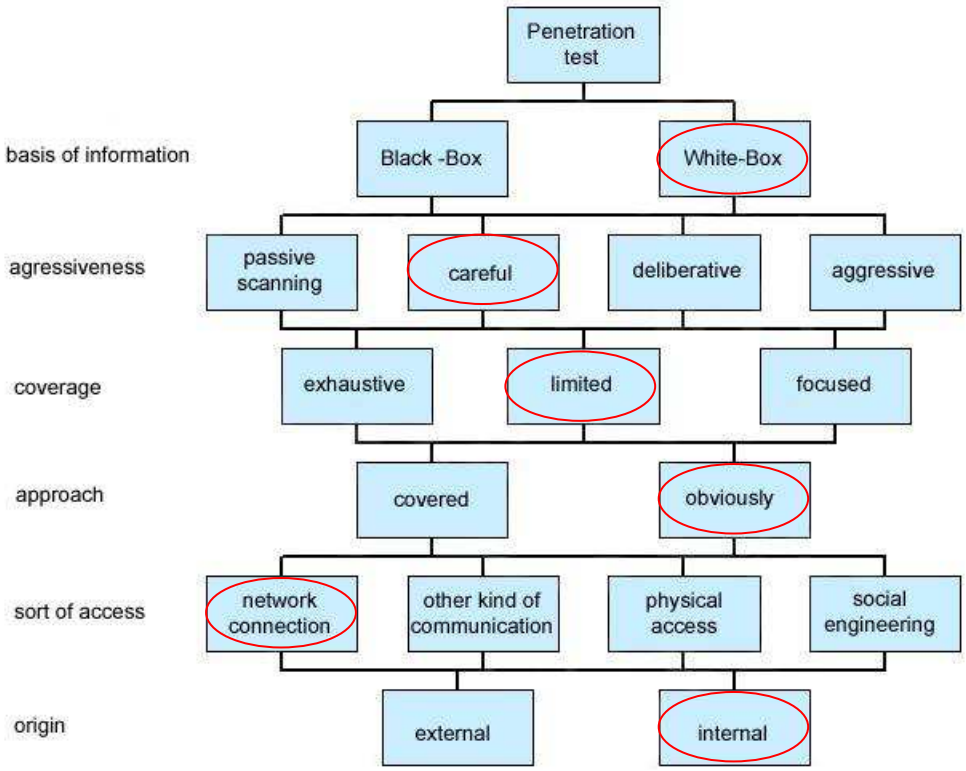

Figure: OSWAP test criteria diagram

The application level vulnerability tests followed the guidelines provided in the OWASP Testing Guide. Thus tests were performed in the framework of the following categorisation: Information Gathering, Configuration Management Testing, Authentication Testing, Session Management Testing, Authorization Testing, Business Logic Testing, Data Validation Testing, Denial of Service Testing, Web Services Testing, AJAX Testing.

Additional tests outside OWASP testing criteria were conducted in order to identify additional typical application vulnerability. In particular, specific XML oriented applicative security tests were conducted on the A2A access link, in order to detect possible XML vulnerabilities.

2.3.3. Test Execution

- **Tests in Region 2**

Tests were carried out in Deutsche Bundesbank (Region 2) from 15/09/2014 to 23/09/2014 by an external third party in order to provide an independent evaluation of T2S application services.

The following test steps (not exhaustive list) were performed:

- Application services discovery and information gathering:
    - Map visible content;
    - Discover hidden & default content;

  - Test for debug parameters;
  - Identify data entry points;
  - Identify the technologies used;
  - Map the attack surface.
- Testing of handling of access
  - Authentication tests;
  - Test password quality rules;
  - Test for username enumeration;
  - Test resilience to password guessing;
  - Test any account recovery function;
  - Test any "remember me" function;
  - Test any impersonation function;
  - Test username uniqueness;
  - Check for unsafe distribution of credentials;
  - Test for fail-open conditions (non-authenticated access);
  - Test any multi-stage mechanisms;
  - Session handling;
  - Test tokens for meaning;
  - Test tokens for predictability;
  - Check for insecure transmission of tokens;
  - Check for disclosure of tokens in logs;
  - Check mapping of tokens to sessions;
  - Check session termination;
  - Check for session fixation (client-side authentication token definition);
  - Check for cross-site request forgery;
  - Check cookie scope;
  - Access controls;
  - Understand the access control requirements;
  - Test effectiveness of controls, using multiple accounts;
  - Test for insecure access control methods (Referer, etc).
- Testing handling of input
  - Fuzz all request parameters;
  - Test for SQL injection;
  - Identify all reflected data;

  - Test for reflected XSS;
  - Test for HTTP header injection;
  - Test for arbitrary redirection;
  - Test for stored attacks;
  - Test for OS command injection;
  - Test for path traversal;
  - Test for script injection;
  - Test for file inclusion;
  - Test for SMTP injection;
  - Test for native software flaws (Bof, integer bugs, format strings);
  - Test for SOAP injection;
  - Test for LDAP injection;
  - Test for XPath injection.
- Test application logic
  - Identify the logic attack surface;
  - Test transmission of data via the client;
  - Test for reliance on client-side input validation;
  - Test any thick-client components (Java, ActiveX, Flash);
  - Test multi-stage processes for logic flaws;
  - Test handling of incomplete inputs;
  - Test trust boundaries;
  - Test transaction logic.
- Assess application hosting
  - Test segregation in shared infrastructures;
  - Test segregation between applications;
  - Test for web server vulnerabilities;
  - Default credentials;
  - Default content;
  - Dangerous HTTP methods;
  - Proxy functionality;
  - Virtual hosting mis-configuration;
  - Bugs in web server software.
- Miscellaneous tests
  - Check for DOM-based attacks;

- Check for frame injection;
- Check for local privacy vulnerabilities;
- Persistent cookies;
- Caching;
- Sensitive data in URL parameters;
- Forms with autocomplete enabled;
- Follow up any information leakage;
- Check for weak SSL ciphers.

- Deny of service on applications tests
- Attempts to exploit the previously discovered vulnerabilities.

The output of the activity was a 4CB *internal* report listing all of the identified non compliances and potential security issues (vulnerabilities). Each vulnerability was addressed by the related teams who proposed a set of mitigation measures (most of which were retained in the action plans foreseen to lower the level of residual risk to a minimum).

4CB technical observers controlled the proper performance of the activity throughout the period and scrutinised the findings reported as well as the subsequent 4CB internal follow-up.

- **Tests in Region 3**

Tests were carried out in Banque de France (Region 3) by the BDF CERT "Red" Team from 01/07/2014 to 11/07/2014 to evaluate the security level of the LTSI module.

The Application-level vulnerability assessment of LTSI comprised web server security checks as well as the assessment of application common vulnerabilities. The Nessus Burp Suite was used.

4CB technical observers controlled the proper performance of the activity throughout the period and scrutinised the findings reported as well as the subsequent 4CB internal follow-up.

Prior test results were also considered in the assessment of the LEA module though no external interface is offered to T2S Actors.

2.3.4. Test Results - Test Case Objective Achievement

- **Tests in Region 2**

The tests had a focus on U2A (User to Application) and A2A (Application to Application) interfaces of the T2S Application. Additionally, access was given to the Data Migration Tool (DMT) via an "upload-only" user.

U2A

The provided user accounts included access to 2 NCB Accounts and 2 CSD accounts with 2 tokens. These accounts all have different access levels and rights. The OWASP Testing Guide (V3) was used to check against common vulnerability classes. In particular, the application provides a robust protection against Injection attacks throughout the tested accounts. Most of the input fields and values have predefined character sets that are accepted by the application. Other characters are rejected without being processed.

Restriction: It was impossible to test the "Working/Closing Days" section in Static Data due to missing privileges.

A2A

The testers accessed the A2A interface using an AIX machine that accepts prepared XML data in defined directories. The directories are polled for new files that are then signed and sent to the SWIFT SAA system. This system appends SWIFT related data and sends everything to the A2A interface of T2S.

With this approach, the processing that involved SWIFT heavily modify the XML files so the planned attacks did not reach the A2A interface as they were modified and rejected at the SWIFT level.

At the end of the testing time no modified XML files had reached the A2A interface. All test cases were blocked at the SWIFT SAA stages.

Restriction: the testers could not comment on the possible security status of the T2S Connector as it was not readily available during the testing period.

DMT

The accounts used to test the DMT only had the ability to upload XLSX and CSV files. The testers were not able to "release" these files to the T2S system for further processing. In this context, initial parsing of the uploaded files and other OWASP relevant issues were tested.

Results for Region 2 Tests

As a result of U2A, A2A and DMT tests, a number of technical vulnerabilities were identified. The 4CB security experts linked them to the following threats:

- T01 Carrying out denial of service attacks
- T02 Hacking
- T13 Introducing malicious code
- T16 Gaining unauthorized access to systems or networks
- T17 Changing system privileges to either enable or deny access to information or functionality
- T21 Misusing systems to commit fraud

After careful review of the findings by the relevant technical experts, some of the initial findings were dismissed as false positives, and for all vulnerabilities the presence of which was acknowledged by the technical experts, appropriate mitigation actions were approved by the relevant line managers, planned and (as of 01 December 2014, partially) executed.

The 4CB security experts considered the mitigation action plans and the related status reports to assess the residual risk situation as of the go live date (see · '**Test case objective achievement**' below).

- **Tests in Region 3**

LTSI

Restriction: web applications provided access to empty databases when the tests were conducted, which somewhat lowers the relevance of these tests[7].

LEA

Restriction: No 4CB technical observers were involved in the domestic tests performed by Banque de France teams. However, the findings were shared with the 4CB technical observers and 4CB security experts.

