

Report of the 2009 TSL Remote Interoperability Event



Reference

DIGIT/R2/PN/2009/089 Plugtests Services

Keywords

TSL

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex -
FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93
65 47 16

Siret N°348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N°7803/88

Report of the 2009 TSL Interoperability Remote Event

March 2010

This version:

Author:

Andrea Caccia, UNINFO

Juan Carlos Cruellas, UPC

Konrad Lanz, A-SIT

Daniele, Mongiello, InfoCert

Laurent Velez, ETSI

Editor:

Laurent Velez, ETSI <laurent.velez@etsi.org>

Abstract

This document is the report of the TSL Interoperability Remote Event organized by ETSI within the Framework of European Commission project DIGIT/R2/PN/2009/089 and conducted using the ETSI portal supporting remote interoperability Plugtests™.

For further details on ETSI Plugtests, please see
<http://www.etsi.org/Website/OurServices/Plugtests/home.aspx>

Status of this Document

This document is provided by [ETSI Interopolis](#) Services. For further details on Plugtests services, please see [ETSI Plugtests](#).

Contents

1	INTRODUCTION	5
2	ORGANIZATION AND CONTENTS OF THE PORTAL	6
2.1	PUBLIC PART OF THE PORTAL	6
2.2.1	<i>Contents of Common area of Private part</i>	<i>7</i>
2.2.1.0	Cryptographic material pages.....	7
2.2.1.2	Online PKI-related services page	8
2.2.1.3	Online PKI services access page.....	8
2.2.1.4	Online TSA services access page	8
2.2.1.5	Attribute certificate issuance page	8
2.2.1.6	TSL Tools	8
2.2.1.7	Participants' List page.....	9
2.2.1.8	Meeting Support page	9
2.2.1.9	Face 2 Face Meeting page	9
2.2.1.00	Presentations pages.....	9
2.2.1.01	Mailing list archive.....	10
2.2.1.02	Chat page	10
2.2.1.03	Site map page	10
2.2.2	<i>Contents of TSL Life Cycle areas of Private part</i>	<i>11</i>
2.2.2.1	Conducting Life Cycle Tests.....	11
2.2.2.2	Test Cases pages	11
2.2.2.3	TSL contents for the TSL lifecycle test cases	12
2.2.2.4	TSL Testcase Definition Language.....	12
2.2.2.5	TSL Life Cycle Checks	12
2.2.2.6	Individual verification reports.....	13
2.2.2.7	Statistics per form	15
2.2.2.8	Upload Life Cycle TSL pages	15
2.2.2.10	Known issues pages.....	16
2.2.2.11	Questions and answers pages.....	16
2.2.3	<i>Contents of TSL Plugtests area of Private part</i>	<i>17</i>
2.2.3.1	Conducting Plugtests.....	17
2.2.3.1.0	Conducting Plugtests: Starting Plugtests	17
2.2.3.1.2	Conducting Plugtests: Generating XAdES Signatures.....	18
2.2.3.1.3	Conducting Plugtests: Verifying XAdES Signatures.....	18
2.2.3.2	Check Certificates page.....	18
2.2.3.3	Conformance Checker page	18
2.2.3.4	Test Cases pages	19
2.2.3.5	Individual verification reports.....	20
2.2.3.6	Testcase Results Overview.....	20
2.2.3.7	Statistics per form	20
2.2.3.8	Upload pages.....	21
2.2.3.9	Download pages.....	21
2.2.3.10	Test data directory pages	21
2.2.3.11	Questions and answers pages.....	21
3.	PARTICIPATION.....	22
3.1	TSL INTEROP TEAM	22
3.2	PARTICIPANTS LIST	22
3.3	WEB CONFERENCE MEETINGS	25
3.4	FACE TO FACE MEETING	27
4.	INTEROPERABILITY EVENT CONCLUSIONS.....	29
4.1	GENERAL CONCLUSIONS	29
4.2	CONTRIBUTIONS TO STANDARDISATION.....	29
4.3	BENEFIT FOR MEMBER STATES AND EUROPEAN COMMISSION	30
A.	ANNEX: LIST OF WORK PACKAGE DELIVERABLES	31

1 Introduction

The present document aims at reporting the 2009 TSL Interoperability Remote Event. It is the Final Report defined in to the Work Package 6 of the DIGIT/R2/PN/2009/089 project – Plugtests Services.

The goal of this Interoperability remote event was :

- ❑ To enable participants to assess the level of support to TSL life cycle of the tools used in the EU Member States for generating TSLs providing information on CSPs issuing Qualified Certificates.
- ❑ To enable participants to assess the level of interoperability of signature tools TSL-enabled, i.e., tools able to incorporate TSL checks of the status of the CSPs issuing QCs during the validation of electronic signatures coming from both, the same and different EU Member States.
- ❑ To identify additional issues that may hinder a quick deployment of the European TSL framework for supporting cross-border recognition of electronic signatures among the EU Member states, and by doing this, to ease the deployment of such an infrastructure.

The main objective of the Tests was twofold and could be split into the following two interrelated Plans:

- ❑ TSL Lifecycle Management Tests (19 Oct 2009 – 2nd Nov 2009):
- ❑ TSL Interoperability Tests (2nd Nov – 28 Dec 2009)

The present document is organized as indicated below:

Section 2 provides details on how the material of the portal is organized and the kind of services it provides to the participants of the Interoperability Events.

