

Report for the September 2008 XAdES Remote Plugtest Event

October 2008



Report for the September 2008 XAdES Remote Plugtest Event

October 2008
This version:

Authors:

Juan Carlos Cruellas, UPC <cruellas@ac.upc.edu>

Konrad Lanz, A-SIT <Konrad.Lanz@iaik.tugraz.at>

Peter Kremer, ETSI <Peter.Kremer@etsi.org>

Kenji Urushima, Entrust Japan Co., Ltd <kenji.urushima@entrust.com>

Gregory Sun, Macao Post eSignTrust Certification Services <gregsun@esigntrust.com>

Editors:

Juan Carlos Cruellas, UPC <cruellas@ac.upc.es>

Konrad Lanz, A-SIT <Konrad.Lanz@iaik.tugraz.at>

Contributor:

Copyright © 2008 ETSI , All Rights Reserved.

Abstract

This document is the report of the 2008 September Plugtest Event on XAdES v1.3.2, organized by ETSI and conducted using the ETSI portal supporting remote interoperability plugtests.

Status of this Document

This document is provided by ETSI Interopolis Services. For further details on Plugtests services, please see ETSI Plugtests.

Table of Contents

- 1 Document History
- 2 Introduction
- 3 Organization and contents of the portal
 - 3.1 Public part of the portal
 - 3.2 Private part of the portal
 - 3.2.1 Participants list page
 - 3.2.2 Meeting information page
 - 3.2.3 Conducting plugtest information pages
 - 3.2.4 Known issues page
 - 3.2.5 Cryptographic material pages
 - 3.2.6 Presentations pages
 - 3.2.7 Former XAdES plugtests page
 - 3.2.8 Testcases definition language page
 - 3.2.9 Testcases page
 - 3.2.10 Download page
 - 3.2.11 Upload page
 - 3.2.12 Online PKI services details
 - 3.2.13 Online PKI services access
 - 3.2.14 Online TSA services access
 - 3.2.15 Mailing List Archives
 - 3.2.16 Chat
- 4 Plugtest participants
- 5 Plugtest conclusions
 - 5.1 General conclusions
 - 5.2 Lessons Learned
 - 5.3 Technical Conclusions
- 6 Feedback to standardization process
 - 6.1 Check of time indication in xades:SigningTime property with regards to time indications within time-stamp tokens
 - 6.2 MimeType and Encoding attributes in xades:DataObjectFormat and ds:Object
 - 6.3 xades:CompleteCertificateReferences and not CA certificate references
 - 6.4 Dealing with empty elements
 - 6.5 XAdES Forms and extra information
 - 6.6 Computation of the digest of a Signature Policy document aligned with ETSI TR 102038 or ETSI TR 102272
- 7 Interoperability matrixes for positive test cases
 - 7.1 Test cases for XAdES-BES form
 - 7.2 Test cases for the XAdES-EPES form
 - 7.3 Test cases for XAdES-T form
 - 7.4 Test cases for XAdES-C form
 - 7.5 Test cases for XAdES-X form
 - 7.6 Test cases for XAdES-XL form
 - 7.7 Test cases for XAdES-A form

8 Interoperability matrixes for negative test cases

8.1 Test cases for XAdES-BES form

8.2 Test cases for the XAdES-EPES form

8.3 Test cases for XAdES-T form

8.4 Test cases for XAdES-C form

8.5 Test cases for XAdES-X form

8.6 Test cases for XAdES-XL form

8.7 Test cases for XAdES-A form

9 References

A Author's Adress

(Non-Normative)

1 Document History

Date	Comment
October 2008(initial version)	First version ...

2 Introduction

The present document provides details on:

- o Specification, design and implementation of the portal supporting remote interoperability tests events on XAdES specification. This includes an overview of the contents of the portal as well as the on-line PKI-related services provided to its users.
- o The remote plugtest event on XAdES organized by ETSI and held from Monday 8th to Thursday 18th September 2008.

The present document is organized as indicated below.

Section 3 provides details on how the portal is organized and the kind of services it provides to the participants of the plugtest events.

Section 4 lists the participants to the September 2008 XAdES remote interoperability plugtest event.

Section 5 provides an overview of the most interesting results and conclusions of the plugtest.

Section 6 provides details on a number of issues related to the XAdES specification as identified by the participants. These issues will be sent to the ESI TC for this to take into consideration for future XAdES standardization activities.

Finally section 7 shows the interoperability matrixes for the test-cases that were defined for the plugtest event.

3 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. Details on the contents of each part are provided below.

3.1 Public part of the portal

The public part of the portal may be reached at this address

The public part of the portal includes the following pages:

- o The XAdES Plugtest page, providing some more details on the September 2008 plugtest itself, namely targeted specification, targeted audience, etc.
- o The XAdES/CAAdES Plugtest page, providing some more details on the February 2009 plugtest including interoperability tests on both XAdES and CAAdES.
- o The Mailing List page, providing some details on participants' mailing list support provided by the portal for facilitating exchange of information during the plugtest.
- o The Registration page, providing details on the plugtest registration process.
- o The Login to Plugtest Area page, access to the protected area of the portal.

3.2 Private part of the portal

This part is visible only for the participants of the plugtest event. It includes a number of pages whose contents are detailed in the following sections.

3.2.1 Participants list page

The Participants' List page lists the details of all the participants of the plugtest, including contact details.

3.2.2 Meeting Support page

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

- o Calendar for the meetings (conference calls).
- o Dialing details for the phone bridge.
- o URL for accessing a chat server accessible through a Web browser where the calls were muted and participants could write their comments, questions and statements.
- o The agenda for each meeting.
- o Links to the minutes of each meeting.

3.2.3 Conducting plugtest information pages

The Conducting Plugtest page is the first of a set of four pages providing detailed explanations on how to conduct interoperability tests during the plugtest.

This first page details the two types of interoperability tests provided at this plugtest:

- o Generation and cross-verification tests. 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.
- o Only-verification tests. ETSI has generated a number of invalid XAdES signatures (the so-called "negative testcases") by different reasons. Each participant may, at her own discretion, try to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.

It also provides high level description of the steps that participants must perform for conducting the two different types of interoperability tests aforementioned.

The rest of pages of the set provide details on:

- o How to download material from the portal for starting conducting the plugtest (Downloading material page).
- o How to generate XAdES signatures and uploading them to the portal so that the rest of participants may download and verify them (Generating Signatures page).
- o How to verify other participants' signatures, report on verification results and uploading of these reports to the portal so that the portal keeps track of the current status of the plugtest (Verifying Signatures page).