Results for Region 3 Tests

As a result of the application vulnerability assessment of LTSI and LEA, a number of technical vulnerabilities were identified. The 4CB security experts linked them to the following threats:

- T01 Carrying out denial of service attacks
- T04 Cracking passwords
- T08 Spoofing user identities
- T16 Gaining unauthorised access to systems or networks
- T17 Changing system privileges without authorisation
- T19 Modifying or inserting transactions files or databases without authorisation
- T21 Misusing systems to commit fraud
- T22 Installing unauthorised software
- T24 Disclosing business information

After careful review of the findings by the relevant technical experts, some of the initial findings were dismissed as false positives, and for all vulnerabilities the presence of which was acknowledged by the technical experts, appropriate mitigation actions were approved by the relevant line managers, planned and (as of 01 December 2014, partially) executed.

The 4CB security experts considered the mitigation action plans and the related status reports to assess the residual risk situation as of the go live date (see · '**Test case objective achievement**' below).

- **Test case objective achievement**

The 4CB security experts assessed the U2A to provide a soundly secure access to T2S. All user inputs are either sanitised or entirely rejected if not compatible with T2S specifications. For A2A and DMT, as well as for the LTSI, the 4CB security experts also assessed the solution to be safe with the caveat that as some restrictions applied to the scope of tests the security assessment is likewise somewhat (but not significantly) restricted in its scope[8].

[7] Additional tests will be run during the 1st quarter of 2015 and any residual risks will be brought to the attention of the ISSG as required.

[8] Further testing will be performed during the 1st quarter of 2015 and any residual risks will be brought to the attention of the ISSG as required.

All in all, no significant risk was identified during the assessment of the test results. Moreover, the residual risk situation is deemed acceptable considering all actions taken as of 01 December 2014 and those planned to be completed by the T2S go live date (22 June 2015).

2.4. SEC_02: T2S infrastructure vulnerability tests

In December 2013, the 4CB Project Steering Committee approved the Letter of Authorisation (LOA) describing the test campaign, thus giving the green light to organise and execute the T2S infrastructure level vulnerability tests. The LOA addressed at once application-level and infrastructure-related tests.

2.4.1. Test objective

The objective of the infrastructure vulnerability tests is to address URD T2S.18.1300 / T2S SRC 14.2.2 ("Technical Compliance Checking") by ensuring that infrastructure built to host and operate the T2S platform is free of any relevant security threat and is not exposing any unneeded service.

2.4.2. Test case description

The internal T2S components, **not connected to external networks**, were submitted to a vulnerability assessment. The test was executed for each category of components, not repeating it for components of identical configuration.

The T2S components **connected to external networks** were submitted to a vulnerability assessment. Additionally, a few selected critical components were submitted to penetration test activities. The tests were executed for each category of components.

The involved components are the T2S assets accessible using IP addresses[9]:

- all installed operating systems[10] and the related baseline components, and
- all active network devices.

As some components are shared by T2S and the TARGET2 SSP, the test activity was conducted referring, for those components used by T2S, to the outcome of similar infrastructure vulnerability tests performed by TARGET2.

[9] Non-IT devices will not be included in the tests. For appliances, tests will conducted where technically possible (e.g. the appliances must have an IP address and must have some software interacting wirh the network).

[10] The z/OS systems' configuration will be verified manually, based on configuration documentation.

The selection of the testing path for the vulnerability assessment will be done according to the FOIS Penetration Testing Model[11]:

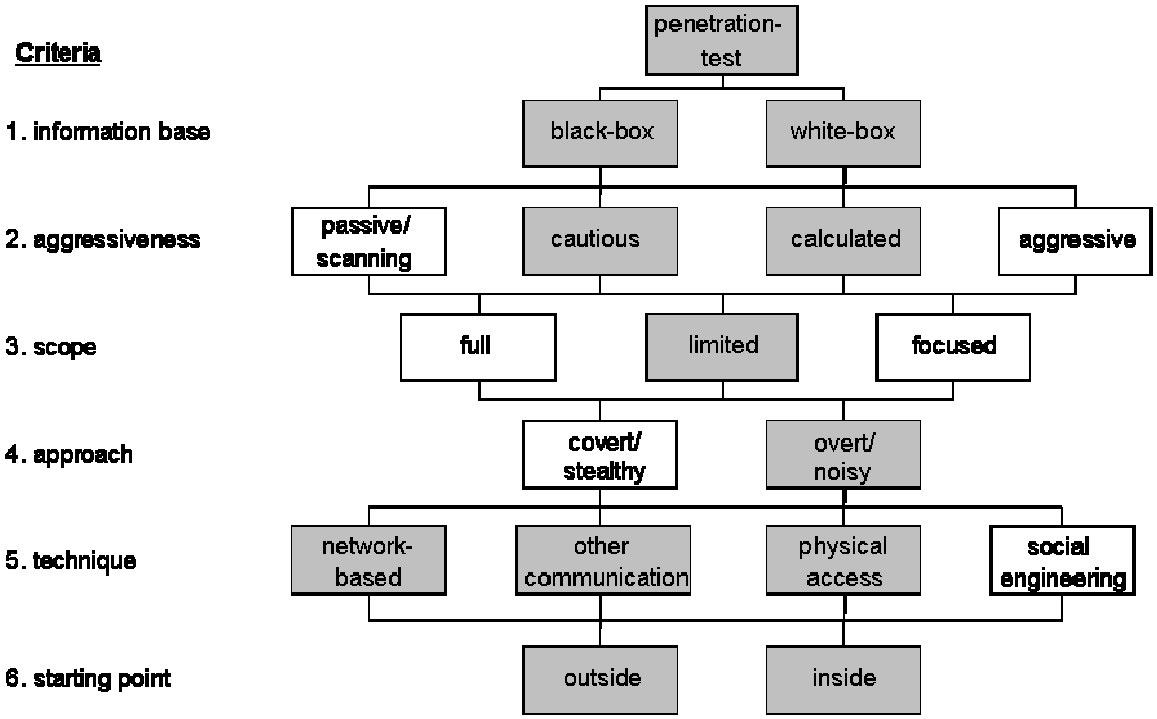

Figure: FOIS Penetration Testing Model

2.4.3. Test Execution

- **Tests in Region 1**

Tests were carried out in Banca d'Italia (Region 1) from 26/05/2014 to 06/06/2014 by an external third party in order to provide an independent evaluation of the T2S infrastructure. Tests were performed as much as possible using automatic security software tools, or alternatively by performing manually a compliance checking of the configurations of the assets in line with the applicable "T2S SRC" controls.

Network security tests

The following test steps (not exhaustive list) were performed:

- Network discovery and information gathering;
- Network devices common vulnerabilities (firmware version, missing security patches, etc.);

[11] German Federal Office for Information Security - Penetration Testing Model: https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/28198/penetration_pdf.pdf (pages 13 -17)

- Detectable ports scanning;
- Detectable services scanning;
- Filtering configuration checks (VLANs, firewalls rules, etc.);
- Network devices administration security checks (authentication method, authorized admin protocols, password policy, etc.)
- IDS/IPS configuration and detection capabilities checks;
- Network denial of service attempts;
- Attempts to exploit the previously discovered vulnerabilities.

System security tests

The following tests (not exhaustive list) were performed during the vulnerability assessment on identified groups of operating systems:

- Operating system common vulnerabilities;
- Base application common vulnerabilities;
- Useless, weak or obsolete available services;
- Security configuration settings checks (access rights, security settings, etc.);
- Privilege escalation security checks,
- Gain administrative access (remotely);
- Gain a shell (remotely);
- Execution of unauthorized functions or software;
- Local vulnerabilities;
- Access to unauthorized or sensitive business or technical information;
- System deny of service attempts;
- Attempts to exploit the previously discovered vulnerabilities.

The output of the activity was a 4CB *internal* report listing all of the identified non compliances and potential security issues (vulnerabilities). Each vulnerability was addressed by the related teams who proposed a set of mitigation measures (most of which were retained in the action plans foreseen to lower the level of residual risk to a minimum).

4CB technical observers controlled the proper performance of the activity throughout the period and scrutinised the findings reported as well as the subsequent 4CB internal follow-up.

- **Tests in Region 3**

Tests were carried out in Banque de France (Region 3) by the BDF CERT "Red" Team from 01/07/2014 and 11/07/2014 to evaluate the security level of the LTSI-related infrastructure components.

The infrastructure level vulnerability assessment of LTSI comprised a network assessment from internal Banque de France´s network to T2S servers, with a scan of Detectable and useless ports and a scan of Detectable and useless services. Nmap was used as tool for network sweeping.

4CB technical observers controlled the proper performance of the activity throughout the period and scrutinised the findings reported as well as the subsequent 4CB internal follow-up.

Prior test results were also considered in the assessment of the LEA though no external interface is offered to T2S Actors.

2.4.4. Test Results - Test Case Objective achievement

- **Tests in Region 1**

The tests focused on active network devices, AIX systems, Linux systems and Windows systems, for which a complete vulnerability assessment was carried out.

Scope of the tests:

- All the VLAN were scanned during a first phase of "information gathering".
- A vulnerability scanning phase was conducted as follows:
    - About 30 servers (or other devices) of different types (AIX, Linux, Windows) were scanned.
    - All 4CBNet devices (about 45) were checked, including routers, switches, RADIUS servers and network management platform configuration either via a scanning tool or manually.
    - The Firewalls (FW) configuration check was conducted on about 20 devices (logical or physical) of all the 4CBNet: a tool was used and, as a heuristic approach, 10% of the checks were conducted manually.
- The number of intrusive tests (and exploitation of vulnerabilities) was defined after the vulnerability scanning phase. Due to the limited timeframe, exploitation was attempted for the most critical 10% of the discovered vulnerabilities.

It has to be noted that additional checks (but not vulnerability scanning per se) were carried out on the z/OS mainframe in order to identify potential security misconfigurations or other issues.