Section 3 lists the participants to the Event, including a description of the Face 2 Face meeting that has been held in ETSI premises from 23 to 26 Nov 2009.

Section 4 provides an overview of the most interesting results and conclusions of the interoperability event..

Finally in Annex, there are the list of the deliverables that are provided to the European Commission as defined in the document “Plugtest Service” DIGIT/R2/PN/2009/089 Annex II – List of Services covered by the Contract and Schedule of price.

2 Organization and contents of the portal

The portal has two different parts, namely one public part, that anybody may visit, and a private part accessible only for the participants subscribed to the plugtest event.

2.1 Public part of the portal

This part is accessible to everybody, at the url <http://xades-portal.etsi.org>

It contains the following public information and a link to login to the private part of the portal.

- The XAdES/CAAdES Plugtest page, providing some more details on the past events (targetted specification, targetted audience, etc...)
- TSL Interop: presentation of the event and overview of the 2 Test Phases : Life Cycle and Plugtests.
- The Mailing List page, providing some details on participants' mailing list support provided by the portal for facilitating exchange of information during the plugtest.
- The Registration page, providing details on the plugtest registration process.
- Face 2 Face meeting : Presentation of the meeting (23-26 Nov 2009) and link for registration.
- The Login to Interop event Area page, access to the protected area of the portal.
- Presentation of the TSL Interop team

2.2 Private part of the portal

This part is visible only for the participants of the interoperability event. It is structured in three main areas:

- **Common area.** This area contains a number of pages that provide generic information to the participants, which is relevant to participants of both XAdES and CAdES interoperability tests.
- **Life Cycle specific area.** This area contains a number of pages that support the Life Cycle (Conformance) tests on TSL.
- **Plugtests specific area.** This area contains a number of pages that support the interoperability tests (Plugtests) on TSL.

Sub-clauses below provide details of the contents of these pages.

2.2.1 Contents of Common area of Private part

2.2.1.0 Cryptographic material pages

The Cryptographic Material page is the first one of a set of pages providing details on the cryptographic material handed to the participants at the beginning of the plugtest.

The portal deployed a **Trust Framework** consisting in a certification hierarchy of three levels with a root CA and two subsidiary CAs in **two levels**.

Each CA also provided **OCSP** responses reporting the status of the certificates issued by that CA. In addition to that, each CA issued **CRLs** reporting the revoked certificates.

The portal also includes a **Timestamping Authority** able to generate time-stamp tokens on request by the participants.

It must be mentioned that the portal did not include an Attribute Authority able to generate Attribute Certificates, required for certain test-cases in both XAdES and CAdES. ENTRUST Japan Co., Ltd., was so kind as to generate **attribute certificates** for those participants that requested them.

The Scenario SCOK page provides details of the first scenario supported by the portal for the Trust Framework aforementioned, namely, a scenario where all the certificates are valid.

The Scenario SC1 page provides details of the second scenario supported by the portal for the Trust Framework aforementioned, namely, a scenario where a revoked end-entity certificate and an expired end-entity certificate exist for being used in some of the **only-verification test cases**.

2.2.1.2 Online PKI-related services page

The current version of the plugtest portal incorporates a number of online PKI-related services.

The **Online PKI services details page** describe all of them and provides details on how the participants may access them.

This page also contains a link to a Java class implementing basic login/password authentication mechanism required for accessing these services, so that participants had not to develop such a mechanisms in their tools.

2.2.1.3 Online PKI services access page

The Online PKI Services access page allows to access to most of the on-line PKI-related services provided by the portal, namely: access to the CA software for requesting generation of a key-pair and the corresponding end-entity certificate for generating signatures, connection details for accessing the LDAP server where CRLs and CA certificates are stored, etc.

2.2.1.4 Online TSA services access page

The Online TSP Services access page allows to access to the TSA server deployed in the server for requesting generation of time-stamp tokens.

2.2.1.5 Attribute certificate issuance page

At present, the Remote Plugtest© Portal does not incorporate an Attribute Authority module. As it has been already reported, ENTRUST Japan Co., Ltd. very kindly offered its resources for generating attribute certificates to those participants interested in those XAdES and CAdES test cases dealing with attribute certificates.

The attribute certificate issuance page provides details on:

- The trust Framework completed with the Attribute Authority at ENTRUST Japan Co., Ltd.'s headquarters in Japan that issued attribute certificates for this Plugtest©.
- The procedures to be followed by participants for requesting to ENTRUST Japan Co., Ltd. the issuance of an attribute certificate.

2.2.1.6 TSL Tools

In this page, it can find a link to download TSL tools :

TSL Edit from project OSOR :

<http://forge.osor.eu/projects/tsledit/>

Note: Just keep present that the tool has been released at the end of July, when the first draft of the TSLv3 was still not published. The tool may have some issues but it can anyway be useful to build a "skeleton" of the TSL, keeping in mind that the output will have to be reviewed "by hand" in some parts.

2.2.1.7 Participants' List page

This page lists the details of all the companies/organisations and people that participated in the interop event as well as their coordinates. Each participant represents an European Member State.

