

FEEDBACK REPORT

Version 1.0

Date: 29th June 2004



Reference

<Workitem>

Keywords

<keywords>

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

Important notice

Individual copies of the present document can be downloaded from:
<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

Contents

1	INTRODUCTION	4
2	DEFINITIONS AND ABBREVIATIONS	4
2.1	DEFINITIONS	4
2.2	ABBREVIATIONS	4
3.	GOALS OF THE EVENT.....	5
4	LIST OF PARTICIPATING COMPANY.....	6
	EVENT’S PLANNING.....	7
	TEST S BEDS	8
	XADES TEAM	8
	PKI TEAM	8
	TESTS RESULTS FOR XADES.....	9
	XADES PARTICIPATING IMPLEMENTATIONS	9
	UPC:.....	9
	Microsoft :	10
	CDC Mercure :	11
	SEB IT :	12
	TESTS RESULTS BY PARTICIPANTS	13
	UPC	13
	Microsoft.....	13
	SEB IT.....	14
	CDC Mercure	14
	INTEROPERABILITY RESULTS FOR XADES TESTS.....	15
	TESTS RESULTS FOR PKI	16
	PARTICIPATING IMPLEMENTATIONS	16
	SSH	16
	IDEALX	16
	INTEROPERABILITY RESULTS	16
	EE certification enrolment:	16
	Cross Certification Enrolment.....	16
	Validation tests	17
	TECHNICAL FEEDBACKS ON XADES SPECIFICATIONS.....	18
	GENERAL COMMENTS ON XADES	19

1 Introduction

The event was held from 24-28 May 2004 at ETSI headquarters in Sophia Antipolis in the South of France. The main field of this event was the security, including PKIs systems and XAdES standards.

It was organized in co-operation with ETSI's Services and Actimage.

For the first time, PKIs solutions are able to test their capacity of interoperability with others systems.

The testing event focused on interoperability between different PKI systems, in particular about the validator system of each solution, and tested the compatibility of the XAdES messages generated by different providers.

2 Definitions and abbreviations

2.1 Definitions

End Entity: This entity is optional and has the responsibility to register the new end-users.

Validator: It's a system which is able to validate a certificate issued by a CA.

Enveloped signature: The signature is over the XML content that contains the signature as an element. The content provides the XML root document element. Obviously, enveloped signatures must take care to not include their own value in the calculation of the SignatureValue.

Enveloping signature: The signature is over the content found within an Object element of the signature itself. The Object (or its content) is identified via a Reference (via a URI fragment identifier or transform).

Canonicalization algorithm: This algorithm is simply a process that reads XML and converts it to a consistent form. The Canonicalization ensures that XML documents containing same intrinsic representation have the same binary representation, and therefore the same signature.

2.2 Abbreviations

XAdES: XML Advanced Electronic Signatures

PKI: Public Key Infrastructure

SCEP: Simple Certificate Enrollment protocol

PKCS#10: Public Key Cryptography standard 10 see RFC 2314

CRL: Certification Revocation list

CRLDP: CRL Distribution Point

LDAP: Lightweight Directory Access Protocol

CA: Certification Authority

OCSP: Online Certificate Status Protocol

EE: End Entity

3. Goals of the Event

The interoperability event was organized around two technologies: XAdES and PKI.

Followings goals and advantages have been identified for this interoperability event:

- · Check the interoperability between PKI solutions.
- · Improve and validate the XAdES standardization (ETSI TS 101903 v1.2.2 published in April 2004). For sure the results of this event may have an impact in the next version.
- · Opportunity to quickly discover errors in implementations with fast turn-around testings
- · Bring Competitors together to progress on specification development and implementation

4 List of Participating Company

- Actimage
- CDC-Mercure
- GIP-MDS
- Idealx
- Macao Post eSignTrust Certification Authority
- Microsoft EMEA
- Panasonic Communication Co
- SIEIB IT Partner
- SETCCE
- SSH Communications Security Corp.
- University of Catalunya