3.2.4 Known issues page

The Known Issues page lists all the different issues that were raised during the event. These issues were classified in two groups, namely:

- o Issues that are related to the the plugtest itself (test cases definitions, restrictions, portal infrastructures, etc).
- o Issues related to the specification, which may impact further standardization activities.
- o Issues related to both the plugtest itself and to the specification.

3.2.5 Cryptographic material pages

The Cryptographic Material page is the first one of a set of three 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. Finally, a Time-stamping Authority was also deployed able to generate time-stamp tokens on request by the participants.

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 exists for being used in some of the only-verification test cases.

3.2.6 Presentations pages

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

- o A presentation on the ETSI ESI TC , the body in charge of standardizing XAdES.
- o A presentation on the history of XAdES , which includes details on the different published versions.
- o An Introductory Presentation for the newcomers to the plugtest, presenting the plugtest concept. The STF-351 team organized an introductory meeting before the official start of the plugtest, so that the newcomers to the plugtest could prepare themselves for participating in the plugtest.
- o An Orientation Presentation of the plugtest itself, which was made available before the start of the plugtest, where the participants were given the most relevant information on the event, including rules to be followed, etc

3.2.7 Former XAdES plugtests page

The Past Events page that include links to the final reports of the two face-to-face former XAdES interoperability plugtest events organized by ETSI and also of the first a remote XAdES plugtest event organized also by ETSI on March 2008.

3.2.8 Testcases definition language page

This page contains a document specifying a XML language for defining a test case. Such a language specifies what XAdES properties have to be included in the to-be-generated XAdES signatures and which values they must be given when required. This language has two advantages:

- o Participants may build processors of such a language on their application and then they are sure that the signatures generated will actually correspond to the requirements established in each test case.

- o Designers of the portal may make usage of latest XML technologies for building up a html document containing textual and tabular details of the different test cases.

3.2.9 Testcases page

This is a page containing a document with the complete specification of the test cases. This is a document that incorporates XSLT and javascript technologies. These technologies allow:

- o To browse the aforementioned test definition documents and build pieces of text and tables corresponding to each test case within this document.
- o To browse reports of verification (simple XML documents) of each single XAdES signature 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.

3.2.10 Download page

The Downlad page is used by the participants for downloading the initial package (cryptographic material, test-definition files, some initial signatures) and the latest version of the whole material generated by the participants at each instant of the plugtest (including both XAdES signatures and verification reports generated by all the participants).

3.2.11 Upload page

The Upload page provides mechanisms for uploading new signatures, new verification reports or both. Once uploaded, the portal re-builds a new downloading package and makes it available for all the participants at the Dowload page. Within this package, they will find all the signatures and verification reports generated up to that instant in the plugtest.

3.2.12 Online PKI services details

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.

3.2.13 Online PKI services accesls

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 an

the corresponding end-entity certificate for generating signatures, connection details for accessing the LDAP server where CRLs and CA certificates are stored, etc.

3.2.14 Online TSA services accesls

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

3.2.15 Mailing List Archives

The Mailing List Archives page archives all the email messages exchanged by the participants during the plugtest through the supporting e-mail list provided by the plugtest portal.

3.2.16 Chat

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.

4 Plugtest participants

There have been 28 different organizations and 29 persons registered in the event. With the addition of two persons from ETSI, this makes a total of 31 persons involved in the daily activities of the event.

The table below shows the list of some of the participants that have given permission for being listed in the present report:

Company	Acronym
Intervencion General de la Administracion del Estado (IGAE)	IGAE
Albalia Interactiva	AI
A-SIT (IAIK) - Austria	IAIK
Dictao S.A.	DIC
Entrust Japan Co., Ltd.	ENT
Polysys	PS
SAFELAYER Secure Communications S.A.	SL
Universitat Politècnica de Catalunya	UPC

Participants in the interoperability matrixes are anonymized (they are denoted by P1, P2, and so on), except those ones that have an acronym assigned in the table above.

5 Plugtest conclusions

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

5.1 General conclusions

This second remote plugtest event on XAdES has confirmed the usefulness of the of remote remote plugtests concept in different aspects:

- o The possibility of remote participation, including low participation cost, have lead to a much higher number of participants than in the former face-to-face plugtest events conducted before.
- 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.
 - o Phone bridge is crucial for having a number of meetins during the plugtest where participants may discuss specific issues of the plugtest and even on the standardization of the specifications.
 - o 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 plugtest: participants have asked questions, raised comments on the plugtest 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 plugtest.
 - o 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 At this second remote XAdES plugtest event, new standardization issues have been raised that had not been raised in the former event. This list, which will be added to the former one and forwarded to the ESI TC committee constitutes by itself a major outcome of the plugtest: this proves that XAdES is being used and there are a number of maintenance changes that the standardization process must take care of.
- o The remote but yet continous contact among participants lead to maintain interesting technical discussions on XAdES and related topics.

5.2 Lessons Learned

After organizing and conducting this second plugtest, the organizing team has learnt some very valuable lessons for the future:

- o After the first remote plugtest, the organizing team identified the suitability that participants were given introductory information on the portal and the plugtest participation rules before the official start of the plugtest. At this second plugtest, an introductory meeting took place on Wednesday 3rd of September, the week before the start of the plugtest. The portal was then opened for allowing the participants to get used with the environment and practicing with the most relevant features. This meeting proved to be very useful as the participants could work in the interoperability tests tasks since the very official start of the plugtest.
- o Organizers took care of presenting the on-line PKI-related services provided by the portal, as well as the deployed Trust Framework in order to identify potential sources of conflict with applications from participants. It turned out that none of the participants had problems in supporting such a Trust Framework and in consequence in conducting the interoperability tests with the cryptographic material generated by the different services..
- o Again, although due to calendar restrictions by ETSI, the initial duration of the plugtest was one week, it was proved that this is a clearly short duration for this kind of events where people are not sitting one before the other for the whole day. The plugtest, in fact, lasted from Monday 8th to Thursday 18th September 2008. The next plugtest event, which will also include CADES within its scope, is scheduled to have a duration of two weeks.
- o Web-based tools have proved be very well accepted. The organizing team has taken this into account in the provision of access to certificates and CRLs generated by the CAs deployed in the portal.
- o As for the analysis of the results, although during the plugtest a relevant number of issues were identified in the exchanged signatures, which helped participants to improve their implementations, a complete analysis of all the situations where interoperability failed could not be conducted. A proposal for articulating such a study even after the conclusion of the plugtest could be interesting for maximizing the benefits of such events, but would require much more resources by the participants at the plugtests. Indeed the organizing team, as well as the participants did their best for, in the days that the plugtest lasted, identifying potential sources of interoperability failures and a number of them were solved.