Results for Region 1 Tests

As a result of the aforementioned vulnerability scanning, a number of technical vulnerabilities were identified. The 4CB security experts linked them to the following threats:

- T04 Cracking passwords

- T13 Introducing malicious code
- T17 Changing system privileges to either enable or deny access to information or functionality
- T34 Malfunction of system software
- T35 Malfunction of computer / network equipment

The 4CB security experts considered the mitigation action plans and the related status reports to assess the residual risk situation as of the go live date (see · '**Test case objective achievement**' below), and in particular identified one residual risk related to T17:

T17 Changing system privileges to either enable or deny access to information or functionality

The Juniper JunOs installation on some 4CBNet network devices contains a vulnerability that allows local users to raise their privileges. However, the Juniper SIRT is not aware of any malicious exploitation of this vulnerability. Moreover the JunOs versions run on some network devices will be updated by end 2014. It is foreseen that for the remaining devices, an upgrade will be available by the end of 2015. In this context, it is recommended to accept the residual risk until next upgrade cycle.

- **Tests in Region 3**

Results for Region 3 Tests

As a result of the application vulnerability assessment of LTSI and LEA, a number of technical vulnerabilities were identified. The 4CB security experts linked them to the following threats:

- T01 Carrying out denial of service attacks
- T04 Cracking passwords
- T08 Spoofing user identities
- T16 Gaining unauthorised access to systems or networks
- T17 Changing system privileges without authorisation
- T21 Misusing systems to commit fraud
- T22 Installing unauthorised software

After careful review of the findings by the relevant technical experts, some of the initial findings were dismissed as false positives, and for all vulnerabilities the presence of which was acknowledged by the technical experts, appropriate mitigation actions were approved by the relevant line managers, planned and executed.

The 4CB security experts considered the mitigation action plans and the related status reports to assess the residual risk situation as of the go live date (see · '**Test case objective achievement**' below).

- **Test case objective achievement**

All in all, and considering all actions taken as of 01 December 2014 and those planned to be completed by the T2S go live date (22 June 2015), only one significant residual risk was identified during the assessment of the test results. Consequently, the 4CB security experts reckon the residual risk situation as follows:

Risk situation as of T2S go-live (22 June 2015)	Residual Risk				Explanation
	Likelihood	Impact			
		Business	Reputation	Financial	
T17 Changing system privileges to either enable or deny access to information or functionality	2	2	3	1	The residual risk at go-live date will remain as the identified JunOS vulnerability will be get rid of (it is foreseen by end 2015). **After the upgrade of JunOS on all the impacted network devices, the likelihood will be decreased to value 1 ('Rare')**

Table: T2S residual risk.

The residual risk (T17) needs to be accepted temporarily until all network equipment gets rid of the vulnerability.

3. Performance

3.1. Summary

Four performance test scenarios have been prepared and executed: Night Time Settlement (NTS), Day Time for A2A (RTS), Day Time for U2A (U2A), End of Day (EoD).

***The Night Time Settlement** tests were conducted beyond the limits of the assumed peak; their results are presented below.*

***The Day Time A2A** tests were performed using two scenarios defined by the 4CB, under a number of conditions, awaiting the finalization of the volumetric figures by the ECB. The test results are presented in this document along with additional information about response time distribution for those U2A and A2A queries that are not fully in line with the expected results.*

***The Day time U2A** scenario was designed and executed successfully; this document contains the results of the test and additional information regarding response times for the queries that are not fully in line with the expectations.*

***The EoD** test scenario was designed and executed based on the latest news about the expected volume of security accounts. Performance indicators related to file transfer throughput and results from the report generation process have been provided in this document.*

3.2. Scenario 1: Night Time Settlement

The Night Time Settlement (NTS) scenario is based on a complete run of the first NTS cycle.

This test was conducted beyond the limits of the assumed peak volumes, with respect to the test description distributed to the ECB/market: in the executed test case 3,619,467 instructions were processed.

The volumes of each instruction type were slightly adapted in order to prepare a coherent test case; the following table provides further detailed information[12]:

12 In the document «T2S Non Functional Tests - Performance Test Case description», the extreme peak for NTS is represented by 3,409,680 instructions to be settled during the NTS.

	%	#	NTS1		NTS2	
			80%		20%	
SI volume for NTS		4,524,334		3,619,467		904,867
NTS	10.00%	452,433		361,946		90,487
DTS	90.00%	4,071,901		3,257,521		814,380
Corporate Actions	6.00%	271,460	7.50%	271,460		0
FOP	20.00%	904,867	25.00%	904,867		0
Other Transactions (mainly DVP)	74.00%	3,348,007	67.50%	2,421,424		926,583

Figure: Instructions distribution for NTS1 and NTS2 (peak scenario) per phase and per instruction type.

3.2.1. Test Conditions

The following hardware and software configuration of system/subsystems and application modules was used during the test execution:

- **Software version (Infrastructure)**

  z/OS V1R13

  IMS V13R1

  Websphere MQ V7R1

  WAS V8R5M5

  DB2 V10

  Websphere Message Broker V8

- **Software version (Application)**

  Software Iteration 14.0

- **Hardware configuration**

  Processor: IBM zEnterprise EC12 Model 718 (Type 2827 Model H89) 434 GB storage with 6 ICFs

  DASD: EMC VMAX 40K

- **Components involved**

  Middleware:

  IDM → Interface to the external networks

LCMM:

SIV → Instructions Validation

SIM → Instructions Matching

SMM → Management Module

SSM → Status Management

SIN → Instructions Maintenance

SETT:

SPS → Standardization and preparation to Settlement

NTS → Night time settlement

including :

- GRO → Gross Settlement
- MOM → Mathematical Optimization Module
- ACO → Auto Collateralization

INTF-A2A:

GIDINP → Input Management

GIDOUP → Output Management

GIDEVT → Event Management

SDMG - IST – Static Data Management :

IRP → Rules and Parameters Data Management Module

ISA → Securities Accounts Data Management Module

ICA → T2S Dedicated Cash Accounts Data Management Module

ISY → Securities Data Management Module

IPD → Party Data Management Module

3.2.2. Test Objective

The following table summarizes the test cases executed:

ID	Short description
Perf_04	Batch Settlement throughput

Below is the objective measured for the above test cases :

I. Batch Settlement throughput

- Test case identification

Test Case Perf_04 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.D)

- Test description

The objective of the test is to verify that Batch Settlement Throughput is compliant with the expected target value.

Batch Settlement Throughput is the ratio of the number of settlement instructions processed and the time that elapsed for processing them (i.e. between the start and end of the processing cycles). All instructions that are ready for settlement are considered, regardless of whether they have been settled or not.

The compliance of Perf_04 test case with the expected result will be checked during the execution of Scenario 1 – Night time.

- Expected Result

The Batch Settlement throughput is measured based on timestamps stored as part of the audit trail in the T2S database.

Rn=In/Tn

Where:

Rn = Batch Settlement Throughput

In = number of settlement instructions processed during night-time settlement

Tn = Total elapsed time, expressed in seconds, for the night-time settlement cycles

The expected result is that Batch Settlement Throughput is equal or greater than 80 instructions per second.

3.2.3. Test Data and Instructions

Please find below the characteristics and the composition of the data and instructions used during the test.

Static Data configuration:

Parties:

The scenario is based on 6 CSD and 6 NCB Euro and a total of 168 parties

- Each NCB has a party as NCB and a party as CSD participant in the CSD of its country
- Each CSD has a party as CSD and a party as CSD participant in each other CSD
- Each NCB has 10 Settlement banks
- Each CSD has 10 CSD Participants
- Each CSD Participant is the same legal entity as one Settlement bank

Securities:

- Each CSD is issuer of 40 securities
- Each CSD is investor in each other security directly with the issuer
- Each CSD declare every other CSD as its eligible counterpart for each CSD issuer

Auto-collateralisation:

- Each NCB provides Auto-Collateralisation following the REPO rule
- Each NCB chooses half of the securities issued by each CSD as eligible for auto-collateralisation
- Each NCB provides a price for the securities chosen

Cash accounts (66):

- 1 NCB cash account per NCB
- 1 cash account per Settlement Bank
- 1 External RTGS account per cash account
- 1 primary CMB per cash account
- Each CMB is configured for REPO auto-collateralisation except the one of the NCB cash account

Securities accounts (138):

- Each CSD has an issuance account
- Each CSD has a mirror account per other CSD (5)
- Each CSD has an omnibus account opened in its books by each other CSD (5)
- Each CSD has 2 securities accounts owned by the corresponding NCB for the auto-collateralisation
- Each CSD Participant has a securities account
- Each CSD defines a CSD account link with every other CSD (5 links per CSD)
- Each securities account is linked to a cash account through a primary CMB

Input data:

Settlement Instructions (TRAD):

1 222 105 prematched messages + 1 951 624 unmatched messages = 3 173 729 messages

Settlement Instructions (CORP):

32 464 prematched messages + 542 134 unmatched messages = 574 658 messages

Liquidity Transfer (Immediate):

60 messages, one to initialize each cash account

Name	%	Number or Instructions
SI volume (TRAD)		4 395 834
Prematched	55%	2 444 210
Unmatched	45%	1 951 624
SI volume (CORP)		607 062
Prematched	10%	64 928
Unmatched	90%	542 134

Figure: Settlement Instructions processed during Night Time

It has to be highlighted that the actual scenario used for the tests includes a number of instructions beyond the peak for a total amount of 4,395,834 (vs. 3,525,056 meaning +25% vs original scenario).

		NTS1
SI volume for NTS		4,395,834
Corporate Actions	13.81%	607,062
FOP	20.00%	879,167
Other Transactions (mainly DVP)	66.19%	2,909,605

Figure: Instructions distribution for NTS1 (actual test scenario)

3.2.4. Test Execution

- **Test Schedule**

The test contained in this report was executed on April 15th; a "cycle 1" of NTS, including sequences 0 to 4, was performed.