Event's Planning

	24 May	25 May	26 May	27 May	28 May
9h		Test preparation	INTEROP (XADES and PKI)	INTEROP (XADES and PKI)	INTEROP (XADES and PKI)
10h	Introduction Philippe COUSIN (ETSI)	XAdES Standardization and interoperability issues (Juan Carlos Cruellas - UPC)		Implementation of XAdES standard in Slovenia for e-invoicing (Mr. Blazic - SETCCE)	
11h	Context and security needs for french social institution and institutional view of the PKI problems (Alain ROUX - GIP MDS)	INTEROP (XADES and PKI)		Open Source Security Solution in European Context (Vincent GASS - CONSEN)	
12h					
13h					
14h	Test preparation	INTEROP (XADES and PKI)	ASIA PKI Interoperability Guideline (Gregory Sun - eSignTrust)	INTEROP (XADES and PKI)	
15h			INTEROP (XADES and PKI)		
16h	IPV6 Camera presentation (Panasonic)		INTEROP (XADES and PKI)		
17h	Test preparation				
18h		Debriefing	Debriefing	Debriefing	

Test s beds

XAdES Team

The following tables show the different types of XAdES signature tested and the different interoperability tests built between each participants.

Company	Type of XAdES					Language			
	XADES	XAdES-T	XAdES-C/X	XAdES-X-L	XAdES-A	C	Java	C++	C#
UPC	X	X	X	X	X		X		
CDC	X					X	X	X	
SEB-IT	X		X	X		X	X	X	
MICROSOFT	X	X	X	X					X

Generator\Validator	UPC	SEB-IT	MICROSOFT
UPC		X	X
SEB-IT	X		X
MICROSOFT	X	X	
CDC	X		X
IAIK(1)	X	X	X
Baltimore(1)			X
BeTrusted(1)	X		

(1)Not Present in this event but his XAdES implementation has been tested.

PKI Team

Only two companies participated to the PKI solutions interoperability testing: IdealX and SSH Communications Security Corp.

Tests Results for XAdES

XAdES Participating Implementations

UPC:

Implementation by	UPC
Implementation language	Java
Base cryptographic toolkit	Java SDK, SUN cryptographic provider
Base xml-signature toolkit	UPC-xslib (a XMLDSIG tool implemented by UPC)
Base xml toolkit	JDOM using xerces parser
Will be available in the following form	Probably commercial licence
Source code availability	No
Person to contact	Juan Carlos Cruellas, cruella@ac.upc.es
Other information of interest	

Microsoft :

Implementation by	Microsoft
Implementation language	C#
Base cryptographic toolkit	Microsoft .NET runtime 1.1
Base xml-signature toolkit	XMLDSIG standard implementation in .NET runtime
Base xml toolkit	
Will be available in the following form	Toolkit
Source code availability	Free
Person to contact	Eddy Rubens, eddyrube@microsoft.com
Other information of interest	

CDC Mercure :

Implementation by	CDC-Mercure – FAST Project	
Implementation language	C	Java
Base cryptographic toolkit	Microsoft Crypto API OpenSSL	JCE SUN
Base xml-signature toolkit	Aleksey Security Library (www.aleksey.com/xmlsec)	Apache XML Security Library (http://xml.apache.org/security)
Base xml toolkit	LibXML2 (www.xmlsoft.org)	Xerces / Xalan
Will be available in the following form	CFAST Toolkit (Win32 / *nix) FAST ActiveX (Win32)	JFAST Toolkit (Win32 / *nix) FAST Applet (Win32)
Source code availability	no	
Person to contact	Julien Montagne, julien.montagne@caissedesdepots.fr	
Other information of interest	The CFAST Toolkit is currently undergoing evaluation within the French Common Criteria Evaluation and Certification Scheme (DCSSI)	

SEB IT :