5.3 Technical Conclusions

It has not been possible yet to make a detailed study of the interoperability matrix for each participant and extract general conclusions, like which ones seem to be the properties where the participants have experienced more problems to for verifying onther's signatures, the reasons why this happens, etc.

Hundreds of signatures and verification reports have been generated and exchanged through the portal. A number of interoperability issues were reported and solved during the plugtest but certainly not all, as the interoperability matrixes show.

Nevertheless, the participants, by conducting this plugtest 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 and interop matrixes, proceed further in their indagations on why certain results are not as they expected.

As for the organizers of the plugtest, at this stage, only a statistical analysis may be carried out, providing the final figures of signatures produced, signatures verified, number of correct results, number of non correct results, etc. A deep analysis of each failure, its reasons and its impact is out of the scope of the present report.

6 Feedback to standardization process

A number of issues affecting XAdES specification contents were raised during the plugtest. These issues will be incorporated in the XAdES Interim Maintenance List, circulated to the ESI TC and cause the production of the corresponding disposition of comments and potential changes in the XAdES specifion.

The sections below summarize these issues

6.1 Check of time indication in xades:SigningTime property with regards to time indications within time-stamp tokens

According to the specification "all the times indicated by the time-stamp tokens in the property are posterior to the one indicated in the SigningTime property". This may bring problems when the time accuracy of the equipment where the siganture is generated is not good enough.

6.2 MimeType and Encoding attributes in xades:DataObjectFormat and ds:Object

This issue complements the issue [24] of first remote XAdES Plugtest Event, March 2008. At that plugtest some ds:Object elements had missing MimeType and Encoding attributes, whereas the corresponding xades:DataObjectFormat had them, and some participants accepted those signatures. At the present plugtest there are some signatures where it happens that the ds:Object contains some MimeType and/or Encoding attribute and that some of them are missing in the xades:DataObjectFormat.

6.3 xades:CompleteCertificateReferences and not CA certificate references

The proposal was raised for modifying XAdES spec for allowing the incorporation of a reference to the signing certificate within xades:CompleteCertificateRefs property. .

6.4 Dealing with empty elements

The XAdES XML schema actually allows that certain XAdES properties are empty. Some discussions took place on how to behave before those situations.

6.5 XAdES Forms and extra information

Some of the participants generated XAdES signatures consisting in a repertoire of properties corresponding to a specific XAdES form PLUS other complementary XAdES properties. The overall set of properties did not actually match any pre-defined XAdES form. Discussions took place on how an application should behave in these situations. Additional guidance on this aspect should be provided in the specification.

6.6 Computation of the digest of a Signature Policy document aligned with ETSI TR 102038 or ETSI TR 102272

Some considerations were raised during the plugtest on the way the digest of a Signature Policy definition document aligned with ETSI TR 102038 or ETSI TR 102272. The next version of XAdES should clarify the process for computing such a digest.

7 Interoperability matrixes

The following sub-sections contain the interop matrixes resulting from conducting the plugtest. No details are provided here on the test cases corresponding to each interop matrix. These may be found at the test cases definition document produced by the organizers of the plugtest, which may be found at the private pages of the portal. Rows in the tables correspond to verifiers. Columns in the tables correspond to signers. In consequence each cell in the tables reports the result of the verification of a signature generated by the participant indicated in the first cell of the column, carried out by the participant indicated in the first cell of the row.

Mark V appears in cells of green colour and stand for those signatures generated by one participant that have been successfully verified by another participant.

Mark F appears in cells of red colour and stand for those signatures generated by one participant and whose verification by another participant has failed. It is out of the scope of this report, however, to conclude whether the signer or the verifier does not respect the standard in these cases.

Each sub-section provides a number of interoperability matrixes for each XAdES form.

7.1 Test cases for XAdES-BES form.

X-BES-1.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P2	P7	P6	P11	P9	SL	P12	IAIKENT	P3	P8	DIC
P10	V	NA	NA	NA	V	NA	NA	F	NA	V	V	NA	NA	NA	NA	NA	NA

	P10	P5	P1	AI	PS	UPC	P2	P7	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8	DIC
P5	V	V	V	V	V	V	V	N	V	V	V	V	V	V	V	V	V	N
	V	V	V	N	V	V	V	N	N	V	V	V	V	V	V	V	V	N
AI	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
PS	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
P2	N	N	N	N	N	N	V	N	N	N	N	N	N	N	N	N	N	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	V	V	V	V	NA	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	F	V	F	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
IAIK	V	V	V	V	V	V	V	I	V	V	V	V	V	V	V	V	V	N
ENT	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
P8	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	N	V	N	V	V	V	V	V	V	V	V

X-BES-2.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P2	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8	DIC
P10	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P5	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	N	V	V	V	N	V	V	V	V	V	V	V	V	N
AI	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
PS	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P2	N	N	N	N	N	N	V	N	N	N	N	N	N	N	N	N	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
IAIK	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
ENT	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
P8	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	N	V	V	V	V	V	V	V	V

X-BES-3.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P7	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8	DIC
P10	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
P5	V	V	V	V	V	V	N	V	V	V	V	V	V	V	V	V	N
	V	V	V	N	V	V	N	N	V	V	V	V	V	V	V	V	N
AI	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
PS	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	V	V	V	NA	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	F	V	F	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
IAIK	V	V	I	V	V	V	I	V	V	V	V	V	V	V	V	V	N
ENT	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	N
P8	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	N	V	N	V	V	V	V	V	V	V	V

X-BES-4.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P6	P9	SL	P12	IAIK	ENT	P8
P10	V	V	V	V	V	F	V	V	V	V	V	V	V
P5	N	V	V	N	N	N	V	V	N	V	V	N	N
	V	V	V	N	V	N	N	V	V	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	F	V	V	V	V	V	V	V
IAIK	V	V	I	V	V	I	V	V	V	V	V	I	V
ENT	V	V	V	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V	V
P8	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V	V	V	V

X-BES-5.xml

And results in the following Interop Matrix:

	P5	AI	UPC	P6	P11	P9	P12	IAIK	ENT	P8
P5	V	V	N	V	N	N	N	V	N	N
	V	N	F	N	V	N	V	V	N	N
AI	V	V	V	V	V	F	V	V	F	F
PS	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	NA	F	V	V	V	V	V
P12	V	V	F	V	V	F	V	V	V	V
IAIK	V	V	I	V	I	I	V	V	I	I
ENT	F	F	F	F	F	V	F	F	V	V
P8	V	V	V	V	NA	V	V	V	V	V
DIC	V	V	V	V	N	V	V	V	V	V