2.2.1.8 Meeting Support page

The Meeting Support page contains all the information related to the meetings that took place during the plugtest event. It includes:

- Introduction presentation. This presentation was made available before the start of the plugtest, and it provides the most relevant information on the event, including structure of the portal, relevant URLs, rules to be followed during the participation, etc
- Calendar for the meetings (conference calls).
- Dialing details for the "GotoMeeting" web conference and phone bridge.
- URL for accessing a chat server accessible through a Web browser where the calls were minuted and participants could write their comments, questions and statements.
- The agenda for each meeting.
- Links to the minutes of each meeting..

2.2.1.9 Face 2 Face Meeting page

The F2F Meeting page contains all the information related to the meeting hosted by ETSI from 23rd to 26th November 2009, in Sophia-Antipolis , France.

This includes a presentation of the meeting, the link to register, the agenda and also some logistics information (access to ETSI premises, airport info, hotels details, etc...)

2.2.1.00 Presentations pages

The Presentations page is the first of a set of pages containing presentations. At present, there are two presentations available:

- A presentation on the ETSI ESI TC , the body in charge of standardizing XAdES.
- A presentation on the history of XAdES , which includes details on the different published versions.

2.2.1.01 Mailing list archive

A Electronic mail list with archival capabilities, whose use was restricted to the participants in the Plugtest©, was set up for supporting exchange of messages among them.

2.2.1.02 Chat page

The Chat page provides access to a web-based chat that participants use during the conference calls for sharing notes. It is also used for taking notes of the meetings. These notes are the core component of the meetings minutes.

2.2.1.03 Site map page

This page displays the current hierarchical structure of the Plugtest© Portal, and provides links for all the pages shown in the map.

2.2.2 Contents of TSL Life Cycle areas of Private part

The portal contains, within the private part of the portal, a specific area for Life Cycle Testing (Conformance) that is tested in this Interoperability event.

The Life Cycle tests allowed each Member State to test the publishing and lifecycle management of the TSL implementation of their Trusted List (e.g. creation of the first version of the TSL, update of the existing entries with regards to supervision/accreditation status, inclusion of new services to be listed).

The associated Test Plan would include the conformity check of Member States' TSLs against the Trusted List Technical Specifications (i.e., according to ETSI TS 102 231 version 3 provided it is available).

2.2.2.1 Conducting Life Cycle Tests

The present document provides detailed information on how participants must conduct the so-called lifecycle tests on TSLs.

The present document also specifies a set of rules that participants **MUST** follow to ensure their successful participation (7 Rules for conducting the tests). Participants are strongly requested to carefully read this section and strictly follow these rules throughout these tests.

This full document is included in Work Package 1, referenced as "WP1 Conducting TSL Life Cycle Test version 1.0"

2.2.2.2 Test Cases pages

These are pages containing documents with the complete specification of the test cases for TSL Life Cycle.

Below follows a high level description on the mechanics of these tests:

- The portal will include a number of XML documents following the syntax defined in the test case specification language document. One of these XML documents will contain instructions for building up an initial fake TSL listing status of the services provided by a number of fake CSPs. The rest of XML documents will contain information reporting changes in the CSPs and services to be reported by the TSL (i.e., appearance of new CSPs, changes in the status of certain services provided, etc.) and will, in consequence, instruct the participants to generate new instances of the TSL reporting the aforementioned changes.
- Participants will generate and upload the different instances of the TSLs, which will be assessed by the portal tools.
- The portal tools will then carry out a number of checks on the TSL contents and will report the checks results to the participants.

The full description of the test cases are included in the Work Package deliverable referenced as "WP1 TSL Life Cycle Testcases-1.0"

2.2.2.3 TSL contents for the TSL lifecycle test cases

The present page provides details of the contents of the fake TSLs that participants in the TSL lifecycle tests have to generate. It wants to serve as the starting point for building up a common view on how a TSL would change its contents when listed services, listed CSPs or Scheme Operators details suffer specific changes.

The rest of the document is organized as follows:

1. The notation section provides details on the notation used throughout the rest of the document for presenting the contents of the fake TSLs.
2. For each test case, this document contains one section providing details on the relevant contents of the TSL.

The full description of the item is included in the Work Package deliverable referenced as "WP1 TSL contents for the TSL lifecycle test cases 1.0"

2.2.2.4 TSL Testcase Definition Language

The present document specifies a XML language for defining test cases for the so-called lifecycle tests on TSLs. Below follows a high level description on the mechanics of these tests:

- The portal will include a number of XML documents following the syntax defined in the present document. One of these XML documents will contain instructions for building up an initial fake TSL listing status of the services provided by a number of fake CSPs. The rest of XML documents will contain information reporting changes in the status of certain services provided, and will, in consequence, instruct the participants to generate new instances of the TSL reporting the aforementioned changes.
- Participants will generate and upload the different instances of the TSLs, which will be assessed by the portal tools.
- The portal tools will then carry out a number of checks on the TSL contents and will report the checks results to the participants.

The full description of the definition language is included in the Work Package 1 deliverable : "WP1 TSL Life Cycle test cases Definition Language version 1.0".

2.2.2.5 TSL Life Cycle Checks

This document provides details on the checks that the tools deployed in the ETSI Portal for supporting remote interoperability events performs on the fake TSLs to be uploaded by the participants in the TSL lifecycle tests.

The document shows a number of tables where:

- o Details on the rules on some part of the TSL (i.e a specific value of a certain element, or a certain relationship between two elements, etc). Each rule is assigned a unique code that allows to track it in the repertoire of rules.
- o Indication whether not satisfying this rule is a WARNING or an ERROR.

