Digitally Signed SPSCertificate message

Overview of prototype of digital signature applied to SPSCertificate message to TRACES

UN/CEFACT Forum Sardinia, Oct 14-18 2013
Overview

Non-signed certificate submission, as demoed earlier is available

- **SPSCertificate**, wrapped in TRACES-specific element containing credentials, XMLGate service ID etc.

*How do we apply digital signature?*

- On the incoming messages (**SPSCertificate**)
- On the reply (**SPSAcknowledge**)
- Based on recommendations made in analysis presented in Geneva in April
Applying digital signature

Choice of technology – ESSI:

- corporate Commission signature infrastructure, with support for:
  - signing documents (XAdES, PAdES)
  - validation (incoming signed document)
  - extension – timestamp, digital certificate inclusion
  - long-time archiving (re-signing, but not for physical storage of signed docs)
  - security aspects (HSM...)
  - Support EU official list of CA / CSP
Overview

- Signed SPSCertificate message
- Signed SPSCertificate message forwarded
- Signature validated
- Certificate data validated, stored
- SPSAcknowledgement created, signed
- SPSAcknowledgement returned
Actual steps in the prototype

Prepare the document for signature
  • Without XMLGate envelope
  • With TRACES credentials

Sign the data
  • Upload to ESSI
  • Sign it (using ESSI built-in test certificate)

Put signed message in XMLGate envelope
Send it to XMLGate
Signed certificate ready to send

Enveloping Signature

SPSCertificate enveloped in the Signature
Signed acknowledgement message

Enveloping Signature

SPSAcknowledgement enveloped in the Signature
Corrupt or manipulated data or signature

Enveloping Signature

SPSAcknowledgement enveloped in the Signature, indicating error
Summary

The key mechanisms are in place and work

For a Production deployment some steps are needed:

- Agreement on CA / CSP of SPSCertificate issuing authority, agree on equivalence criteria
- Adapt ESSI for this additional CA / CSP
- Develop archival facility
- Agreement on details (timestamping, audit logging...) may depend on bilateral agreements

WS-security not considered at this moment