The effective duration of the test was around 4 hours.

Additional details about the test sequences duration are reported below.

- **Test execution detailed information**

The real number of Business Transactions processed in the test is described below and includes the T2SgSI (realignment and auto-collateralisation transactions).

NFT 2014-04-15 - NTS Cycle 1 , BD= 20150625 - Business results				
CURRENCY	**Category**	**STATUS**	**CREATED BY**	**Nb Transactions**
EUR	COLA	SETT	SETT	1 135
EUR	LQTR	SETT	LQMG	60
EUR	STND	SETT	LCMM	1 749 598
	REAL	SETT	LCMM	559 057
	STND	SETT	LCMM	557 623
EUR	STND	USET	LCMM	59 215
	REAL	USET	LCMM	53 618
	STND	USET	LCMM	34 290
			Total	**3 014 596**

Table: NTS Cycle 1 Business results

The throughput is expressed in business transactions per second, then multiplied by 2 to obtain throughput in Instructions/seconds.

Business description	Total BT processed	Total BT settled	Duration	Bath Settlement Throughput in BT/sec	Bath Settlement Throughput in Inx/sec
Seq 0 - Liquidity Transfer[13]	**60**	60	00:06:45	0.1	0.2
Seq 1 - Corporate action	**582 260**	582 260	00:37:29	258.9	517.8
Seq 2 - Free Of Payment	**-**	-	00:03:42	0	0
Seq 3 - Central Bank Operation	**-**	-	00:03:22	0	0
Seq 4 - all transactions	**2 432 276**	2 285 153	03:11:15	212	424
Total For Cycle 1	**3 014 596**	**2 867 473**	**04:02:33**	**207.1**	**414.2**

Table: Batch Settlement Throughput

[13] C1S0 duration depends upon a preparation phase executed (on time) as far as the transactions are available and ready for NTS, whatever the sequence they are related. During NFT tests most of the instructions were in the system before Cycle 1 sequence 0.

The Batch Settlement Throughput is **207.1 Business Transactions per second => 414.2 Instructions per second.**

More than 95% of the transactions were settled during the test.

3.2.5. Test Results - Test Case Objective achievement

I. Batch Settlement throughput

The test case objective was successfully achieved as the measured Batch Settlement throughput (around 414 instructions/sec) is by far greater than the objective (80).

Test Case	Scenario 1	NFT goal	Measured goal
Batch Settlement throughput	NTS	80 trx/sec	**414 trx/sec**

3.3. Scenario 2: Day Time for A2A

In 2013, the NFT performance test scenarios were designed on the basis of the ECB documentation available at that time[14]. In 2014, the volumetric assumptions were reviewed; the last version of the volumetric assumptions document was delivered by the ECB at the end of October 2014.

The Day Time for A2A scenario greatly differs from the Night Time Settlement scenario, as it was heavily affected by the evolution of the T2S volumetric assumptions; for this reason, the initial design of this test case was changed in order to fit in new information coming from the ECB and from the market. Despite these changes, it should be borne in mind that the Day Time for A2A test was executed with figures that are not yet final.

The Day Time A2A peak workload was redrafted using different kinds of messages representing different workloads (inbound settlement instructions, inbound maintenance instruction, inbound Static Data update instructions, A2A queries, real time settlement activities) without a full overlap of each single message type peak.

Composition and distribution of messages injected into the system represents a mix of different message types and settlement activities as described below:

- during day time, incoming settlement instructions with Intended Settlement Date (ISD) greater than the current business day (d+n) peak do not overlap with the settlement activities peak;
- hold/release instructions from the major CSDs will come close to DVP cut off, overlapping with the incoming peak but not with the settlement activities peak;
- static data updates can happen at any time during the day, most probably before the SOD; CSDs requested for flexibility in this context.

Following the above mentioned principles, two different scenarios (2.A and 2.B) were used for the Day Time for A2A tests:

14 "T2S PROCESSING VOLUME ANALYSIS V1" - (18/4/2013)
"Note on T2S Processing Volumes for the technical Sizing of the T2S Platform" (26/08/2013)

Scenario 2.A: settlement peak / low inbound activities

Day Time for A2A – Scenario 2.A - Instruction life cycle						
Name	**%**	**#**	**Message**	**#**	**Files** [15]	**#**
SI Day Time [standard] peak day		1,596,646				
SI pending from previous NTS cycle		55,868				
SI D+0 Peak hour during Day Time		83,112				
Prematched	53.45%	44,424	36%	16,116	64%	28,308
Unmatched	46.55%	38,688	36%	13,869	64%	24,819
SI D+n Peak hour during Day Time						
Prematched						
Unmatched						
Hold/Release of Settlement Instructions						
Amendment of SI	0.44%	6,953	100%	6,953		
Cancellation of SI	1.25%	20,000	100%	20,000		

Table: Day Time for A2A – Scenario 2.A - Instruction life cycle

Pending settlement instructions from previous NTS cycles have been taken into consideration in the design of this scenario as they increase the volume of instructions to be settled. Therefore the total amount of settlement instructions processed during the test is 138,980.

[15] It is required that the upper limit for the number of messages contained in one single file has to be equal to 4000.

Scenario 2.B: No settlement / high inbound activities

Day Time for A2A – Scenario 2.B - Instruction life cycle						
Name	**%**	**#**	**Message**	**#**	**Files**	**#**
SI Day Time [standard] peak day		1,596,646				
SI D+0 Peak hour during Day Time						
Prematched						
Unmatched						
SI D+n Peak hour during Day Time		130,510				
Prematched	55.52%	72,464	36%	26124	64%	46,340
Unmatched	44.47%	58,046	36%	41808	64%	37,142
Hold/Release of Settlement Instructions	9%	50,419	100%	50,419		
Amendment of SI	0.44%	6,953	100%	6,953		
Cancellation of SI	1.25%	20,000	100%	20,000		

Table: Day Time for A2A – Scenario 2.B - Instruction life cycle

Scenario 2.B was executed twice using two different SD configurations in order to collect Business Validation Time with and without massively MSAs/restriction rules (perf_01 and perf_14).

Since this scenario is also used to measure the expected results related to Static Data Processing, the workload of the SD component must be taken into account. According to the T2S Processing Volume Analysis document, the peak hour composition of SD maintenance instructions is the following:

A2A SD maintenance instructions/hour	55850
Party maintenance instructions	2000
T2S Dedicated Cash Account maintenance instructions	150
Securities maintenance instructions	25000
Security CSD Link instructions	28700

Table: A2A SD maintenance instructions per hour

During day-time we expect a peak volume of 10,000 A2A requests per hour. The request types shall be distributed as follow:

A2A Queries / hour		10,000
Securities settlement instruction queries	45.00%	4,500
Securities account position queries	20.00%	2,000
Cash related queries	25.00%	2,500
SD Queries	10.00%	1,000

Table: A2A Queries per hour

3.3.1. Test Conditions

The following hardware and software configuration of system/subsystems and application modules was used during the test:

- **Software version (Infrastructure)**

  z/OS V1R13

  IMS V13R1

  Websphere MQ V7R1

  WAS V8R5M5

  DB2 V10

  Websphere Message Broker V8

- **Software version (Application)**

  Software Iteration 14.0

- **Hardware configuration**

  Processor: IBM zEnterprise EC12 Model 718 (Type 2827 Model H89) 434 GB storage with 6 ICFs
  DASD: EMC VMAX 40K

- **Components involved**

  Middleware:

  IDM → Interface to the external networks

  LCMM:

  SIV → Instructions Validation

  SIM → Instructions Matching

  SMM → Management Module

  SSM → Status Management

  SIN → Instructions Maintenance

  SETT:

  SPS → Standardization and preparation to Settlement

  VPB → Validation provisioning and booking

  including :

  - CLP → Common Limit Provisioning

- BKG → Booking
- ACO → Auto Collateralization
- FMS → Failure Management and Settlement Outcome

R&O → Recycling and Optimization

INTF-A2A:

GIDINP → Input Management

GIDOUP → Output Management

GIDEVT → Event Management

SDMG - IST – Static Data Management :

IRP → Rules and Parameters Data Management Module

ISA → Securities Accounts Data Management Module

ICA → T2S Dedicated Cash Accounts Data Management Module

ISY → Securities Data Management Module

IPD → Party Data Management Module

3.3.2. Test Objective

The following table summarizes the test cases executed:

ID	Short description
Perf_01	Business Validation Time
Perf_02	Matching Time
Perf_03	Real-time Settlement Time
Perf_05	SD processing time
Perf_06	A2A query response time – Simple Queries
Perf_07	A2A query response time – Complex Queries
Perf_08	A2A message response time
Perf_14	Business Validation Time using massively MSAs/restriction rules

Below are the objectives for the test cases measured in the scenario:

I. Business Validation Time

- **Test case identification**

Test Case Perf_01 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.A)

- **Test description**

Business validation time is the time that elapses between the reception of an instruction by T2S and the end of the business validation process (i.e. creation of the related business objects in the T2S database or creation of the rejection message).

- **Expected Results**

The expected result is that the elapsed time between the timestamps created by the T2S system after successfully receiving the message and the timestamps stored as part of the audit trail in the T2S database is **within 3 minutes for 95% of iterations and within 9 minutes for 100% of iterations.**

II. Matching Time

- **Test case identification**

Test Case Perf_02 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.B)

- **Test description**

Matching time is the time that elapses between the end of a successful business validation and the end of the first matching attempt. The end of a matching attempt is marked by the successful creation of the matching object in the T2S database or the detection that there is not yet a matching instruction available.