Implementation by	SEB-IT	
Implementation language	C	Java
Base cryptographic toolkit	OpenSSL	Bouncy-Castle
Base xml-signature toolkit	CDigiDoc	JDigiDoc
Base xml toolkit	Libxml2	Xerces-J
Will be available in the following form	C library toolkit for Win32, Linux, FreeBSD COM component for Win32	Java library toolkit
Source code availability	Libraries are available today www.openxades.org	
Person to contact	Sinivee Veiko, veiko.sinivee@seb.se	
Other information of interest	GUI application for Win32 available at www.id.ee GUI application for Linux available at http://www.sourceforge.net/projects/gdigidoc WebService based on SOAP and offering simpler XML signature service for web applications in test. Will be soon available at www.sk.ee	

Tests results by participants

In this event, the priority of this test were twofold:

- To go on with tests already defined in the first interoperability event. This was justified for both, implementations present in the first event and for those already present in the first event, as these new interoperability tests could raise new issues not raised in the first event.
- To validate test failures cases where the tools should notify a failure in the verification of XAdES signatures.

Tests leading to validation failure:

- Tests with failures related with SigningCertificate
- Tests with failures related to SignaturePolicyIdentifier
- Tests with failures related to CompleteCertificateRefs
- Test with failures related to CompleteRevocationRefs
- Test failures related with CertificateValues property
- Test failures related with RevocationValues property
- Test failures related with AllDataObjectsTimeStamp property
- Test failures related with IndividualDataObjectsTimeStamp property
- Test failures related with SignatureTimeStamp property
- Test failures related with SigAndRefsTimeStamp property
- Test failures related with RefsOnlyTimeStamp property
- Test failures related with ArchiveTimeStamp property

UPC

1. Verifying signatures
 - SEB-IT: all XAdES signature tests passed
 - Microsoft: all XAdES signature tests passed
 - CDC: all XAdES signature passed
 - IAIK: all XAdES signature tests passed
 - Betrustrad: all XAdES signature tests passed
2. Producing signatures
 - All XAdES forms have been produced

Microsoft

1. Verifying signatures
 - UPC: all XAdES signature tests passed
 - SEB-IT: all XAdES signature tests passed

- CDC: all XAdES signature tests passed
 - Baltimore: all XAdES signature tests passed
 - IAIK: all XAdES signature tests passed
2. Producing signature
 - All XAdES forms have been produced (except XAdES-A)

SEB IT

1. Verifying signatures
 - UPC: The verification failed because the certificate was expired. SEB IT recommends to use timezone info either in form CCYY-MM-DDTDD:HHZ or CCYY-MM-DDTTDD:HH-xx:yy for the SigningTime Element. Finally, he can read UPC Signature and validate then except the certificate problem.
 - Microsoft: Validate Microsoft's XAdES#1 form but recommends to use timezone info either in form CCYY-MM-DDTDD:HHZ or CCYY-MM-DDTTDD:HH-xx:yy for the SigningTime Element.
 - IAIK: The verification failed because the KeyInfo element was missed. SEB IT said probably he was able to validate IAIK's signature soon by reading signers certificate from file.
2. Producing signature
 - XAdES form has been produced

CDC Mercure

1. Verifying signatures
 - No signature of the other participants validated.
2. Producing signature
 - XAdES form (enveloped signature and enveloping signature)

« This first participation to an ETSI PlugTest has proven to be a really useful experience for CDC-Mercure and the FAST project.

Before coming to Sophia we didn't know exactly what to expect because we were only able to create enveloped signature and the tests specifications were exclusively dedicated to enveloping signature. But we were reassured as soon as we arrived.

Achieving the validation test cases on our XAdES implementation was a combined effort of all participants. We had to modify our API to change the canonicalization algorithm from its exclusive to its inclusive form while other implementers were adding enveloped signature support in their validation tools. Finally we were able to verify that the FAST signature format met XAdES requirements and we would like to warmly thank all the participants for this result.

This event gave use the opportunity to gain a better knowledge of the latest XAdES evolutions and of their potential impact on our work. It gave us excellent inputs for our future developments, both on the signature creation and signature validation sides. » (Jérôme Bordier, CDC-Mercure).