The full description of the Life Cycle Checks is included in the Work Package 1 deliverable : "WP1 TSL Life Cycle Checks version 1.0".

2.2.2.6 Individual verification reports

This area contains a page where each Member State may find its own interoperability matrixes, i.e. matrixes that report the verification results obtained by the rest of the participants after trying to verify each of his/her signatures.

These matrixes include links to the TSL files , to the pretty print versions of the TSL and to the verification report files, as well an indication of the verification result.

For instance for the Testcase TSL-LC-001.xml :

- The TSL of the MS XX TSL-LC-001.xml
- Pretty printed TSL of the MS (Html format): HumanReadable_TSL-LC-001.xml.html
- Pretty printed TSL of the MS (PDF format): HumanReadable_TSL-LC-001.xml.pdf
- VerificationDetails_of_MS_TSL-LC-001.xml.shtml
- VerificationSummary_of_MS_TSL-LC-001.xml
- Verification_of_MS_TSL-LC-001.xml
- XSD-CHK: Schema Check of the TSL

Each participant access from the main page of the portal to her own verification reports page, and from there, each participant may directly access to the verification reports pages of the rest of the participants.

For example, here is the Links to verification report pages:

[AT](#), [BE](#), [BG](#), [CY](#), [CZ](#), [DE](#), [DK](#), [EE](#), [ES](#), [ETSI](#), [EU](#), [FI](#), [FR](#), [GB](#), [GR](#), [HU](#), [IE](#), [IT](#), [LT](#), [LU](#), [LV](#), [MT](#), [NL](#), [NO](#), [PL](#), [PT](#), [RO](#), [SE](#), [SI](#), [SK](#)

This report was generated on Monday, 25-Jan-2010 15:12:11 CET
Signer company: **ETSI**

The following table shows the verification results for the signatures of ETSI in case of TSL-LC0.200910.

Verifiers → TestCases ↓	ETSI
LC-001.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-002.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-003.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-004.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-010.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-011.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-012.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-020.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-021.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-022.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-030.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-031.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-040.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-041.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-050.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-051.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-060.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-070.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-080.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-081.xml	TSL: PRP-TSL: PRP-TSL-PDF: ERROR(S): Summary: Details: XSD-CHK
LC-500.xml	TSL: PRP-TSL: PRP-TSL-PDF: SUCCESS: Summary: Details: XSD-CHK
LC-901.xml	TSL: NOT-YET: NOT-YET: Summary: Details
LC-902.xml	TSL: NOT-YET: NOT-YET: Summary: Details
LC-903.xml	TSL: NOT-YET: NOT-YET: Summary: Details
LC-Name.xml	TSL: NOT-YET: NOT-YET: Summary: Details
LC-SchemeInformationURI.xml	TSL: NOT-YET: NOT-YET: Summary: Details
LC-Address.xml	TSL: NOT-YET: NOT-YET: Summary: Details

2.2.2.7 Statistics per form

This area contains a table that summarizes the number of generated TSL for Life Cycle Testcases , for each Member State.

2.2.2.8 Upload Life Cycle TSL pages

This area contains a page that participants use for uploading their TSL for each Test case.

Filename format: TSL-[LifecycleTestDefinitionFilename].xml

Once uploaded, the portal re-builds verification reports for the corresponding Member State.

2.2.2.9 Test data directory pages

This area contains a page that participants use for browsing the folders structure where the portal stores the Life Cycle TSLs and the verification files generated by all the participants.

This allows a detailed inspection of the files uploaded in a certain instant to the portal.

2.2.2.10 Known issues pages

This area contains a page that lists all the different issues that were raised during the event.

2.2.2.11 Questions and answers pages

This area contains a page that collects the most relevant questions raised during the Life Cycle Testing and their corresponding answers if they have been agreed.

2.2.3 Contents of TSL Plugtests area of Private part

The portal contains, within the private part of the portal, a specific area for Plugtests that is tested in this Interoperability event.

The purpose of the Plugtests was to validate the simulated use of the Trusted Lists TSL implementations in cross-border use (validation) of qualified electronic signatures and advanced signatures based on qualified certificates.

Those tests have been conducted in parallel with the lifecycle management tests of the TSL to validate the effects of such tests in the context of the validation of electronic signatures.

2.2.3.1 Conducting Plugtests

This page provides details on how participants in the remote TSL plugtest event will conduct interoperability tests, by submitting to the portal simple forms of XAdES-Signatures and by verifying signatures created by the rest of participants. As integral part of these verifications, the participants will check the status of the issuers of the qualified certificates (and also TSA's, OCSP responder's and CRL certificates when necessary) in the suitable TSLs. It must be emphasized that during this event, the TSLs used will be the real ones, actually deployed in the different European Member States. This event will allow, in this way, to assess the degree of interoperability that may be achieved using this infrastructural piece within the European Union.

This plugtest will mainly deal with the so called generation and cross-verification test cases. Throughout this plugtest, each participant is invited to generate a certain set of valid XAdES signatures with certain characteristics (generation). The rest of participants are invited afterwards to verify these signatures (cross-verification). The plugtest portal automatically generates an updated set of interoperability matrixes that all the participants may access.

Two different participant profiles are foreseen:

1. [PROFILE-1]: Participants with TSL-enabled signature verification tools .
2. [PROFILE-2]: Participants with NOT TSL-enabled signature verification tools .