X-BES-6.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P6	P9	SL	P12	IAIK	ENT	P3	P8
P10	V	V	V	V	V	V	NA	V	V	V	V	V	V	V
P5	V	V	V	V	V	V	V	V	V	V	V	N	V	V
	N	V	V	N	V	V	N	N	N	N	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V	F
	V	V	V	V	V	V	V	V	V	V	V	V	V	NA
P9	V	V	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	V	V	V	V	V	V	V	V	V
IAIK	V	V	I	V	V	V	I	V	V	V	V	I	V	V
ENT	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V	V	F
P8	V	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V	V	N	V	V

X-BES-7.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P9	SL	P12	IAIK	ENT	P3	P8
P10	V	V	V	V	V	V	V	V	V	V	F	V	V
P5	V	V	V	V	V	V	V	V	V	V	V	V	V
	N	V	V	N	N	V	N	N	N	V	V	V	N
AI	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	F	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	NA	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	V	F	V	V	V	V	V	V	V	V	V	V
IAIK	V	V	I	V	V	V	V	V	V	V	I	V	V
ENT	V	V	V	V	V	V	V	V	V	V	V	V	V
P3	V	V	V	V	V	V	V	V	V	V	V	V	V
P8	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V	V	V	V

X-BES-8.xml

And results in the following Interop Matrix:

	P10	P1	AI	PS	UPC	P6	P9	SL	P12	IAIK	ENT	P3	P8
P10	V	V	V	V	V	F	V	V	V	V	V	V	V
	N	V	N	V	V	N	N	N	N	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	F	V	V	V	V	V	V	V
IAIK	V	V	V	V	V	I	V	V	I	V	I	V	V
ENT	V	V	V	V	V	V	V	V	V	V	V	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V	V
P8	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V	V	V	V

X-BES-9.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3
P10	V	V	V	V	V	NA	V	V	V	V	V	V
P5	N	V	V	V	V	V	V	V	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	F	V	V	V	V	V
P12	V	V	F	V	V	V	V	V	V	F	V	V
IAIK	V	V	V	V	V	I	V	V	V	V	I	V
ENT	V	V	F	V	V	F	F	V	V	V	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	V	V	V	V	V	N	V	V	V	V	V

X-BES-10.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT
P10	V	V	V	V	V	V	V	V	V	V	V
P5	N	V	V	V	V	N	V	V	V	V	V
	N	V	N	V	V	N	V	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	F	V	V	V	V	V
SL	V	V	V	V	V	V	F	V	V	V	V
P12	F	V	F	V	V	F	V	V	V	F	V
IAIK	N	V	V	V	V	F	V	V	V	V	I
ENT	V	V	F	V	V	F	F	V	V	F	V
P3	F	V	V	V	V	V	V	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	V	V	V	V	V	N	V	V	V	V

X-BES-11.xml

And results in the following Interop Matrix:

	P10	AI	PS	UPC	P9	SL	IAIK	ENT	P3	P8
P10	N	NA	N	N	N	N	N	N	V	N
	N	N	N	N	V	N	N	N	N	N
AI	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	F	V	V	V	V	F
UPC	V	V	V	V	V	V	V	V	V	F
	V	V	V	V	V	V	V	V	V	V
	V	V	V	F	F	V	F	V	V	NA
P9	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	NA	V	V	V	V	F
P12	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
IAIK	V	I	V	V	V	I	V	I	V	F
ENT	V	F	V	V	V	NA	V	V	V	V
P3	F	V	V	F	F	V	F	V	V	F
P8	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	N	V	V	V	V	N

X-BES-15.xml

And results in the following Interop Matrix:

	P10	AI	PS	UPC	P6	P9	P12	IAIK	ENT	P3
P10	V	V	V	F	NA	F	V	V	F	NA
AI	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	F	V
UPC	V	V	V	V	V	V	V	V	F	V
	V	V	V	V	V	V	V	V	V	V
	NA	NA	NA	NA	NA	NA	NA	NA	NA	V
P9	V	V	V	V	F	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V
P12	V	F	V	F	F	F	V	F	V	F
IAIK	V	V	V	I	F	I	I	V	F	I
ENT	V	F	V	V	V	V	V	F	V	V
P3	F	V	V	V	V	V	V	V	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	V	V	V	V	V	V	V	V	V

7.2 Test cases for the XAdES-EPES form.

X-EPES-1.xml

And results in the following Interop Matrix:

	P10	P1	AI	PS	UPC	P9	SL	P12	IAIK	ENT	P3	P8
P10	V	F	F	F	F	V	F	F	F	F	F	F
P5	V	N	N	V	N	N	V	V	N	V	N	V
	V	V	N	V	V	V	N	V	V	V	N	V
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	F	NA	NA	V	NA	NA	NA	V	NA	V	V	F
UPC	V	V	V	V	V	F	V	V	V	V	F	F
	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
P9	V	V	F	F	F	V	V	F	F	F	F	V
SL	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	F	F	V	V	F	V	V	V	V	V	V
IAIK	V	I	I	V	V	F	I	I	V	V	V	V
ENT	V	F	V	V	V	F	V	V	V	V	V	V
P3	F	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
P8	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V	V	V

X-EPES-2.xml

And results in the following Interop Matrix:

	P10	P1	AI	UPC	P9	SL	P12	IAIK	ENT	P8
P10	V	F	F	F	F	F	F	F	F	F
P5	V	N	N	V	N	V	V	V	V	V
	N	V	N	N	N	N	N	V	V	N
AI	V	V	V	V	F	V	V	V	F	F
UPC	V	V	V	V	F	V	V	V	F	F
	V	V	V	V	F	V	V	V	NA	V
P9	V	V	F	F	V	V	F	F	F	V
SL	V	V	V	V	V	V	V	V	V	V
P12	V	F	F	F	F	F	V	V	V	V
IAIK	V	F	I	I	I	I	V	V	I	I
ENT	F	F	F	V	F	V	F	N	V	V
P8	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	V	V

7.3 Test cases for XAdES-T form.

X-T-1.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P2	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8	DIC
P10	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P5	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	N	V	V	V	N	V	V	V	V	V	V	V	V	N
AI	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
PS	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V	V
P2	N	N	N	N	N	N	V	N	N	N	N	N	N	N	N	N	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	F
SL	V	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	V
P12	V	V	V	V	V	V	V	V	F	F	V	V	V	V	F	V	N
IAIK	V	V	V	V	V	V	V	V	V	F	V	V	V	V	F	V	V
ENT	V	V	V	V	V	V	V	V	V	V	V	V	F	V	F	V	V
P3	F	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	N
P8	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
DIC	N	V	V	V	V	V	V	V	N	V	V	V	V	V	V	V	V