- **Expected Results**

The expected result is that Matching Time is **within 2 minutes in 95% of iterations and within 5 minutes in 100% of iterations.**

III. Real-time Settlement Time

- **Test case identification**

Test Case Perf_03 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.C)

- **Test description**

Real-time Settlement Time is the time that elapses between the end of the creation of the matching object (i.e. after successful matching) and the end of the first settlement attempt. The end of the settlement attempt is marked by actual settlement or the detection of a business reason (e.g. lack of cash) that prevents settlement. This indicator is relevant only for Settlement Instructions sent on the Intended Settlement Date after the start of the real-time settlement phase of T2S.

- **Expected Results**

The expected result is that Real-time Settlement Time, measured based on timestamps stored as part of the audit trail in T2S, is **within 7 minutes in 95% of iterations and within 20 minutes in 100% of iterations**.

IV. SD processing time

- **Test case identification**

Test Case Perf_05 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.E)

- **Test description**

The static data processing time is the time that elapses between the end of a successful business validation and the end of the processing of this request. This indicator is relevant only for all types of static data maintenance instructions.

- **Expected Results**

The static data processing time is measured based on timestamps stored as part of the audit trail in the T2S database.[16]

It is expected that 95% of the static data updates are processed in 5 seconds, and 100% in 5 minutes.

V. A2A query response time – Simple Queries

- **Test case identification**

Test Case Perf_06 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.F)

- **Test description**

[16] In Batch Settlement mode certain types of static data maintenance requests might be queued to ensure the consistency of the settlement processing. In these cases the processing is considered complete after the creation of a new revision for the relevant entities even though this revision is only activated at a later point in time.

User Queries are processed in real time, based on the latest available data. The response to a User Query always contains the timestamp specifying the T2S system time when the data selection was actually performed.

- **Expected Results**

The expected result is that the A2A response time for simple Queries is **within 3 seconds in 95% of iterations and within 120 seconds in 100% of iterations.**

VI. A2A query response time – Complex Queries

- **Test case identification**

Test Case Perf_07 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.G)

- **Test description**

User Queries are processed in real time, based on the latest available data. The response to a User Query always contains the timestamp specifying the T2S system time when the data selection was actually performed.

- **Expected Results**

The expected result is that the A2A response time for complex Queries is **within 120 seconds in 95% of iterations and within 10 minutes in 100% of iterations.**

VII. A2A message response time

- **Test case identification**

Test Case Perf_08 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.H)

- **Test description**

The test is conducted by simulating the arrival to T2S, the production and the sending of instructions.

The traffic workload will be compliant with the test case scenario and will represent a realistic distribution of the instructions over the network connections and for DCP.

To simulate incoming traffic, the instructions will be inserted into messages and files that will be injected into the T2S ‘’incoming queues”.

The outgoing traffic will be automatically produced by the processing of incoming messages.

- **Expected Results**

The expected result is that the A2A response time for other messages is **within 5 seconds in 95% of iterations and within 120 seconds in 100% of iterations.**

VIII. Business Validation Time using massively MSAs/restriction rules

- **Test case identification**

Test Case Perf_14 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.N)

- **Test description**

The objective of the test is to verify that Business Validation Time is still compliant with the expected value when some CSDs reach the current limits of MSAs and restriction rules per CSDs.

- **Expected Results**

The expected result is that the elapsed time between the timestamps created by the T2S system after successfully receiving the message and the timestamps stored as part of the audit trail in the T2S database is **within 3 minutes for 95% of iterations and within 9 minutes for 100% of iterations**.

3.3.3. Test Data and Instructions

The characteristics and the composition of the data and instructions used in the test are described below.

Static Data configuration:

Parties:

The scenario is based on 6 CSD and 6 NCB Euro and a total of 168 parties

- Each NCB has a party as NCB and a party as CSD participant in the CSD of its country
- Each CSD has a party as CSD and a party as CSD participant in each other CSD
- Each NCB has 10 Settlement banks
- Each CSD has 10 CSD Participants
- Each CSD Participant is the same legal entity as one Settlement bank

Securities:

- Each CSD is issuer of 40 securities
- Each CSD is investor of each other security directly with the issuer
- Each CSD declare every other CSD as its eligible counterpart for each CSD issuer

Auto-collateralisation:

- Each NCB provides Auto-Collateralisation following the REPO rule
- Each NCB chooses half of the securities issued by each CSD as eligible for auto-collateralisation.
- Each NCB provides a price for the securities chosen.

Cash accounts (66):

- 1 NCB cash account per NCB
- 1 Cash account per Settlement Bank
- 1 External RTGS account per Cash account
- 1 primary CMB per cash account
- Each CMB is configured for REPO auto-collateralisation except the one of the NCB cash account.

Securities accounts (138):

- Each CSD has an issuance account
- Each CSD has a mirror account per other CSD (5)
- Each CSD has an omnibus account opened in its books by each other CSD (5)
- Each CSD has 2 securities accounts owned by the corresponding NCB for the auto-collateralisation
- Each CSD Participant has a Securities account
- Each CSD defines a CSD account Link with every other CSD (5 links per CSD)
- Each Securities account is linked to a cash account through a primary CMB

Additional Static Data configurations with MSAs/restriction rules (perf_14):

Usage of alphanumeric MSAs, with 3 different values. (Applicable on Parties, Securities Accounts and Securities).

At least 15% of the parameter values correspond to values of the MSAs contained in a rule.

Two types of MSA configurations were defined:

1. Complex MSA configuration:

- 2 CSDs have 10 different MSAs with a maximum of 5 MSAs within the same rule.

- 10 Specific Restriction Validation Rules have been created of type rejection and CSD Validation Hold, with positive and negative parameters for each of those 2 CSDs.
- Number of rules according to its type
  - 8 Rules of Rejection/CSD Validation Positive
  - 2 Rules of Rejection/CSD Validation Negative
- Number of rules according to its MSA configuration:
  - 1 Rule with massive usage of MSA (5MSAs within the rule)
  - 1 Rule with high usage of MSA (2 MSAs within the rule)
  - 8 Rules with standard usage of MSA (1 MSA within the rule)

2. Standard MSA configuration:

- 4 CSD have defined 3 different MSAs each.
- 6 Specific Restriction Validation Rules have been created of type rejection and CSD Validation Hold, with positive and negative parameters.
- Number of rules according to its type per CSD
  - 5 Rules of Rejection/CSD Validation Positive
  - 1 Rules of Rejection/CSD Validation Negative
- Number of rules according to its MSA configuration:
  - 6 Rules with standard usage of MSA (1 MSA within the rule)

Input data

Below is the distribution of XML objects (messages and files) used as input for the two test scenarios.

Scenario 2.A: settlement peak / low inbound activities

XML files/messages used as input data	Type	#
Amendment instructions	Single Message	6,953
Cancellation instructions	Single Message	20,000
SD update instructions	Single Message	54,987
Settlement Instruction	File	422
	Single Message	21,927

Table: XML files/messages used as input data in scenario 2.A

Scenario 2.B: no settlement / high inbound activities

XML files/messages used as input data	Type	#
Amendment instructions	Single Message	6,953
Hold instructions	Single Message	30,419
Release instructions	Single Message	20,000
SD update instructions	Single Message	54,987
Settlement Instruction	File	640
	Single Message	33,966

Table: XML files/messages used as input data in scenario 2.B

A2A queries

XML type	Query Type	#
semt.026	Securities settlement instruction query (Ins)	1,500
semt.026	Securities settlement instruction query (Sec)	1,500
semt.026	Securities settlement instruction query (SA)	1,500
semt.025	Securities settlement position query (SA)	2,000
camt.003	Cash related query (CASH)	1,250
camt.003	Cash related query (CASB)	1,250
acmt.025	SD Query (CASH)	500
reda.019	SD Query (SARD)	500

Table: A2A Query Types

3.3.4. Test Execution

- **Test Schedule**

The above described tests were executed on:

1) Scenario 2.A and 2.B: July 23rd (Perf_01, Perf_02, Perf_03 and Perf_05)
2) Scenario 2.B: October 13th (Perf_08)
3) Scenario 2.B with MSA/restriction rules: November 10th (Perf_14)
4) A2A queries: November 12th (Perf_06 and Perf_07)

Additional details about the timing of the tests are provided below.

- **Timeline Scenario 2.A – 23rd July:**

16:01:13 Scenario injection start
17:47:00 Latest outbound message put on VAN provider outbound queue

Total duration of the test 1h 47'

- **Timeline Scenario 2.B – 23rd July:**

10:30:00 Scenario injection start
12:12:00 Latest outbound message put on VAN provider outbound queue

Total duration of the test 1h 42'

- **Timeline Scenario 2.B – 13th October:**

This test used only single messages in order to assess A2A single message response time:

16:44:00 Scenario injection start
17:05:00 Latest outbound message put on VAN provider outbound queue

Total duration of the test 1h 1'

- **Timeline Scenario 2.B with MSA/restriction rules – 10th November:**

In order to check the A2A queries behaviour with single messages and files, this test has been divided into two steps:

- Single Message + A2A queries

12:28:34 Scenario injection start
13:36:00 Latest outbound message put on VAN provider outbound queue

Total duration of the test 1h 7'

- Files + A2A queries

14:38:20 Scenario injection start
14:38.25 Latest outbound message put on VAN provider outbound queue

Total duration of the test 1h 4'

- **Timeline A2A queries – 12th November:**

17:34:00 start injection A2A query messages
18:31:02 end injection A2A query messages
18:34:00 end of the test

Total duration of the test 1h

- **Test execution detailed information**

Scenario 2.A: settlement peak / low inbound activities

This test involved all backend modules: settlement due to RTS processes, matching and validation in order to process inbound instructions, middleware and interface modules for the inbound/outbound management and Static Data module to support real time processing and SD update instructions.