2.2.3.1.0 Conducting Plugtests: Starting Plugtests

This page describes how participants must conduct TSL interoperability tests using the ETSI Electronic Signatures Portal. It provides details on the operations that participants shall perform for starting the TSL plugtest.

2.2.3.1.2 Conducting Plugtests: Generating XAdES Signatures

This document provides details on how participants must generate XAdES signatures and upload them to the portal.

2.2.3.1.3 Conducting Plugtests: Verifying XAdES Signatures

This document provides details on the operations that participants shall perform for verifying XAdES signatures generated by other participants and how to use, if they want, the tool deployed in the portal that, given a set of certificates, checks the status of the corresponding Certification Services in the corresponding TSLs.

2.2.3.2 Check Certificates page

This section allows participants to upload a certificate for checking it against a real EUMS TSL.

If a list of the lists is present in the EU folder, the tool first takes this list of lists, and looks for the PointersToOtherTSLs, retrieves the corresponding EUMS list and proceeds.

This tool is provided into the portal as a help tool.

2.2.3.3 Conformance Checker page

On the request of the EC, a conformance checker has been intergrate into the portal. Participants had the possibility to upload their TSL and check the result.

As the lifecycle tool, the conformance checker generates a xml file whose root element and namespace are the ones that the lifecycle tool generated. Errors and warnings are reported in the same way (same elements <svrl:failed-assert>, same content structure "[ERROR] Rule.....")

The Main difference in the report: now the file contains ALL the checks performed, including those ones that have succeeded.

This version of the conformance checker also incorporates the check on X.509 certs present in the service history instances.

After having uploaded his TSL , each participant got the following result:

- Conformance Checker report
- PrettyPrint Pdf version of the uploaded TSL
- PrettyPrint Html version of the uploaded TSL
- Schema Check : The schema is checked against TS 102 231 v3.1.2 (published officially and downloadable from the ETSI site).

2.2.3.4 Test Cases pages

This document defines test cases for the remote interoperability tests of the TSL v3.1.0 [TSL_v3.1.0], CD L 274/36 [CD-L_274-36] and XAdES specification [XAdES_v1.3.2]. The intention of the test cases is to support software developers in creating interoperable implementations and to get feedback from implementers as input for the TSL and XAdES maintenance process and future versions of the TSL and XAdES specification.

The test cases will consist of testcase definitions and signed XML documents. XML signatures will be generated according to the details specified in the testcase definitions and the present document.

The XAdES-Form identifies the XAdES form and is composed of XAdES-[Form].

The Form can be

- BES - Basic Electronic Signature (4.4.1, page 13)
- EPES - Explicit Policy based Electronic Signature
- T - with Time-stamp
- C - Complete validation data
- X - eXtended validation data (B.1, page 57)
- XL - eXtended Long (B.2, page 58)
- A - Archiving validation data (B.3, page 59)

The documents are written in XML and incorporate XSLT stylesheets and javascript technologies. These technologies allow:

- To browse the aforementioned test definition documents and build pieces of text and tables corresponding to each test case within this document.
- To browse reports of verification (simple XML documents) of each single XAdES and TSL verified by each participant, process them and keep up to date the interoperability matrixes, which show what signatures of each participant have been verified by what other participants and the results of such verifications.

The TSL test case document actually incorporates the whole set of interoperability matrixes resulting from the uploading of the participants of their verification report. It is worth to mention that XSLT and javascript technologies allow that each time a participant uploads a set of signatures and/or verification reports, the interoperability matrixes shown within the TSL test case document, are updated, so that participants always see the up to date information on interoperability tests carried so far.

2.2.3.5 Individual verification reports

This area contains a page where each MS may find its own interoperability matrixes, i.e. matrixes that report the verification results obtained by the rest of the participants after trying to verify each of his/her signatures.

These matrixes include links to the signature files and to the verification report files, as well an indication of the verification result.

Each participant access from the main page of the portal to her own verification reports page, and from there, each participant may directly access to the verification reports pages of the rest of the participants.

Example :

Links to verification report pages:

[AT](#), [BE](#), [BG](#), [CY](#), [CZ](#), [DE](#), [DK](#), [EE](#), [ES](#), [ETSI](#), [EU](#), [FI](#), [FR](#), [GB](#), [GR](#), [HU](#), [IE](#), [IT](#), [LT](#), [LU](#), [LV](#), [MT](#), [NL](#), [NO](#), [PL](#), [PT](#), [RO](#), [SE](#), [SI](#), [SK](#)

Signer company: ETSI

The following table shows the verification results for the signatures of ETSI in case of XAdES-BES.SCOK. X-BES-1.xml and X-BES-2.xml

	A T	B E	B G	C Y	C Z	D E	D K	E E	E S	ET SI	E U	F I	F R	G B	G R	H U	I E	I T	L T	L U	L V	M T	N L	N O	P L	P T	R O	S E	S I	S K
X- BES- 1.xml																														
X- BES- 2.xml																														

2.2.3.6 Testcase Results Overview

This pages contains a table showing results in an Interop matrix per Testcases.

2.2.3.7 Statistics per form

This pages contains a table of the number of generated TSL Plugtests signatures from each Member State.

2.2.3.8 Upload pages

This area contains a page that participants use for uploading their signatures and / or verification reports.