7.4 Test cases for XAdES-C form.

X-C-1.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P2	P7	P6	P11	P9	SL	P12	IAIK	ENT	P13	P3
P10	V	F	F	V	V	V	V	F	F	V	F	F	F	V	V	NA	F
P5	N	V	V	V	V	V	V	N	V	V	V	V	V	V	V	N	V
	N	V	V	N	V	V	V	N	N	V	V	V	V	V	V	N	V
AI	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
PS	V	F	F	V	V	V	V	F	V	V	V	F	F	V	V	F	V
UPC	V	F	F	F	V	V	V	F	F	V	F	F	F	V	V	F	V
P2	N	N	N	N	N	N	V	N	N	N	N	N	N	N	N	N	N
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
	NA	V	V	V	V	V	V	NA	V	V	V	V	V	V	V	NA	V
P9	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
SL	V	V	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
P12	F	F	V	F	V	V	V	F	F	V	F	F	V	V	V	F	F
IAIK	I	F	F	F	V	V	V	I	V	V	F	F	V	V	V	I	F
ENT	V	V	V	V	V	V	V	F	V	V	V	V	V	F	V	F	F
P3	F	V	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	V	V	N	N	N	V	N	V	N	V	V	N	N	V	N	V

X-C-2.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P7	P6	P11	P9	SL	P12	IAIK	ENT	P13	P3
P10	V	F	V	V	V	F	F	F	F	F	F	V	V	NA	F
P5	N	V	V	V	V	N	V	V	V	V	V	V	V	N	V
	N	V	N	V	V	N	N	N	V	V	V	V	N	N	V
AI	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
PS	V	F	V	V	V	F	F	N	F	F	F	V	V	F	V
UPC	V	F	F	V	V	F	F	V	F	F	F	V	V	F	V
	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
	NA	NA	V	V	V	NA	V	V	NA	V	V	NA	V	NA	V
P9	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
SL	V	V	V	V	V	F	V	V	V	V	V	V	V	F	V
P12	F	F	F	V	V	F	F	V	F	F	V	V	V	F	F
IAIK	I	F	F	V	V	I	F	V	F	F	F	V	V	I	F
ENT	V	V	V	V	V	F	V	F	V	V	V	V	V	F	F
P3	F	V	V	V	V	F	V	V	V	V	V	V	V	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	V	N	N	N	N	N	N	N	V	N	N	V	N	V

7.5 Test cases for XAdES-X form.

X-X-1.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P13	P3	DIC
P10	V	F	V	V	V	F	V	F	F	V	V	NA	F	F
P5	V	V	V	V	V	V	V	N	V	V	V	N	V	N
	V	V	N	V	V	N	V	V	V	V	V	N	V	N
AI	V	V	V	V	V	V	V	V	V	V	V	F	V	N
PS	V	F	V	V	V	V	V	V	F	V	V	F	V	N
UPC	V	F	F	V	V	F	V	F	F	V	V	F	V	F
	F	V	V	V	V	V	V	V	V	F	V	V	V	V
	NA	V	V	V	V	V	V	V	V	V	V	NA	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	F	V	F
P12	V	F	F	V	V	F	V	F	V	V	V	F	V	N
IAIK	V	F	F	V	V	V	V	F	F	V	V	I	V	F
ENT	V	V	F	V	V	V	V	V	V	F	V	F	V	V
P3	F	F	F	V	V	V	V	F	V	V	V	F	V	N

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P13	P3	DIC
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	V	N	V	N	N	V	N	N	V

X-X-2.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P2	P6	P11	P9	P12	IAIK	ENT	P3
P10	V	F	F	V	V	V	V	F	V	F	F	V	V	F
P5	V	V	N	V	V	V	V	V	V	V	V	V	V	V
	V	V	V	N	V	V	V	N	V	V	V	V	V	V
AI	V	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	F	F	V	V	V	V	V	V	V	F	V	V	V
UPC	V	F	F	F	V	V	V	F	V	F	F	V	V	V
P2	N	N	N	N	N	N	V	N	N	N	N	N	N	N
	F	V	F	V	V	V	V	V	V	V	V	F	V	V
	NA	V	NA	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	F	F	F	V	V	V	F	V	F	V	V	V	F
IAIK	V	F	F	F	V	V	V	V	V	F	F	V	V	F
ENT	V	V	F	F	V	V	V	V	V	V	V	F	V	F
P3	F	F	F	F	V	V	V	F	V	F	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	V	V	N	V	N	N	V	N

X-X-3.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P13	P3
P10	V	F	V	V	V	F	F	F	F	V	V	NA	F
P5	V	V	V	V	V	V	V	V	V	V	V	N	V
	V	V	N	V	V	N	N	V	V	V	N	N	V
AI	V	V	V	V	V	V	V	V	V	V	V	F	V
PS	V	F	N	V	V	F	N	F	F	V	V	F	V
UPC	V	F	F	V	V	F	V	F	F	V	V	F	V
	F	V	V	V	V	V	V	V	V	F	V	V	V
	NA	NA	V	V	V	V	V	NA	V	NA	V	NA	V
P9	V	V	V	V	V	V	V	V	V	V	V	F	V
P12	V	F	F	V	V	F	V	F	V	V	V	F	V
IAIK	V	F	F	V	V	F	V	F	F	V	V	I	V
ENT	V	V	F	V	V	V	F	V	V	F	V	F	V

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P13	P3
P3	F	F	F	V	F	V	F	F	V	F	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	N	N	N	N	V	N	N

X-X-4.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3
P10	V	F	V	V	V	F	F	F	F	V	V	F
P5	V	V	V	V	V	V	V	N	V	V	V	V
	V	V	N	V	V	N	N	V	V	V	N	V
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	F	N	V	V	F	N	F	F	V	V	V
UPC	V	F	F	V	V	F	V	F	F	V	V	V
	F	V	V	V	V	V	V	V	V	F	V	V
	NA	NA	V	V	V	V	V	NA	V	NA	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V
P12	V	F	F	V	V	F	V	F	V	V	V	F
IAIK	V	F	F	V	V	F	V	F	F	V	V	F
ENT	V	V	F	V	V	V	F	V	V	F	V	F
P3	F	F	F	V	V	F	V	F	V	V	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	N	N	N	N	V	N

