ETS\textsuperscript{I} Security week
eIDAS Thematic stream

Open source for creation and validation of signatures

Sophia Antipolis, France
25/06/2015

Robert Bielecki (ARhS SpikeSeed, Luxembourg)
Robert.Bielecki@arhs-spikeseed.com
Context
Findings
Standards
Principles
Validation report
Intrinsic interoperability
Context

- ETSI Plugtests
  - X/C/PAdES/ASiC/eSIGN

- SD-DSS Open source
  - Java Library

- Cross-border signature validation

- Various EU projects
  - eJustice/eCodex/TED/CheckLex
Findings

- Significant differences in the interpretation of standards
- Strong influence of national laws
- Habits related to countries and organizations
- The weight of the existing
- The lack of a common way of expressing the result of validation
- Signature validation in the European context remains quite difficult
- Common/Shared language needs to be defined
Interoperability issue

http://en.wikipedia.org/
Possible Solutions

Improving standards

Adoption of a common Open Source library
A regular validation process

Constraint
Constraint

Signature Validation
Application

Signed data
Signed data

Signature
Signature

Validation Report
At least one signature is invalid.

Signature is invalid:

- There are errors in the formatting or information contained in the signature.
- The signature was verified with the assign.ECDSA plug-in.
- Signing time is not available.
- Last checked: 2015.06.10 08:27:30 +02’00’
- Field: PDF-AS Signature #1 (invisible signature)
Observation: Who should read the report?

End user without any knowledge of signing

End user knowing the general concepts of signing

Helpdesk

Digital signature Expert
Observation: What rules must be checked?

Digital Trust

Cryptographic

Legal

Structural

Business process
What’s the solution

As IT experts we are not able to provide common validation policy, however we can provide a mechanism to express it!
Standards

Signature/Validation Policies

- 2002 Final
  - ETSI TR 102 038
    - XML format for signature policies

- 2015 Draft
  - ETSI TS 119 172-1
    - Signature policies: human readable

- 2016
  - ETSI TS 119 172-2
    - XML format for Signature Policies
Standards

Validation

2001 Info
- RFC 3126
  - Formats for long term electronic signatures/beginnings

2012 Final
- ETSI TS 102 853
  - Signature validation procedures and policies

2015 Finalising
- ETSI EN 319 102-1
  - Procedures for Creation and Validation of .../Part 1: Creation and Validation
Pragmatic approach

Definition of constraints

Execution of validation rules

Report generation

- Diagnostic data
- Detailed Report
- Simple Report
Validation policy: constraints

<SigningCertificate>
  <Recognition Level="FAIL"/>
  <AttributePresent Level="FAIL"/>
  <DigestValuePresent Level="FAIL"/>
  <DigestValueMatch Level="FAIL">true</DigestValueMatch>
  <IssuerSerialMatch Level="WARN">true</IssuerSerialMatch>
</SigningCertificate>

• **Levels:**
  • IGNORE – the rule is ignored
  • INFORM – when checking the rule the data are reported
  • WARN – when processing the rule FAIL is transformed to simple warning
  • FAIL – the process of the validation is stopped

**NOTE:** The use of warning can lead to exotic results
Validation reports

- **Diagnostic data**
  - Signature format abstraction
  - These data never change in time

- **Detailed report**
  - It contains a descriptive account of findings from the execution of all the rules defined in the ETSI standard and in the validation policy (constraint.xml)
  - It is difficult to understand by an end-user

- **Simple report**
  - A simplified version of the detailed report easily understood by non-IT user

All these reports are encoded using XML, which allows the implementer to easily manipulate and extract information for further analysis.
HTML based Validation Report

Interactive

Report
Validation Report & Open Source SD-DSS

SD-DSS framework

Validation constraints
  • ETSI 119 172-2

Validation Process
  • ETSI 102 853
  • ETSI 319 102-1
  New contribution!

Validation Report
  • ETSI 319 102-2
Intrinsic interoperability

- Standards
- Libraries
- Reference
- Standards are affected

Library is the guardian of interoperability
Thank you for your attention