The Upload pages provide mechanisms for uploading new signatures, new verification reports or both.

Once uploaded, the portal re-builds a new downloading package in the corresponding specific area and makes it available for all the participants at the corresponding Download page. Within this package, participants will find all the signatures and verification reports generated up to that instant in the plugtest.

As it has been already mentioned, the upload of a package has the immediate effect of updating the corresponding interoperability matrixes and the individual verification reports within the suitable specific area.

2.2.3.9 Download pages

This area contains a page that participants use for downloading the corresponding initial package that includes cryptographic material, test-definition files, and a folder structure suitable for uploading signatures and verification reports).

These pages are also used for downloading the whole material generated by the participants at a certain instant of the plugtest.

2.2.3.10 Test data directory pages

This area contains a page that participants use for browsing the folders structure where the portal stores the TSLs and the verification files generated by all the participants during the Plugtests.

This allows a detailed inspection of the files uploaded in a certain instant to the portal.

2.2.3.11 Questions and answers pages

This area contains a page that collects the most relevant questions raised during the Plugtests and their corresponding answers if they have been agreed.

3. Participation

3.1 TSL Interop Team

Below follows the list of members of the TSL Interop team that contribute to the Interoperability event.

- **Caccia, Andrea** - UNINFO, Italy
- **Chaulot-Talmon, Emmanuelle** - ETSI, France (Secretariat)
- **Cruellas, Juan Carlos** - the Universidad Politècnica de Catalunya, Spain
- **Lanz, Konrad** - IAIK/SIC, Austria
- **Mongiello, Daniele** - Infocert, Italy
- **Reina Ortega, Miguel Angel** ETSI, France (Secretariat)
- **Velez, Laurent** - ETSI, France (Secretariat)

3.2 Participants list

The table below shows the details of all the organizations and persons that have participated in the Autumn 2009 TSL Remote Interoperability Event.

There have been 22 organisations participating in the event including 20 Member States and and ETSI and European Commission representants.

This makes a total of 64 persons involved in the daily activities of the event.

Name	Login name	CC	Company
Ulrich Latzenhofer	latzenhofer	AT	Rundfunk und Telekom Regulierungs-GmbH
Frank Cornelis	cornelis	BE	FedICT
Jan Dvorak	dvorak	CZ	MathAn Praha
Lucie Rut Bittnerova	bittnerova	CZ	MathAn Praha
Jaroslav Tomanek	tomanek	CZ	Ministry of the Interior of the Czech Republic
Juergen Schwemmer	schwemmer	DE	Bundesnetzagentur (BNetzA)
Petra Wohlmacher	wohlmacher	DE	Bundesnetzagentur (BNetzA)
Konstantin Goetze	gotze	DE	Bundesnetzagentur (BNetzA)
Frank Jeschka	jeschka	DE	OpenLimit SignCubes GmbH
Markus Ruppert	ruppert	DE	FlexSecure GmbH

Joerg Apitzsch	apitzsch	DE	Bremen online services
Uuno Vallner	vallner	EE	Ministry of Economic Affairs and Communications
Alfredo Vegas	vegas	ES	Ministerio de Industria, Turismo y Comercio
Carlos Guerra	guerra	ES	Ministerio de Industria, Turismo y Comercio
Oscar Martinez	martinez	ES	Ministerio de Industria, Turismo y Comercio
Juan Antonio Perez	perez	ES	Ministerio de Industria, Turismo y Comercio
Raul Guerra Gimenez	guerra-jimenez	ES	Ministerio de Industria, Turismo y Comercio
Emmanuelle Chaulot-Talmon	chaulot-talmon	ETSI	ETSI
Konrad Lanz	lanz	ETSI	A-SIT (IAIK) - Austria
Juan Carlos Cruellas	jccruellas	ETSI	Universitat Politecnica de Catalunya
Andrea Caccia	caccia	ETSI	UNINFO
Daniele Mongiello	mongiello	ETSI	INFOCERT
Miguel Angel Reina Ortega	reinaortega	ETSI	ETSI
Laurent Velez	velez	ETSI	ETSI
Per-Olav Gramstad	gramstad	EU	European Commission
Anneli Andresson	andresson	EU	European Commission
John Stienen	stienen	EU	European Commission
Olivier Delos	delos	EU	European Commission
Laurent Voillot	voillot	FR	DGME
Olivier Pallany	pallany	FR	DGME
Nikolaos Diamantidis	diamantidis	GR	EETT
Antonis Stasis	stasis	GR	Hellenic Ministry of Interior
Konstantinos Rantos	rantos	GR	Hellenic Ministry of Interior
Patroklos Papapetrou	papapetrou	GR	Hellenic Ministry of Interior
Panos Karvounis	karvounis	GR	Hellenic Ministry of Interior
Istvan Renyi	renyi	HU	National Communications Authority
Agnes Juhasz	juhasz	HU	National Communications Authority