7.6 Test cases for XAdES-XL form.

X-XL-1.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P7	P6	P11	P9	SL	P12	IAIK	ENT	P3
P10	V	V	V	V	V	F	V	V	V	V	V	V	V	F
P5	V	V	V	V	V	N	V	V	N	V	V	V	V	N
	V	V	N	N	V	N	N	V	V	V	V	V	V	N
AI	V	V	V	V	V	F	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	F	V	V	V	V	V	V	V	V
UPC	V	V	V	V	V	F	F	V	V	V	V	V	V	V
	F	V	V	V	V	V	V	V	V	V	V	F	V	V
	V	V	V	V	V	NA	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	F	V	V	V	V	V	V	V	V

	P10	P5	AI	PS	UPC	P7	P6	P11	P9	SL	P12	IAIK	ENT	P3
SL	V	V	V	V	V	F	V	V	V	V	V	V	V	F
P12	V	V	F	V	V	F	V	V	F	V	V	V	V	V
IAIK	V	F	F	V	F	I	V	V	F	F	F	V	F	V
ENT	V	V	F	V	V	F	V	V	V	V	V	F	V	V
P3	F	V	F	V	V	F	F	V	V	V	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	V	V	V	N	V	V	V	V	V	V	V	N

X-XL-2.xml

And results in the following Interop Matrix:

	P10	P5	P1	AI	PS	UPC	P7	P6	P11	P9	P12	IAIK	ENT	P3
P10	V	V	V	V	V	V	F	V	V	V	V	V	V	F
P5	V	V	N	V	V	V	N	V	V	V	V	V	V	N
	V	V	V	N	N	V	N	N	V	V	V	V	V	N
AI	V	V	V	V	V	V	F	V	V	V	V	V	V	V
PS	V	V	N	V	V	V	F	V	V	V	V	V	V	V
UPC	V	V	F	V	V	V	F	F	V	V	V	V	V	V
	F	V	F	V	V	V	V	V	V	V	V	F	V	V
	V	V	NA	V	V	V	NA	V	V	V	V	V	V	V
P9	V	V	F	V	V	V	F	V	V	V	V	V	V	V
P12	V	V	F	F	V	V	F	V	V	F	V	V	V	V
IAIK	V	F	F	F	V	F	I	V	V	F	F	V	F	V
ENT	V	V	F	F	V	V	F	V	V	V	V	F	V	V
P3	F	V	F	F	V	V	F	F	V	V	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	V	V	V	N	V	V	V	V	V	V	N

X-XL-3.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P13	P3
P10	V	V	F	V	V	V	V	V	V	V	V	V	NA	F
P5	V	V	V	V	V	V	V	V	V	V	V	V	N	N
	N	NA	N	N	NA	N	N	N	NA	N	NA	N	N	N
AI	V	V	V	V	V	V	V	V	V	V	V	V	F	V
PS	V	N	N	V	V	V	V	N	V	V	V	V	F	V
UPC	V	V	F	V	V	F	V	V	V	V	V	V	F	V

	P10	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P13	P3
	F	V	F	V	V	V	V	V	V	V	F	V	V	V
	V	V	V	V	V	V	V	V	V	V	V	V	NA	V
P9	V	V	F	V	V	V	V	V	V	V	V	V	F	V
SL	V	V	V	V	V	V	V	V	V	V	V	V	F	F
P12	V	V	F	V	V	V	V	F	V	V	V	V	F	F
IAIK	V	F	F	V	F	F	V	F	F	F	V	F	I	F
ENT	V	V	F	V	V	V	V	V	V	V	F	V	F	F
P13	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	V	NA
P3	F	F	F	V	F	V	F	F	V	V	F	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	N	N	N	N	N	V	N	N

X-XL-4.xml

And results in the following Interop Matrix:

	P10	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3
P10	V	V	F	V	V	V	V	V	V	V	V	F
P5	V	V	V	V	V	V	V	N	V	V	V	N
	N	NA	N	N	NA	N	N	N	N	NA	N	N
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	N	V	V	V	V	V	N	V	V	V	V
UPC	V	V	F	V	V	F	V	V	V	V	V	V
	F	V	F	V	V	V	V	V	V	F	V	V
	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	F	V	V	V	V	V	V	V	V	V
P12	V	V	F	V	V	V	V	F	V	V	V	V
IAIK	V	F	F	V	F	F	V	F	F	V	F	V
ENT	V	V	F	V	V	V	V	V	V	F	V	V
P3	F	V	F	V	V	F	V	F	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	N	N	N	N	V	N

7.7 Test cases for XAdES-A form.

X-A-1.xml

And results in the following Interop Matrix:

	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
P5	V	V	V	V	V	V	F	V	V	V	V	F

	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	N	V	V	V	V	V
UPC	V	V	V	V	F	V	V	V	V	V	V	V
	V	F	V	V	V	V	V	V	V	F	F	V
	V	NA	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	F
P12	V	F	V	V	V	V	V	V	V	V	V	F
IAIK	N	N	N	N	N	V	N	N	N	V	N	N
ENT	V	F	V	V	F	V	V	V	V	F	V	F
P3	V	F	V	V	F	V	V	V	V	V	V	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

X-A-2.xml

And results in the following Interop Matrix:

	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3	DIC
P5	V	V	V	V	V	V	V	V	V	V	N	N
AI	V	V	V	V	V	V	V	V	V	V	V	N
PS	V	V	V	V	V	V	N	V	V	V	V	V
UPC	V	V	V	V	F	V	V	V	V	V	V	F
	V	V	V	V	V	V	V	V	F	F	V	F
	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	N
P12	V	F	V	V	V	V	V	V	V	V	F	N
IAIK	N	N	N	N	N	V	N	N	V	N	N	N
ENT	V	F	V	V	F	V	V	V	F	V	V	N
P3	V	F	V	V	F	V	V	V	V	V	V	N
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
DIC	N	N	N	N	N	N	N	N	N	N	N	V

X-A-3.xml

And results in the following Interop Matrix:

	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
P5	V	V	V	V	V	V	V	V	V	V	V	N
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	V	F	V	V	V	V	V
UPC	V	F	V	V	F	V	V	V	V	V	V	V

	P5	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
	V	F	V	V	V	V	V	V	V	F	F	V
	V	NA	V	V	V	V	V	V	V	V	V	V
P9	V	F	V	V	V	F	V	V	V	V	V	V
SL	F	F	V	F	F	V	F	V	V	F	F	F
P12	V	F	V	V	V	V	F	V	V	V	V	F
IAIK	N	N	N	N	N	V	N	N	N	V	N	N
ENT	V	F	V	V	F	V	V	V	V	F	V	F
P3	F	F	V	F	V	F	F	V	V	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

