Security Interop Event 2004 — V0.2 (2003-12)

Guideline for an interoperability event in the security area

Reference

Security2004-V01

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

History

Document history		
Version	Date	Author - Comment
V0.1	11.12.2003	PETITJEAN Maeva – First draft
V0.2	12.12.2003	P.COUSIN review

Contents

History....3

Intellectual Property Rights....5

1. Introduction....6
1.1. Purpose of this document....6
1.2. Definition of a security interoperability event....6

2. Why a security interoperability event?....6

3. What do we propose for this interop? 7
3.1. XAdES 7
3.2. PKI 7
3.2.1. PKI interop structure....7
3.2.2. History 7
3.2.3. PKI interop at ETSI Plugtests....8
3.3. IPsec / IKEv2....9
3.4. Relation between the three technologies....9

4. Some actors already identified (non exhaustive list) 9
4.1. XAdES 9
4.2. PKI 10
4.3. IPsec / IKEv2....10

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

1. Introduction

The ETSI Interoperability service, called the Plugtests service, is organising interoperability events in a broad range of active technical areas. To date, the service has organised 40 interoperability events and has a plan to organise a minimum of 12 events per year (see more at www.etsi.org/plugtests) .

High market attention is paid today on the Security area that represents an important one where ETSI is involved through, amongst other the technical committee ESI (Electronic Signature and Infrastructure, see http://portal.etsi.org/esi/el-sign.asp). The Plugtests had a first experience in organising on November 2003, the first XAdES (XML Advanced Electronic Signature) interoperability event. In parallel to XadES, many interests where expressed to consider interoperability events for PKI and IPsec. As these topics are inter-related, the idea came up to explore the possibility to organise an interoperability event in 2004 on the overall Security theme which would include the three active topics of (Xad)Electronic Signature, PKI (Public Key Infrastructure) and IPsec (IP secure)

1.1. Purpose of this document

The goal of this document is to define the guideline for an interoperability event in the security area. This event would be organised by ETSI Plugtests in 2004 hopeful in the first half.

1.2. Definition of a security interoperability event

After the first XAdES interoperability event organised at ETSI Plugtests in November 2003, Plugtests plans to organise another interoperability event in the security area. The objective is to realise at the same time one or more interoperability events about the security protocols. This would give the opportunity to create an interaction between testers from different areas, and then increase the interoperability between the security technologies.

2. Why a security interoperability event?

The interest in regrouping such topics in the same event is to offer the opportunity to the participants to interact and exchange ideas. For example, during the last XAdES interop, the participants had to use simulated PKI. The fact to have PKI testers in the proximity during the XAdES tests would allow them to test their signatures with real PKI, and therefore to test their material in more realistic conditions.

The last XAdES interop was successful and should be renewed this year. But there is also an important interest in doing a PKI interoperability event. In fact, the interoperability is one of the most significant lacks in PKI and prevents their deployment in a larger scale. Moreover, this kind of interop has not yet been developed in Europe, whereas some PKI interops have already been done in Asia by JKST-IWG (Japan, Korea, China and Singapore).

3. What do we propose for this interop?

This interoperability event will be centred on the three technologies XAdES, PKI and IPsec/IKEv2.

3.1. XAdES

Since a XAdES event already occurred last year, the testers can run their own tests, but this time with real Certificate Authorities delivering real certificates in order to test their protocol. The fact to collaborate with PKI testers will allow them to do their tests in a better context and will decrease the risk of errors during the tests.

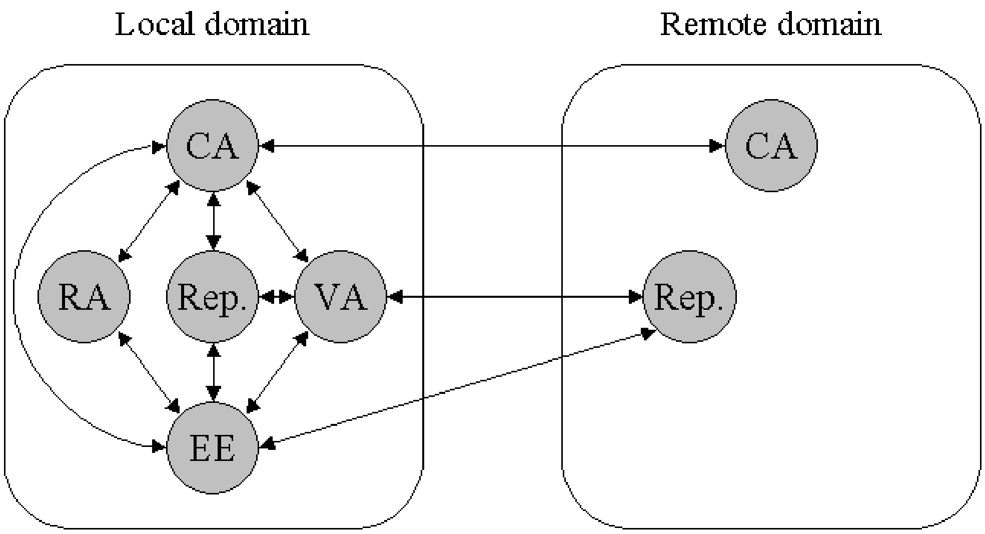
3.2. PKI

3.2.1. PKI interop structure

In order to run an interoperability event, each PKI must at least have the following entities:

- CA: Certification Authority
- RA: Registration Authority
- VA: Validation Authority
- Repository
- End Entity

Those entities have to be able to communicate in a local point of view, but also with entities from a remote domain.