Interoperability results for XAdES tests

The interoperability tests uncovered the following issues:

1. Problem about the certificate serial number length, present in the <ds:X509SerialNumber> element defined in XMLSig. In fact, the content of this element, which contains the serial number, is declared as W3C XML Schema integer. This is a 64 bits type and long certificate serial number cannot be contained in this element. Certificates with serial number greater than the upper boundary can not be dealt with. This problem should be fixed in the next version.
2. Problem with contents of element <ds:X509IssuerName>. XAdES uses this element when making references to certificates. XMLSig clearly references RFC 2253 for specifying the encoding of a Distinguished Name as a String. Nevertheless, some implementations did show interoperability problems when comparing contents of such strings. This is not a problem of XAdES or XMLSig but of the implementations themselves.

Those implementations that had not participated in the first interoperability event had the chance of offering their signatures to other participants so that tests could be made, and vice-versa, they had the opportunity of, after doing some re-factoring (as SEB-IT did), verify the signatures of other participants.

Those implementations that had participated in the first event, could go on with tests that had not been done there. These tests sometimes uncovered problems within the tools themselves and in general made them to go further in the path of achieving interoperable implementations.

Tests Results for PKI

Participating Implementations

SSH

Company	SSH Communication Security Corp.
Product Name	SSH Tectia Certifier v3.0.0beta/v2.1.3 (+ some tools from other SSH Tectia products)
Person to contact	Tomi Kause toka@ssh.com

IDEALX

Company	Idealx
Product Name	IDXPKI
Person to contact	Cyril Lavoisy : clavoisy@idealx.com Julien Gilli : jgilli@idealx.com Benoit Caccinolo : bcaccinolo@idealx.com

Interoperability results

During this event, the two actors of PKI domain (SSH and Idealx) tested some interoperability problems specific to architecture:

EE certification enrolment:

This test is a very basic mutual end-entity certificate enrolment test.

	SSH→Idealx	Idealx→SSH
PKCS#10	OK	Not tested (1)
SCEP	OK	OK

(1) We can notice this test was skipped because the cross certification test the same functionality and more.

Cross Certification Enrolment

Both ends created and submitted (via a web form) a PKCS#10 request for their self-signed root CA. Both CAs mutually accepted each others requests successfully, and the SSH CA successfully published a cross-Certificate Pair to the LDAP directory.

This test required some manual steps from both participants:

- The Idealx CA didn't even claim to support cross-certification, so some manual tweaking was required to preserve the basic Constraints in the request.
- An external script was created for the SSH CA to create and publish the Cross-Certificate Pair object to LDAP.

	SSH→Idealx	Idealx→SSH
PKCS#10	OK	OK

Validation tests

Idealx couldn't do this test because the Idealx System has not a stand-alone validator. That's why the N/A for all the validation tests is written.

- Validation/Simple end-entity validation

	SSH->Idealx	Idealx→SSH
CRL/HTTP CRLDP	OK	N/A
OCSP	Fail	OK (with the regular OpenSSL OCSP client)

The OCSP validation against the Idealx system failed because the SSH validator rejected the self-signed OCSP responder certification of the Idealx responder.

- Validation/Cross recognition

The SSH validator was initialised with multiple trust anchors (self-signed root certifications). With this setup the validator was able to validate EE certifications issued by any of the CAs/SubCAs under those roots.

	SSH→Idealx	Idealx→SSH
CRL/HTTP CRLDP	OK	N/A

- Validation/Cross certification

The SSH validator was initialised with one SSH self-signed root as the trust anchor. The validator successfully validated a certificate issued by the Idealx CA, i.e. trust was propagated thru the cross certificate.

	SSH→Idealx	Idealx→SSH
with CRLs	OK	N/A

Technical feedbacks on xades specifications

This event was scheduled shortly after XAdES version 1.2.2 publication. This version incorporated most of the suggestions raised in the first interoperability event. The scheduling of the event made unfeasible to orient it towards XAdES v 1.2.2, as not many implementations would exist at that time. In consequence, the event addressed tests on XAdES v1.1.1. The tests specified for the first event were enlarged for covering a number of situations where XAdES signatures validation should fail for specific reasons.