From a SETT module perspective the test started at 2014-07-23-16.01.26.163197 and ended at 2014-07-23-17.01.22.824120:

- Beginning of test with 27,934 Transactions unsettled in R&O stock coming from previous NTS execution
- End of test with 22,864 Transactions unsettled in R&O stock at the end of the test
- New transactions received on SETT module (in SPS):
    - 48,056 transactions were received in SETT
    - 8,196 transactions realignments were created
- No intraday restrictions
- 4,155 ACO templates valid for Auto-collateralization processed
- Transactions distributed on resources (cash/cmb/security positions)

	Number of distinct resources used
Cash balances debited	**65**
Cash balances credited	**65**
CMB debited	**65**
CMB credited	**65**
Security positions debited	**4,614**
Security positions credited	**3,605**

Table: Transactions distributed on resources

- Outbound messages produced: 799,716
- 54,987 Static Data maintenance instructions were processed by SDMG module
- Outbound files produced: 1,113

The number of settlement attempts is expressed in number of business transactions:

- including realignments

- including ACO transactions

- including reverse ACO settled but not reverse ACO not settled

- 81,637 collections processed
    - 39,245 created By SPS
    - 41,007 created by R&O-Recycling
    - 1,385 created by R&O-Optimization
- 133,722 settlement attempts leading to final results :
    - 45,408 Settled (including 490 ACO and 0 reverse ACO)
    - 2,743 Unsettled
- 490 transaction auto-collateralizations created to solve lack of cash

Scenario 2.B: no settlement / high inbound activities

Because the SETT module does not save the business transactions D+n into the Settlement backend, this test concerns mainly static data, matching and validation, interface and middleware modules.

The test results provided below show the LCMM and SETT activities recorded between 2014-07-23-10.31.50 and 2014-07-23-11.34.32:

- 130,502 Settlement instructions processed by LCMM as following:
    - 72,458 already matched
    - 58,044 unmatched of which:
        - 541 remained unmatched
        - 57,503 matched in the system
- 10,498 realignments validated and processed in LCMM
- 20,001 Maintenance Instructions not revealed due to error in the performance data collection phase;
- 54,987 Static Data maintenance instructions were processed by SDMG module;
- 57,371 Maintenance Instructions (amendment, hold and release) processed by LCMM;

- 5 Settlement instructions discarded due to digital signature technical error
- Total outbound messages produced: 1,202,509

In the MSAs/restriction (perf_14) test execution, about 57% of the incoming instructions (settlement instruction) either were rejected (28%) or were put on CSD Validation Hold in one of their legs (29%), due to the fulfilment of Restriction Type rules with MSAs.

Additional information for the A2A queries test execution

Below is the distribution of response time for A2A basic and complex queries:

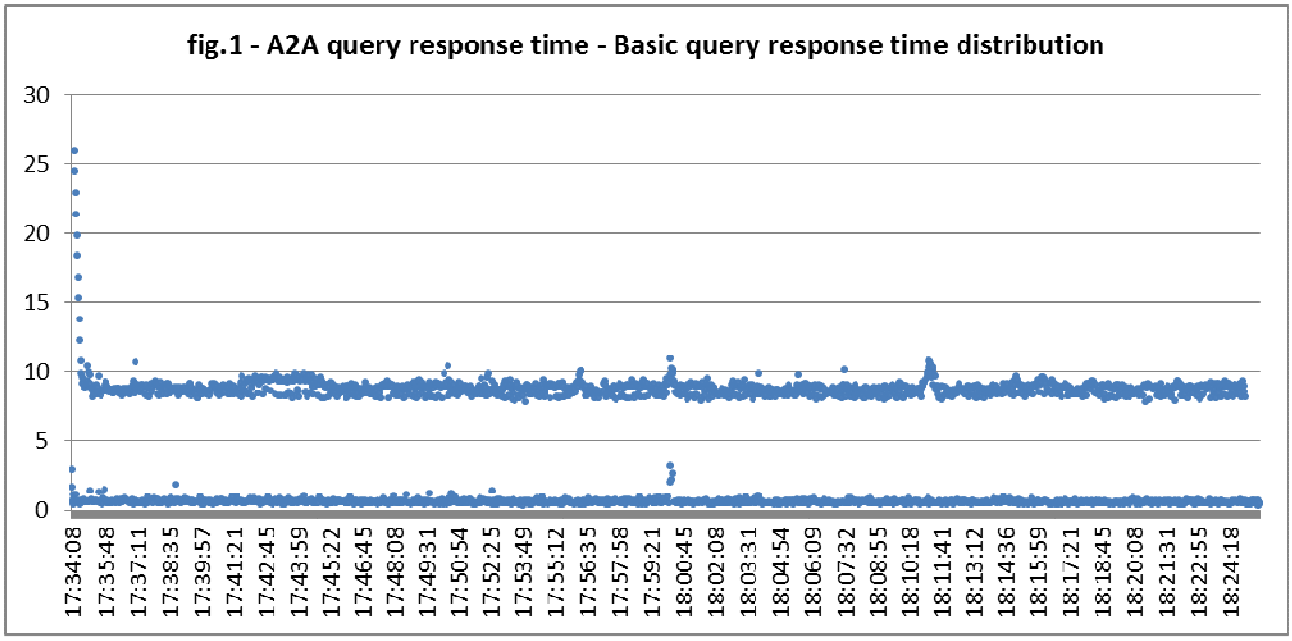

Figure: A2A query response time – Basic query response time distribution

The A2A simple query response time is 86% below 9" and almost all the rest is below 10" (99%).

3.3.5. Test Results - Test Case Objective achievement

I. Business Validation Time

The test case objective was achieved successfully in Scenario 2.A and 2.B:

Test Case	Scenario 2.A	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Business Validation Time	RTS	95% within 3 minutes	**99.9 %**	100% within 9 minutes	**100 %**

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Business Validation Time (BVT)	RTS	95% within 3 minutes	**100 %**	100% within 9 minutes	**100 %**

II. Matching Time

The test case objective was achieved successfully in Scenario 2.A and 2.B:

Test Case	Scenario 2.A	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Matching Time	RTS	95% within 2 minutes	**100 %**	100% within 5 minutes	**100 %**

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Matching Time	RTS	95% within 2 minutes	**100 %**	100% within 5 minutes	**100 %**

III. Real-time Settlement Time

The test case objective was achieved successfully in Scenario 2.B (not applicable in Scenario 2.A):

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Real-time Settlement Time	RTS	95% within 7 minutes	**100 %**	100% within 20 minutes	**100 %**

IV. SD processing time

The test case objective was achieved successfully in Scenario 2.A and 2.B:

Test Case	Scenario 2.A	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
SD processing time	RTS	95% within 5 seconds	**99.9 %**	100% within 5 minutes	**100 %**

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
SD processing time	RTS	95% within 5 seconds	**99.9 %**	100% within 5 minutes	**100 %**

V. A2A query response time – Simple Queries

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
A2A query response time – Simple Queries	RTS	95% within 3 seconds	**38 %**	100% within 120 seconds	**100 %**

VI. A2A query response time – Complex Queries

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
A2A query response time – Complex Queries	RTS	95% within 120 seconds	**100%**	100% within 10 minutes	**100 %**

VII. A2A message response time

The test case objective was achieved successfully:

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
A2A message response time	RTS	95% within 5 seconds	**98.8 %**	100% within 5 minutes	**100 %**

VIII. Business Validation Time using massively MSAs/restriction rules

The test case objective was achieved successfully in scenario 2.B - single messages and A2A queries:

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Business Validation Time using massively MSAs/restriction rules	RTS	95% within 3 minutes	**100 %**	100% within 9 minutes	**100 %**

The test case objective was partially achieved in scenario 2.B - files and A2A queries:

Test Case	Scenario 2.B	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
Business Validation Time using massively MSAs/restriction rules	RTS	95% within 3 minutes	**88.7 %**	100% within 9 minutes	**100 %**

Additionally, it can be reported that the number of occurrences showing Business validation time below 4 minutes was 98% and that the observed BVT was within 5 minutes in 100% of the occurrences.

3.4. Scenario 3: day time for U2A

The following high-level scenario description was agreed by the Non Functional Test workgroup; as per work item quantities derived from the volumetric assumptions provided by the ECB:

"

We expect 20.000 U2A queries per hour and 3.750 U2A updates. The different types of queries[17] and updates shall be distributed as follows:

U2A Queries/hour		*20,000*
Securities settlement instruction queries	*45%*	*9,000*
Securities account position queries	*20%*	*4,000*
Cash related queries	*25%*	*5,000*
SD queries	*10%*	*2,000*

Table: U2A Queries volume distribution.

"

This general volume structure and its four GFS query type groups were further broken down. For each query category both basic and complex queries were selected where feasible. All queries used in this scenario are listed in the table below and shown in the following chapter.

3.4.1. Test Conditions

The following hardware and software configuration of system/subsystems and application modules was used during the test.

- **Software version (Infrastructure)**

z/OS V1R13

IMS V13R1

[17] According to Framework Agreement – Schedule 6, "Simple queries and complex queries are those referenced as such within the User Detailed Functional Specifications (UDFS)".

Websphere MQ V7R1

WAS V8R5M5

DB2 V10

Websphere Message Broker V8

- **Software version (Application)**

Software Iteration 16.0

- **Hardware configuration**

Processor: IBM zEnterprise EC12 Model 718 (Type 2827 Model H89) 434 GB storage with 6 ICFs. DASD: EMC VMAX 40K

- **Components involved**

Middleware:

IDM → Interface to the external networks

INTF-U2A:

Communication Module U2A

Inbound Processing Module U2A

Outbound Processing Module U2A

SDMG - Static Data Management:

IRP → Rules and Parameters Data Management Module

SQRA - Statics-Reports-Queries and Archive

QM → Query Management

3.4.2. Test Objective

The following table summarizes the test cases executed:

ID	Short description
Perf_09	U2A response time – Simple Queries
Perf_10	U2A response time – Complex Queries
Perf_11	U2A response time – other request

I. U2A response time - Simple Queries

- **Test case identification**

Test Case Perf_09 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.I)

- **Test description**

The query response time is defined as the time elapsed between the reception of a query in the T2S system and the sending of the requested information.