Tadgh O'Leary	oleary	IE	IE Department of Finance
Vaidotas Ramonas	ramonas	LT	Information Society Development Committee
Irma Tumaloviciute	tumaloviciute	LT	Information Society Development Committee
Evaldas Zidonis	zidonis	LT	Information Society Development Committee
Audrius Masidlauskas	masidlauskas	LT	Information Society Development Committee
Giedrius Noreikis	noreikis	LT	MitSoft Ltd
Adomas Birstunas	birstunas	LT	MitSoft Ltd
Olivier Barette	barette	LU	ILNAS
Jean-Philippe Humbert	humbert	LU	ILNAS
Maris Freimanis	freimanis	LV	Latvia State Radio And Television Centre
Toms Celmillers	celmillers	LV	Ministry of Regional Development and Local Government of the Republic of Latvia
A.Haasnoot	haasnoot	NL	Ministerie van Economische Zaken
Koos van der Spek	vanderspek	NL	Ministerie van Economische Zaken
Dennis Baaten	baaten	NL	Ministerie van Economische Zaken
Ornulf Storm	storm	NO	Norwegian Post and Telecommunications Authority
Bartosz Nakielski	nakielski	PL	National Bank of Poland
Tomasz Rakoczy	rakoczy	PL	CPI MSWiA
Paulo Balsinhas	balsinhas	PT	National Security Authority - Portugal
Pedro Felix	felix	PT	National Security Authority - Portugal
Kalevi Pitkanen	pitkanen	SE	Tillvaxtverket
Jonas Oholm	oholm	SE	Tillvaxtverket
Gabriella Lundin	lundin	SE	Tillvaxtverket
Fredrik Ahlstedt	ahlstedt	SE	Tillvaxtverket
Johan Bergsten	bergsten	SE	Tillvaxtverket
Maks Romih	romih	SI	Ministry of Public Administration, Slovenia
Peter Rybar	rybar	SK	NATIONAL SECURITY AUTHORITY
Daniela Jakubikova	jakubikova	SK	NATIONAL SECURITY AUTHORITY

3.3 Web conference Meetings

A total of 10 web conf calls were organized during the event. We used gotomeeting web conf tool, that has allowed interactivity in the meeting by sharing screen between participants and the TSL team.

In order to facilitate communications and especially to keep a track of the questions, it was kindly asked to also login to the Chat service.

Meeting #1 (Introduction meeting) - Tuesday 20th October 2009; 15:00-16:00 CET

Agenda

1. Welcome by ETSI
 - 1.0 Presentation of the project (Life Cycle and plugtest)
 - 1.2 Presentation of the TSL interop team
2. Roll call (self introduction by each participant)
3. Presentation of the portal supporting the interop
 - 3.1 Infrastructure for supporting daily communication
 - 3.2 Infrastructure for supporting conference calls
 - 3.3 URLs of interest (list below with their purposes)
4. Meetings during the interop
 - 4.1 Meetings scheduling
 - 4.2 Goals of the meetings
 - 4.3 Minutes of the meetings
5. Conducting Life Cycle tests
 - 5.1 Rules for conducting Life Cycle tests
 - 5.2 Tools
 - 5.3 Questions and answers
 - 5.4 Known issues
6. Conducting plugtests
7. Next meeting, Any Other Business

Meeting #2 - Thursday 22th October 2009; 13:30-15:00 CET

The goal of this meeting is :

- To make a debrief after the first days of the life Cycle testing
- To clarify the conducting Life cycle procedure if needed
- To discuss about the potential portal issues
- To review testcases if any questions or concerns
- Any other topics
- Define the date for next meeting.

Meeting #3 - Monday 26th October 2009; 13:30-15:00 CET

Meeting #4 - Thursday 29th October 2009; 13:30-15:00 CET

Meeting #5 - Tuesday 3rd November 2009; 13:30-15:00 CET

Agenda of the web conf:

1. Presentation of the Plugtest part of the portal
2. Conducting Plugtests
 - 2.1 Rules for conducting Plugtests
 - 2.2 Tools
 - 2.3 Questions and answers
 - 2.4 Known issues
3. Status of the Life Cycle testing
4. F2F meeting in ETSI (23-26 Nov 2009)
5. Next Conf call
6. Any Other Business

Meeting #6 - Tuesday 10th November 2009; 13:30-15:00 CET

Meeting #7 - Wednesday 18th November 2009; 13:30-15:00 CET

Meeting #8 - Tuesday 1st December 2009; 13:30-15:00 CET

Meeting #9 - Thursday 17th December 2009; 13:30-15:00 CET

The goal of this meeting is to present the ☐TSL Conformance checker☐ and also make a review of the pending questions

Meeting #10 - Tuesday 22nd December 2009; 14:00-15:00 CET

The goal of this meeting is to discuss and get feedback from participant about the “TSL Conformance checker” and also make a review of the pending question

3.4 Face to Face Meeting

ETSI Centre for Testing and Interoperability (CTI) has hosted and organized the TSL face to face meeting from 23rd to 26th November 2009, in Sophia-Antipolis , France.

The organization of this meeting, the registration process and the meeting support were the tasks of the Work Package 5.

Attendees to the F2F meeting:

Juergen Schwemmer (DE); Peter Rybar (SK); Agnes Juhasz (HU); Frank Cornelis (BE); Olivier Barette (LU); Konrad Lanz; Laurent Velez; Miguel Angel Reina Ortega; Juan Carlos Cruellas; Andrea Caccia; Per-Olav Gramstad (EC); Olivier Delos.