The first event uncovered a significant number of issues and served for proposing changes to the specification. XAdES v1.2.2 incorporated most of them. As a consequence, not so many issues have been raised in the second one. All of them have already been mentioned before. Below follows a short summary:

- Issue-E2#1. Interoperability tests failed with references to certificates whose serial number is greater than the boundary fixed by the integer type defined in XML Schema. XAdES relies on the definition of <ds:X509IssuerSerial> element present in XMLSig. Perhaps a note to XMLSig email list could raise the issue and make the team in charge of its maintenance to deal with it. A different approach could be to define within XAdES a new type that would overcome this restriction.
- Issue-E2#2. Interoperability tests proved that some problems appeared when dealing with the contents of <ds:X509IssuerName> i.e., Distinguished Names encoded as strings. XMLSig clearly establishes that this encoding must be as specified in RFC 2253. Nevertheless some interoperability problems seem to prove that perhaps a remainder of this reference could be incorporated in XAdES, as a way of facilitating developments.

In addition to that, presentations in the event were certainly interesting. Specially, the one by Mr. Blazic showed the usage of certain XAdES forms in real environments and pointed out a number of issues that could enlarge its scope and increase its usefulness. The proposal of defining archiving properties is one of the most interesting ones, and it may impact future standardization work.

The effort made in the definition of new tests cases, will likely be useful in the definition of tests cases for XAdES v1.2.2

General comments on xades

Comments by Juan Carlos Cruellas:

Below follow comments some comments in the view of the achievements of the event:

- On the scheduling.
 - The fact that the event took place shortly after the publication of XAdES v1.2.2 avoided the possibility of incorporating tests of this version, which would have allowed to assess the goodness of the suggestions made in the first event.
 - On the other hand new tools were present in the event that could be tested with others also present in the first one, so that the range of tools that have been involved in these interoperability event has been enlarged.
 - The event was overlapped with an ESI meeting. As I personally had to attend both events, the result was that I had to split my time between them.
 - In consequence, I would humbly suggest that scheduling of future events would take into account the aforementioned comments. Specifically, I would suggest not to overlap any event with ESI meetings or other meetings directly related with XAdES. I would also suggest for the future, not to celebrate events shortly after the publication of new versions of XAdES.
- On the benefits:
 - UPC was able to go further in tests with Microsoft and with SEB-IT, which in fact made progress the tool itself.
 - At the general level, a number of tests cases for unsuccessful verification of signatures has been added to the initial set of the first event. As XAdES v1.2.2 has a great amount of commonality with XAdES v.1.1.1, this means that a large amount of them will also serve for events organized around XAdES v1.2.2.
 - Few issues not raised in the first event were uncovered in the second one. The lecture of this fact is twofold:
 - First, these issues will feed the standardization process that is not stopped.
 - Second, somehow, this low number is telling us that comments raised during the first event uncovered almost all the relevant issues with respect to the standards.
- On the future:
 - New events must be much more focussed on XAdES v1.2.2, the latest version of the standard. This means that a work has to be done for:
 - Using those tests cases applicable to both versions.
 - Defining new tests cases applicable only to XAdES v1.2.2.

Before the celebration of the next event, ETSI should be more active in supporting the XAdES tools being developed. Somehow it should promote the usage of the email list so that the different entities that participated in both events regularly exchange information on their developments, just as it was done before the first event.

Besides, ETSI and W3C are currently working in setting up a Joint Working Group for dealing with XAdES. This will likely imply that XAdES will eventually reach the W3C Recommendation status. This also implies that anyone interested in XAdES should be aware that there will be an opportunity to become member of this new group once created, and bring her expertise to it and help to improve XAdES.

ETSI and W3C are now dealing with the political, administrative and management stuff.