- **Expected Results**

The expected result is that the U2A response time for simple Queries is **within 3 seconds in 95% of iterations and within 120 seconds in 100% of iterations.**

II. U2A response time - Complex Queries

- **Test case identification**

Test Case Perf_10 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.J)

- **Test description**

The query response time is defined as the time elapsed between the reception of a query in the T2S system and the sending of the requested information.

- **Expected Results**

The expected result is that the U2A response time for complex Queries is **within 120 seconds in 95% of iterations and within 10 minutes in 100% of iterations.**

III. U2A response time – other requests

- **Test case identification**

Test Case Perf_11 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.K)

- **Test description**

The test results will be stored and analysed to predict the platform behaviour beyond the contractual obligations.

- **Expected Results**

The expected result is that the U2A response time for other requests is **within 5 seconds in 95% of iterations and within 120 seconds in 100% of iterations.**

3.4.3. Test Data and Instructions

Please find below the characteristics and the composition of the data and instructions used during the test.

Static Data configuration:

Parties:

The scenario is based on 6 CSD and 6 Euro NCB and a total of 168 parties.

- Each NCB has a party as NCB and a party as CSD participant in the CSD of its country.
- Each CSD has a party as CSD and a party as CSD participant in each other CSD.
- Each NCB has 10 Settlement banks.
- Each CSD has 10 CSD Participants.
- Each CSD Participant is the same legal entity as one Settlement bank

Securities:

- Each CSD is issuer of 40 securities
- Each CSD is investor of each other security directly with the issuer
- Each CSD declare every other CSD as its eligible counterpart for each CSD issuer

Auto-collateralisation:

- Each NCB provides Auto-Collateralisation following the REPO rule
- Each NCB chooses half of the securities issued by each CSD as eligible for auto-collateralisation
- Each NCB provides a price for the securities chosen.

Cash accounts (66):

- 1 NCB cash account per NCB
- 1 Cash account per Settlement Bank
- 1 External RTGS account per Cash account
- 1 primary CMB per cash account

- Each CMB is configured for REPO auto-collateralisation except the one of the NCB cash account.

Securities accounts (138):

- Each CSD has an issuance account
- Each CSD has a mirror account per other CSD (5)
- Each CSD has an omnibus account opened in its books by each other CSD (5)
- Each CSD has 2 securities accounts owned by the corresponding NCB for the auto-collateralisation
- Each CSD Participant has a Securities account
- Each CSD defines a CSD account Link with every other CSD (5 links per CSD)
- Each Securities account is linked to a cash account through a primary CMB

Input data:

The U2A test scenario was executed based on the data resulting from the execution of the Night Time Settlement and Day Time Settlement scenarios.

The general volume structure and the different query and update type groups were further broken down; all queries and updates used are listed in the following section.

3.4.3.1. Securities settlement instruction queries

The following representative query type has been selected for this group securities settlement instruction queries:

Query Type	***U2A Screen***	***Basic***	***Complex***
Settlement Instruction Query	Securities ->Settlement -> Settlement Instructions		x

3.4.3.2. Securities account positions queries

The following representative query types have been selected for this group:

Query Type	***U2A Screen***	***Basic***	***Complex***
Securities Account Position Query	Securities -> Securities Account -> Securities Positions	x	
Securities Posting Query (U2A only)	Securities -> Securities Account -> Securities Postings		x

3.4.3.3. Cash related queries

The following representative query types have been selected for this group:

Query Type	*U2A Screen*	*Basic*	*Complex*
T2S Dedicated Cash Account Balance Query	Cash -> Cash Account -> Cash Account Balances	x	
T2S Dedicated Cash Account Posting Query	Cash-Cash Account-Cash Account Postings		x
Total collateral value per T2S Dedicated Cash Account query	Cash -> Cash Account -> Total Collateral Values per T2S Dedicated Cash Account		x
Collateral value of a security query	Cash -> Cash Account -> Collateral Value of a Security	x	
Collateral value per T2S Dedicated Cash Account query	Cash -> Cash Account -> Collateral Values per T2S Dedicated Cash Account		x
Outstanding Auto Collateralisation Credit Query	Cash -> Liquidity -> Outstanding Auto-collateralisation	x	

3.4.3.4. Static Data and other queries

The following representative query types have been selected for this group:

Query Type	*U2A Screen*	*Basic*	*Complex*
Party List Query	Static Data ->Parties -> Parties	x	
Eligible Counterpart CSD List Query (U2A only)	Static Data -> Parties -> Eligible Counterpart CSDs	x	
Securities CSD Link Query	Static Data -> Securities -> CSD Links		x
ISIN List Query	Static Data -> Securities -> Securities		x
CSD Account Link Query (U2A only)	Static Data -> Securities Account -> CSD Account Links	x	
CMB Securities Account Links List Query (U2A only)	Static Data -> Securities Accounts -> Accounts Links	x	
Securities Account List Query	Static Data -> Securities Account -> Securities Accounts		x
T2S Dedicated Cash Account List Query	Static Data -> T2S Dedicated Cash Account -> Dedicated Cash Accounts	x	
Limit Query	Static Data -> T2S Dedicated Cash Account -> Limit		x
T2S System User Query (T2S Actor Query) (U2A only)	Static Data -> Access Rights -> Users	x	
Current Status of the T2S settlement day (U2A only)	Service -> Additional Services -> Settlement Day	x	
Report List Query (U2A only)	Service -> Additional Services -> Reports	x	

The Real Time Settlement – U2A queries were recorded and parameterized by using the program "WebLOAD IDE". WebLOAD is a testing tool for load and performance testing of applications and can be used for recording, editing and debugging sessions, which are recorded as Java scripts. Furthermore an automatic correlation of dynamic values (e.g. session ids) was performed. Finally, the scripts were parameterized using

text files containing distinct search criteria separated by commas. These measurements ensure that the scripts can be replayed reliably.

The breakdown for the four categorized query categories as well as the Static Data updates which have been recorded, scripted, correlated and parameterized is shown in detail in the following chapter. By executing the recorded scripts and related parameterizations, the various screens are called under the corresponding user's login and search criteria.

Due to the absence of a granular level prediction of future U2A usage patterns, an arithmetic approach to weighting the queries in the 4 respective query categories was selected. The breakdown is calculated as follows:

Weight breakdown per query type used in the WebLOAD mix (per thousand):	
Queries:	***Weight:***
Securities settlement instruction queries	450
Settlement Instruction Query	*450*
Securities account position queries	200
Securities Account Position Query	*100*
Securities Posting Query	*100*
Cash related queries	250
T2S Dedicated Cash Account Balance Query	*42*
Collateral value of a security query	*42*
Outstanding Auto Collateralisation Credit Query	*42*
T2S Dedicated Cash Account Posting Query	*42*
Total collateral value per T2S Dedicated Cash Account query	*42*
Collateral value per T2S Dedicated Cash Account query	*41*
SD and other queries	100
Party List Query	*9*
Eligible Counterpart CSD List Query (U2A only)	*9*
CSD Account Link Query (U2A only)	*9*
CMB Securities Account Links List Query (U2A only)	*8*
T2S Dedicated Cash Account List Query	*8*
T2S System User Query (T2S Actor Query) (U2A only)	*9*
Securities CSD Link Query	*8*
ISIN List Query	*8*
Securities Account List Query	*8*
Limit Query	*8*
Current Status of the T2S settlement day (U2A only)	*8*
Report List Query (U2A only)	*8*

Table: Input Data - Weight breakdown per query type used in the WebLOAD mix

Depending on the associated query structure, the queries either are invoked exclusively by CSD or NCB users or a mix of NCB and CSD users. Each U2A query is executed by six different users with their appropriate search parameters. Due to technical reasons, the technical identifier of the party has to be

added as a parameter to each line of the parameterization file. The different tables for the breakdown of the queries show the category of the query - basic or complex, the query type, which user is involved and the associated search criteria to use the query.

3.4.4. Test Execution

- **Test Schedule**

The above described test was executed on October 10th 2014 from 1:40 P.M. to 2:40 P.M.

The effective duration of the test was around 1 hour.

Additional details about the test execution and duration are provided below.

- **Test execution detailed information**

For the test execution a socalled WebLOAD "template" was created using the WebLOAD Console software. The template contains a WebLOAD "mix" and a schedule. The mix is composed of the different scripts for the queries and SD updates.

Due to an outstanding issue related to the Settlement instruction query and the Securities Account Position Query, it was not possible to include these queries in the WebLOAD mix.

The resulting composition of the executed WebLOAD mix is the following:

Weight breakdown per query type used in the WebLOAD mix :	
Queries:	***Weight:***
Securities account position queries	200
Securities Posting Query	*200*
Cash related queries	250
T2S Dedicated Cash Account Balance Query	*42*
Collateral value of a security query	*42*
Outstanding Auto Collateralisation Credit Query	*42*
T2S Dedicated Cash Account Posting Query	*42*
Total collateral value per T2S Dedicated Cash Account query	*42*
Collateral value per T2S Dedicated Cash Account query	*41*
SD and other queries	100
Party List Query	*9*
Eligible Counterpart CSD List Query (U2A only)	*9*
CSD Account Link Query (U2A only)	*9*
CMB Securities Account Links List Query (U2A only)	*8*
T2S Dedicated Cash Account List Query	*8*
T2S System User Query (T2S Actor Query) (U2A only)	*9*
Securities CSD Link Query	*8*
ISIN List Query	*8*

Securities Account List Query	*8*
Limit Query	*8*
Current Status of the T2S settlement day (U2A only)	*8*
Report List Query (U2A only)	*8*

Table: Test Execution - Weight breakdown per query type used in the WebLOAD mix

During the test execution, 23,753 queries and 671 updates were successfully executed within 1 hour.