X-A-4.xml

And results in the following Interop Matrix:

	P5	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3
P5	V	V	V	V	V	V	F	V	V	V	N
AI	V	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	V	F	V	V	V	V
UPC	V	F	V	V	F	V	V	V	V	V	F
	V	F	V	V	V	V	V	V	F	F	F
	V	V	V	V	V	V	V	V	V	V	V
P9	V	F	V	V	V	F	V	V	V	V	F
P12	V	F	V	V	V	V	F	V	V	V	F
IAIK	N	N	N	N	N	V	N	N	V	N	N
ENT	V	F	V	V	F	V	V	V	F	V	F
P3	F	F	V	F	V	V	F	V	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

X-A-5.xml

And results in the following Interop Matrix:

	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
AI	V	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	F	V	V	V	V	V
UPC	F	V	V	F	V	V	V	V	V	V	F
	V	V	V	V	V	V	V	V	F	F	F
	V	V	V	V	V	V	V	V	V	V	V
P9	F	V	V	V	F	V	V	V	V	V	F
SL	F	F	F	F	F	F	V	V	F	F	F
P12	F	V	V	V	V	F	V	V	V	V	F
IAIK	N	N	N	N	V	N	N	N	V	N	N

	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
ENT	F	V	V	F	V	V	V	V	F	V	F
P3	F	V	F	V	F	F	V	V	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

X-A-6.xml

And results in the following Interop Matrix:

	AI	PS	UPC	P6	P11	P9	P12	IAIK	ENT	P3
AI	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	F	V	V	V	V
UPC	F	V	V	F	V	V	V	V	V	V
	V	V	V	V	V	V	V	F	F	V
	V	V	V	V	V	V	V	V	V	V
P9	F	V	V	V	F	V	V	V	V	V
P12	F	V	V	V	V	F	V	V	V	V
IAIK	N	N	N	N	V	N	N	V	N	N
ENT	F	V	V	F	V	V	V	F	V	F
P3	F	V	F	V	F	F	V	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

X-A-7.xml

And results in the following Interop Matrix:

	P15	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8
P15	V	V	F	V	NA	F	V	F	V	V	V	F	V
AI	V	V	V	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	V	V	V	V	V	V	V	V
UPC	F	V	V	V	F	V	V	V	V	V	V	V	V
	F	V	V	V	V	V	V	V	V	F	F	V	V
	NA	V	V	V	V	V	V	V	V	V	V	V	V
P9	F	V	V	V	V	V	V	V	V	V	V	V	V
SL	V	V	V	V	V	V	V	V	V	V	V	F	V
P12	F	V	V	V	V	V	V	V	V	V	V	F	V
IAIK	N	N	N	N	N	V	N	N	N	V	N	N	N
ENT	V	V	V	V	F	V	V	V	V	F	V	F	V
P3	V	V	V	V	V	V	V	V	V	V	V	V	V
P8	V	V	V	V	V	V	V	V	V	V	V	F	V
DIC	N	N	N	N	N	N	N	N	V	N	N	N	V

X-A-8.xml

And results in the following Interop Matrix:

	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3	P8
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	V	V	V	V	V	V	V	V	V	V	V	V
UPC	V	V	V	F	V	V	V	V	V	V	V	V
	V	V	V	V	V	V	V	V	F	F	V	V
	V	V	V	V	V	V	V	V	V	V	V	V
P9	V	V	V	V	V	V	V	V	V	V	V	V
SL	F	F	F	F	F	V	V	V	F	F	F	V
P12	F	V	V	V	V	V	V	V	V	V	V	V
IAIK	N	N	N	N	V	N	N	N	V	N	N	N
ENT	V	V	V	F	V	V	V	V	F	V	V	V
P3	V	F	F	V	F	V	V	V	V	V	V	V
P8	V	V	V	V	V	V	V	V	V	V	F	V
DIC	N	N	N	N	N	N	N	V	N	N	N	V

X-A-9.xml

And results in the following Interop Matrix:

	P15	AI	PS	UPC	P6	P11	P9	SL	P12	IAIK	ENT	P3
P15	V	V	F	V	NA	F	V	F	V	V	V	F
AI	V	V	V	V	V	V	V	V	V	V	V	V
PS	F	V	V	V	V	V	V	V	V	V	V	N
UPC	F	V	V	V	F	V	V	V	V	V	V	V
	F	V	V	V	V	V	V	V	V	F	F	V
	NA	V	V	V	V	V	V	V	V	V	V	V
P9	F	V	V	V	V	V	V	V	V	V	V	V
SL	V	F	V	F	F	F	F	V	V	F	F	F
P12	F	V	V	V	V	V	V	V	V	V	V	F
IAIK	N	N	N	N	N	V	N	N	N	V	N	N
ENT	N	V	V	V	F	V	V	V	V	F	V	F
P3	V	F	V	F	V	F	F	V	V	F	F	V
P8	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

8 Interoperability matrixes for negative test cases(verification only)

The following section contains negative test cases grouped by XAdES Form.

Cells of interoperability matrixes in this section must be read as indicated below:

- o S:S. Success. The invalid signature was actually verified as invalid, as expected.
- o S:FA. Failure. The invalid signature was actually not verified as invalid.
- o S:NA. Not applicable. A participant did not consider worth to check this test case.

8.1 XAdES-BES form, negative test cases.

The test cases in this section deal with the XAdES-BES form. The following tests have at least one aspect that should cause verification to fail, you will not have to generate them (verification only).

X-BESN-1.xml contains the following Properties

- o SigningTime
- o DataObjectFormat

One xades:DataObjectFormat does not reference any ds:Reference in the signature

And results in the following Interop Matrix:

Signers #	Verifiers #
P10	S : N
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : S
DIC	S : FA

X-BESN-2.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o DataObjectFormat

A signature with a ds:Reference element referenced by a xades:DataObjectFormat refers to a ds:Object whose MimeType is not equal to the one in xades:DataObjectFormat

And results in the following Interop Matrix:

Signers # Verifiers #	
P10	S : N
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : S
DIC	S : FA

X-BESN-3.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o DataObjectFormat

A signature with a ds:Reference element referenced by a xades:DataObjectFormat refers to a ds:Object whose Encoding attribute is not equal to the one in xades:DataObjectFormat

And results in the following Interop Matrix:

Signers # Verifiers #	
P10	S : N
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : S
DIC	S : FA

8.2 XAdES-EPES form, negative test cases.

X-EPESN-1.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignaturePolicyIdentifier

>The digest within xades:SignaturePolicyIdentifier property does not correspond with the digest computed on the document referenced by xades:SPURI

And results in the following Interop Matrix:

Signers # Verifiers #	
P10	S : N
UPC	S : S
P11	S : NA
P9	S : S
P12	S : S
IAIK	S : I
ENT	S : S
P3	S : N
P8	S : NA
DIC	S : FA

8.3 XAdES-T form, negative test cases.

The test cases in this section deal with the XAdES-T form.