Agenda

DAY 1 / Monday 23rd Nov (starting on Monday 14:00)

1. Educational session on how:
 - . to build tsls,
 - . and how to happen in real life
 - . Consolidation of TSL lifecycle related concepts.
2. Operational aspects in the management and lifecycle of the TSLs
 - Publication
 - Evolution

DAY 2 / Tuesday 24th Nov

Summary of DAY1 for those not present and further discussions on these summarized topics

3. Signing TSLs (TSLs may also exist unsigned).
4. Semantics of TSLs contents. Per-State based discussion.

DAY 3 / Wednesday 25th Nov

5. List of lists. (including discussion on notification elements from MS towards the EC)
6. Usage machine processable / non machine processable TSLs.
7. Verification process of the tsl:
 - . Specific details of the process.
 - . Development aspects.
 - . Reference verification process.
 - . States' experiences.

DAY 4 / Thursday 26th Nov

8. Evolution of standard
9. Discussions on other issues raised in the email lists:
 9. 1. ssh publication of tsls.
 etc ...
10. Live TSL test sessions

WIKI

During the F2F meeting, a wiki has been created in order to provide meeting details to the participants and also to share information and documents. It has been usefull to gather feedback and question from participants, in order to creat a meeting report.

Report

A F2F meeting report has been created after the meeting. It includes all the conclusions taken during the meeting, following the discussion on the topics mentioned in the agenda.

This document which is an interim report of the event is provided as a deliverable of the Work Package 6.

4. Interoperability Event Conclusions

This section summarizes the most important conclusions reached after the end of the event.

4.1 General Conclusions

This first remote Interoperability event on TSL has confirmed the usefulness of the event concept in different aspects:

o For a such long event period, the possibility of remote participation have lead to a much higher availability and effectiveness of participants.

o A critical issue for the successfulness of this kind of events is to be provided with a good and reliable communication infrastructure, which allows participants to exchange their views quickly and even conduct voice discussions. The three technologies briefly discussed below have provided once again a high enough degree of communication capabilities for this plugtest.

- Web Conference/Phone bridge is crucial for having a number of meetings during the event where participants may discuss specific issues of the testing and even on the standardization of the specifications.
- An email list with archive capabilities, closed to participants is also crucial for this kind of events: this is by far the communication mean most widely used in this interop event: participants have asked questions, raised comments on the tests and/or standard, have suggested solutions, have been notified that some other participant had uploaded new signatures or verification reports, and be an archive of whatever has been exchanged between participants during this interop event.
- Chat channel has also proved to be useful during the meetings to the point that some participants used more the chat than the voice.

o The remote but yet continous contact among participants lead to maintain interesting technical discussions on TSL and related topics.

4.2 Contributions to Standardisation

A number of issues affecting TSL specification contents were raised during the Interoperability event. These issues have been incorporated in the TSL F2F meeting report that will be circulated to TC ESI. This constitutes by itself a major outcome of the interop event.

It includes change requests and recommendations :

- Changes to ETSI TS 102 231

- Clarifications on the implementation guidelines for Commission Decision 2009/767/EC
- Clarifications for the implementation of Decision 2009/767/EC and future changes

4.3 Benefit for Member States and European Commission

Nevertheless, according to a lot of positive feedbacks, the participants, by conducting this interoperability event have been able to identify aspects in their implementations and in their reading of the specification that have helped to improve them.

Participants may, as they are in the possession of the signatures, proceed further to identify why certain results are not as they expected.

Additional Tasks:

Moreover, during the daily discussions with the participants and the European Commission representatives, it has been identified some new tasks or tools that were not initially requested in to the project contract. These additional tasks were anyway needed for the achieving the goal of the full interoperability of TSL between member states.

Taking benefit of the great scalability of the portal, the TSL team has performed these extra tasks. This has enabled to integrate the Conformance Checker and the Schema Check tool. The tools and the portal has also been adapted to the specific TSL which is the list of the lists.

A. Annex: List of Work Package Deliverables

This project proposes the following deliverables for the Work Packages as described in the contract.

The industrial or intellectual property rights for the following deliverables exist prior to the Contract and will therefore not be owned by the Community as set out in Art I.10.3 and II.8 of the Contract:

- o The Signature verification tools TSL-enabled (for TSL Plugtest) as set out in work package task 3.3 above.
- o The ETSI Plugtest portal to be used within the Plug Test event as set out in work package task 4 and 5 above."

- **Work Package 0 : Project Management**

Meeting Presentations

A CD-ROM with all minutes and reports, as well as all deliverables described below, at the end of the project.

- **Work Package 1: Definition of Conformance Test Suite (TSL life cycle test)**

WP1 Conducting TSL Life Cycle Test-v1.1

WP1 TSL Life Cycle Testcases-v1.1

WP1 Conducting TSL Life Cycle Test Cases definition Language-v1.1

WP1 TSL contents for the TSL lifecycle test cases v1.1

WP1 TSL Life Cycle Checks-v1.1

- **Work Package 2: Definition of Interoperability Test Suite (TSL Plugtest)**

WP2 Conducting Plugtests-v1.1

WP2 TSL Plugtests Testcases-v1.1

WP2 TSL Plugtests - XAdES Testcase Definition v1.1

- **Work Package 3: Provision of tools for conformance and interoperability tests**

TSL checking functions/tools (for TSL life cycle tests);

Pretty Print TSL tool (for TSL life cycle tests and Plugtests conformance checker).

- **Work Package 6: Reporting and meeting for non-ETSI experts**

WP6 F2F Meeting report v1.1 (Interim report)

Final report : WP6 TSL Interop Final Report v1.1