Additional information for the U2A queries test execution

The chart below shows the response time distribution for U2A basic and complex queries:

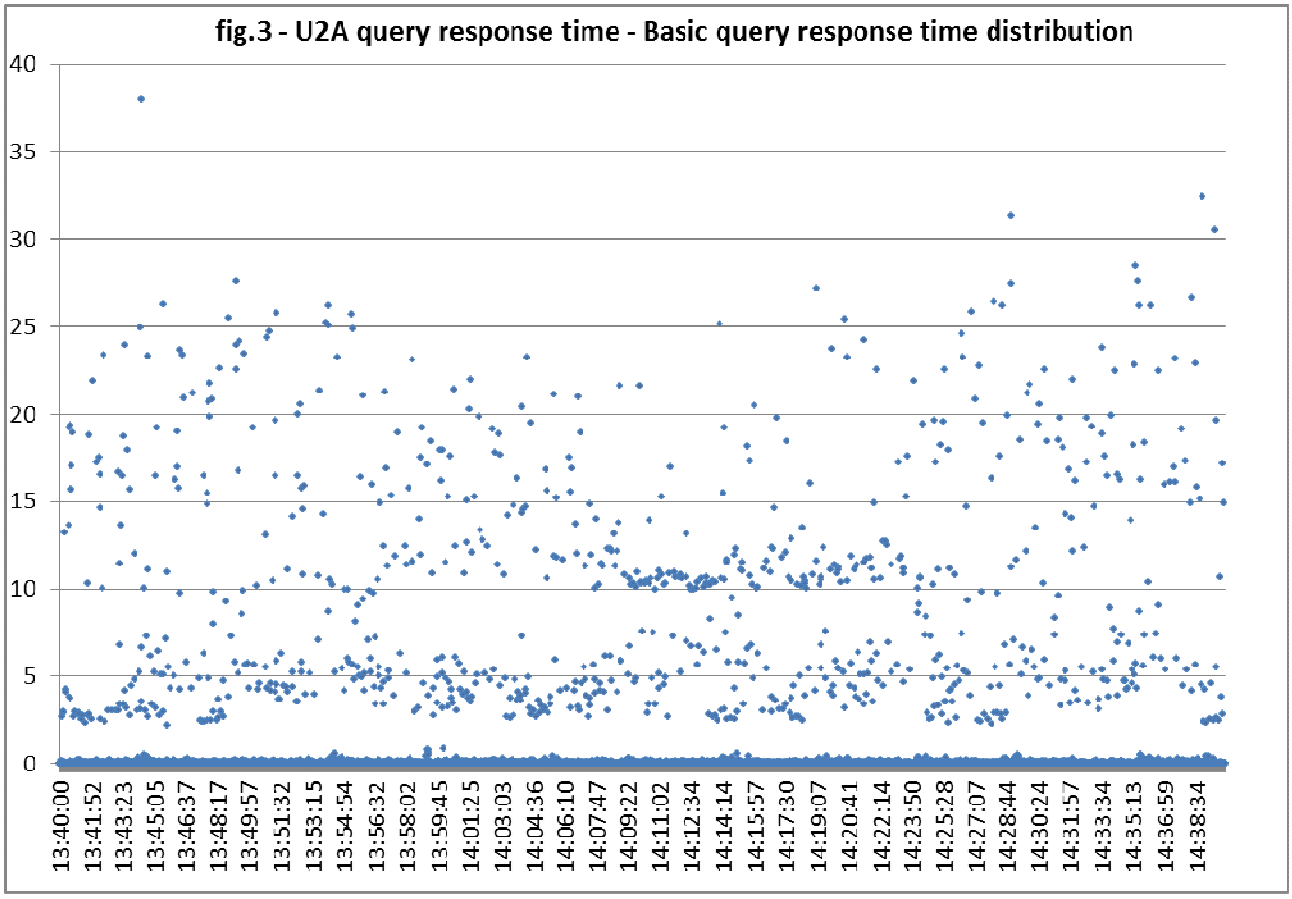

Figure: U2A query response time – Basic query response time distribution

U2A simple query response time is 96% below 7" and 99% below 19".

3.4.5. Test Results - Test Case Objective Achievement

I. U2A response time - Simple Queries

The test case objective was partially achieved:

Test Case	Scenario 3	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
U2A response time - Simple Queries	U2A	95% within 3 seconds	**93 %**	100% within 120 seconds	**100 %**

II. U2A response time - Complex Queries

The test case objective was successfully achieved:

Test Case	Scenario 3	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
II.U2A response time - Complex Queries	U2A	95% within 120 seconds	**100 %**	100% within 10 minutes	**100 %**

III. U2A response time – other requests

The test case objective was successfully achieved:

Test Case	Scenario 3	NFT 1st goal	Measured 1st goal	NFT 2nd goal	Measured 2nd goal
U2A response time – other requests	U2A	95% within 3 seconds	**100 %**	100% within 120 seconds	**100 %**

3.5. SCENARIO 4: End Of Day

The EoD is the phase after the real time settlement.

During the EoD several processes are performed, involving different actors:

- EoD Processing
    - This process involves CBs and payment banks providing static data collateral information as Securities Valuations and Eligible Securities records
- EoD Reporting
    - This process involves every actor for which an EoD report has been configured

3.5.1. Test Conditions

The following hardware and software configuration of system/subsystems and application modules was used during the test.

- **Software version (Infrastructure)**

  z/OS V1R13

  IMS V13R1

  Websphere MQ V7R1

  WAS V8R5M5

  DB2 V10

  Websphere Message Broker V8

- **Software version (Application)**

  Software Iteration 16.0

- **Hardware configuration**

  Processor: IBM zEnterprise EC12 Model 718 (Type 2827 Model H89) 434 GB storage with 6 ICFs. DASD: EMC VMAX 40K

- **Components involved**

  Middleware:

  IDM → Interface to the external networks

  INTF-A2A:

  GIDOUP → Output Management

  GIDEVT → Event Management

  GIDREM → Input Management

  SDMG - IST – Static Data Management :

IRP → Rules and Parameters Data Management Module

3.5.2. Test Objective

The following table summarizes the test cases performed:

ID	Short description
Perf_12	File Transfer Throughput: input
Perf_13	Throughput: output

I. File Transfer Throughput: input

- **Test case identification**

Test Case Perf_12 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.L)

- **Test description**

Verify that File transfer Throughput in Input is 4 gigabytes per hour.

The test is performed by simulating the reception of files in T2S. Files for an amount of 4 GB will be prepared and injected into T2S.

- **Expected Results**

T2S is able to receive 4 Gigabytes of files in one hour

II. Throughput: output

- **Test case identification**

Test Case Perf_13 (T2S Non Functional Tests - Performance Test Case description V 1.9 – Section III.M)

- **Test description**

The test is performed by sending files from T2S. Files for an amount of 4 GB will be prepared and sent by T2S. The production of files will be managed automatically by the application, simulating the End-of-Day procedure. Files are then sent by T2S and the sending capacity at network level is measured.

- **Expected Results**

T2S is able to send 4 Gigabytes of files in one hour.

According to the latest volumetric assumptions working document and considering the expected behaviour of the participants, 3 reports are expected to be produced at the end of a business day:

- Pending settlement instructions
- Settled settlement instructions
- Statement of holdings in delta mode

From a volume point of view, assuming that the exceptional peak for 2017 is the target, the expectations in terms of reported business items would be to have:

Report	*Business items*
Pending settlement instructions	7,119,680
Settled settlement instructions	4,616,667
Statement of holdings - delta report	400,000

Table: Number of reported business items

The main differences compared to the T2S_Non_Functional_Test_cas_Performance v1_9 document are:

- Different business item figures for all of the reports
- New Settled Settlement Instructions report
- New delta report for Statement of holdings
- Statement of securities dropped as the monthly reconciliation is performed by querying the system

3.5.3. Test Data and Instructions

Static Data Configuration

The scenario is based on 6 CSD and 6 NCB for which report configuration have been set-up.

All of the Report Configurations are:

- Full mode
- System Entity wide

For the CSDs, the following Report Configuration has been set-up :

- Statement of Holdings
- Statement of Transactions
- Statement of Pending Instructions

Input Data :

In order to align the test scenario with the latest volumetric assumptions, especially regarding the number of security accounts defined in T2S, 40,000 security accounts have been created and 10,000 of them have been changed using 50,000 FOP instructions.

The input data for EoD reporting is represented by NTS scenario settlement activities.

In order to test inbound file transfer throughput, 60 files containing about 180,000 settlement instructions were used to perform a complete test (including also inbound processing operations) with a reduced amount of data (about 430MB); the final throughput has been derived to test measurement.

3.5.4. Test Execution

- **Test Schedule**

The inbound file processing complete test was successfully performed on 9th October.
The EoD report generation test was successfully performed on 16th October.

- **Test execution detailed information**

The input file transfer test was executed on 18th September with about 400MB of data injected in 6 minutes.

The EoD report generation test was successfully executed on 16th October: the test started at 11.35 A.M. and ended at 12.37 A.M.

18th September test: 449,095,744 Bytes contained in 60 files were received in 5’ 33” (4,52GB per hour).

16th October EoD session produced:

- 122.139 Messages
- 10.463.986 Business Objects
- Reports generated:
    - Statement of Holding
    - Statement of Pending Instruction
    - Statement of Transaction

- 4.189.328.863 Bytes produced and sent in 27’ 37’’ (8,47GB per hour)

3.5.5. Test Results - Test Case Objective achievement

I. File Transfer Throughput: input

The test case objective was successfully achieved:

Test Case	Scenario 4	NFT goal	Measured goal
File Transfer Throughput: input	EoD	4GB per hour	**100 %**

II. File Transfer Throughput: output

The test case objective was successfully achieved:

Test Case	Scenario 4	NFT goal	Measured goal
File Transfer Throughput: output	EoD	4GB per hour	**100 %**