X-TN-1.xml contains the following Properties

- o SigningTime
- o SignatureTimeStamp

The time in xades:SignatureTimeStamp is ulterior to the expiration time of the signing certificate

And results in the following Interop Matrix:

Signers # Verifiers #	
P10	S : N
UPC	S : S
P11	S : S
SL	S : S

Signers # Verifiers #	
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : S

X-TN-2.xml contains the following Properties

- o SigningTime
- o SignatureTimeStamp

The time in xades:SignatureTimeStamp is ulterior to the revocation time of the signing certificate

And results in the following Interop Matrix:

Signers # Verifiers #	
P10	S : N
UPC	S : S
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : S

X-TN-3.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp

The time-stamp token within xades:SignatureTimeStamp is computed to not time-stamp the canonicalized ds:SignatureValue element but other object

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
ENT	S : S
P8	S : S

8.4 XAdES-X form, negative test cases.

The test cases in this section deal with the XAdES-X form.

X-XN-1.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o RefsOnlyTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:RefsOnlyTimeStamp

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XN-2.xml contains the following Properties

- o SigningTime

- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:SigAndRefsTimeStamp

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XN-3.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o RefsOnlyTimeStamp

The time-stamp token in xades:RefsOnlyTimeStamp does not time-stamp the canonicalized xades:CompleteCertificateRefs and xades:CompleteRevocationRefs.

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XN-4.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp

Time within xades:SignatureTimeStamp is ulterior to time within xades:SigAndRefsTimeStamp

And results in the following Interop Matrix:

Signers # Verifiers #
IAIK

8.5 XAdES-XL form, negative test cases.

The test cases in this section deal with the XAdES-XL form.

X-XLN-1.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs

- o RefsOnlyTimeStamp
- o CertificateValues
- o RevocationValues

A signature with a xades:CompleteRevocationRefs that contains a CRL reference whose IssueTime element is not equal to the thisUpdate field of the CRL identified by the Issuer and the crlNumber

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XLN-2.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o RefsOnlyTimeStamp
- o CertificateValues
- o RevocationValues

A signature with a xades:CompleteRevocationRefs that contains a CRL reference whose crlNumber element is not equal to the Number field of the CRL identified by the Issuer and the issueTime

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XLN-3.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o RefsOnlyTimeStamp
- o CertificateValues
- o RevocationValues

A signature with a xades:CompleteRevocationRefs that contains a CRL reference whose digest is not equal to the digest value computed on the CRL identified by the Issuer and the issueTime

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XLN-4.xml contains the following Properties

- o SigningTime

- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp
- o CertificateValues
- o RevocationValues

A signature with a xades:CompleteRevocationRefs that contains an OCSP resp reference whose responderID element contains a name that is not equal to the responderID field of any of the OCSP responses in CertificateValues property

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XLN-5.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp
- o CertificateValues

- o RevocationValues

xades:CompleteRevocationRefs contains an oCSP resp reference whose ProducedAt element is not equal to the producedAt field of the OCSP responses generated by responderID

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

X-XLN-6.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp
- o CertificateValues
- o RevocationValues

xades:CompleteRevocationRefs contains an oCSP resp reference whose digest element is not equal to the digest value computed on the OCSP response identified by the responderID and the ProducedAt elements

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S

Signers # Verifiers #	
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : S
P8	S : NA

8.6 XAdES-A form, negative test cases.

The test cases in this section deal with the XAdES-A form.

X-AN-1.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp
- o CertificateValues
- o RevocationValues
- o ArchiveTimeStamp

Time in xades:SignatureTimeStamp is ulterior to the time in xades:ArchiveTimeStamp

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S

Signers # Verifiers #	
ENT	S : S
P3	S : S
P8	S : NA

X-AN-2.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp
- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o RefsOnlyTimeStamp
- o CertificateValues
- o RevocationValues
- o ArchiveTimeStamp

Time in xades:RefsOnlyTimeStamp is ulterior to the time in xades:ArchiveTimeStamp

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : FA
P8	S : NA

X-AN-3.xml contains the following Properties

- o SigningTime
- o SigningCertificate
- o SignatureTimeStamp

- o CompleteCertificateRefs
- o CompleteRevocationRefs
- o SigAndRefsTimeStamp
- o CertificateValues
- o RevocationValues
- o ArchiveTimeStamp

Time within xades:SigAndRefsTimeStamp is ulterior to time within xades:ArchiveTimeStamp.

And results in the following Interop Matrix:

Signers # Verifiers #	
UPC	S : S
P11	S : S
P9	S : S
SL	S : S
P12	S : S
IAIK	S : S
ENT	S : S
P3	S : FA
P8	S : NA

9. References

XMLDSIG

XML-Signature Syntax and Processing. W3C Recommendation. Donald Eastlake, Joseph Reagle, David Solo. February 2002. <http://www.w3.org/TR/xmlsig-core/>

XAdES_v1.3.2

XML Advanced Electronic Signatures (XAdES). ETSI TS 101 903 V1.3.2 (2006-03) http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21353

A Author's Adress (Non-Normative)

o **Juan Carlos Cruellas Ibarz**

Universitat Politecnica de Catalunya (UPC). Departament de Arquitectura de Computadors (DAC)

c/ Jordi Girona 1-3, Modul D6.103, Barcelona. Spain

Phone: +34 93 4016790

Email: <cruellas@ac.upc.edu>

o **Konrad Lanz**

A-SIT.IAIK - Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie.
Graz University of Technology

Inffeldgasse 16a, 8010 Graz. Austria

Phone: +43 316 873 5547

Email: <Konrad.Lanz@iaik.tugraz.at>

o **Péter Krémer**

ETSI, 650 Route des Lucioles,06921,Sophia Antipolis cedex. France

Email: <Peter.Kremer@etsi.org>

o **Kenji Urushima**

Entrust Japan Co., Ltd

Email: <kenji.urushima@entrust.com>

o **Gregory Sun**

Macao Post eSignTrust Certification Services

Email: <gregsun@esigntrust.com">>