3.2.2. History

An interoperability event on PKI already occurred in Asia in 2003. During the JKST-IWG PKI interop, the three items tested were:

- CAs (Certificate Authorities) interoperability (with the two protocols Cross Certification et Cross Recognition),
- Path processing,
- PKCS#11 application interoperability.

The results of those tests have been published in July 2003.

The PKI Challenge also realised interoperability tests in 2002. Funded by the European commission and organised by EEMA (European Forum for Electronic Business), the PKI Challenge (pkiC) is a two-year project, which started in January 2001. The PKI Challenge aims to provide a solution to interoperability between PKI related products, and to develop specifications and best practice in the world standards area. The 15 participants are Ascertia, Baltimore, Cryptomathic, Entrust, Guardeonic, Microsoft, NetSet, RSA Security, Safelayer, SmartTrust, SSH, TC TrustCenter, UTI Systems, Valicert, VeriSign.

The interoperability was tested between any pair of:

- PKI technologies from different vendors,
- CA service providers,
- PKI enabled client applications.

3.2.3. PKI interop at ETSI Plugtests

ETSI Plugtests proposes the following tests for the PKI interop:

✍✍ Interoperability between CAs

There are different protocols used in order to make two Certification Authorities (CA) interoperable: Cross Certification, Cross Recognition, Bridge CA, Certificate Trust List, Strict Hierarchy. Each protocol has his pros and cons. This way, they have to be tested so that the interoperability between CAs can be improved.

✍✍ Communication ability between PKIs

Since each PKI may have his own history, the programming language or the standard it uses may be different. Therefore, the testers have to verify that their PKIs can intercommunicate, even if they are using different languages or standards.

✍✍ Communications between entities

The PKI entities must be able to exchange information between them, but also with external components. As a consequence, they have to be able to do the following operations:

- o *Certificate Generation*: this includes the generation of the public key digital certificates, Certificate revocation lists (CRL), and cross certificates (exchanged between certification authorities). Those certificates have to use syntax and a format understandable by the other clients applications and other PKIs.
- o *Certificate Distribution*: the clients must be able to access the other user's certificates and the CRL.
- o *Certificate Management*: there must be interoperability between client applications and the CA so that both can dialog and exchange information.

✍✍ Certificate interoperability

The format of the exchanged data must be interoperable with the other PKI and client applications. Those data can be the certificate format, the cryptographic algorithms, the CRL, the certification validation path, the transaction message formats…

3.3. IPsec / IKEv2

The last interop event on IPsec happened in August 2001, in Espoo, Finland. An IPsec Plugtests was also to be held at ETSI in July 2003, but was cancelled due to the lack of participants.

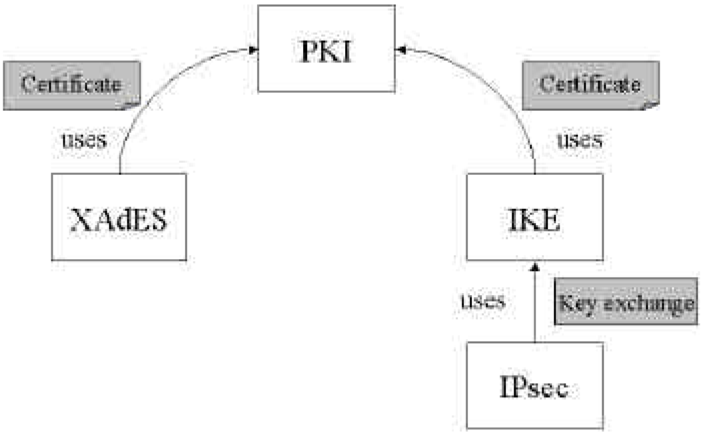
There exist an important interest in doing at the same time interoperability tests for the two domains PKI and IPsec/IKE. In fact, IPsec uses IKE (Internet Key Exchange) in order to share a secret key between peers, and IKE uses certificates and Certificate Authorities, in other words, PKI.

In the domain of IPsec / IKE, even if the interoperability seems to be already validated for IPsec, some problems are still presents for IKE. Therefore, the tests would be more oriented on IKE, especially on the interoperability with the certificates (as PKI would also be present during the tests).

3.4. Relation between the three technologies

The relation between those three protocols (XAdES, PKI, IPsec/IKE) is the following:

- XAdES uses certificates, Certificates authorities, and therefore the presence of PKI developers would allow the XAdES implementers to test in real conditions.
- IPsec uses IKE in order to negotiate the exchange of keys between peers in secrecy, and IKE uses PKI to do authentication and uses PKI certificates.



4. Some actors already identified (non exhaustive list)

4.1. XAdES

The XAdES testers in the last Plugtests interoperability event were:

- UNIVERSITAT POLITECNICA DE CATALUNYA
- IAIK, Graz University of Technology / SIC
- Agència Catalana de Certificació - CATCert
- Kopint-Datorg Rt.
- Sertifitseerimiskeskus
- Microsoft BVBA/SPRL

- Baltimore Technologies
- Microsoft Denmark

4.2. PKI

The European actors in the PKI are few, and the most significant are:

- CertiNomis
- AQL
- Axetel
- INTESA
- FINSIEL
- ON'X
- EADS-Telecom
- Eventually: EDF R&D, France TELECOM, CGE&Y
- American leaders: RSA, Verisign, Entrust, Baltimore and others

4.3. IPsec / IKEv2

The potential actors in an IPsec / IKEv2 interop are:

- VPN Consortium
- NetScreen
- USAGI Project
- Matsushita Electric Works, Ltd.
- Nortel Networks
- Funk Software, Inc.
- Arkoon Network Security
- Ericsson
- Sandelman Software Works - FreeSWAN project
- AudioCodes
- Spirent Communications
- Sun Microsystems