The importance of incorporating XAdES extensions into ongoing XML-Sig work

Authors:
Juan Carlos Cruellas – Universitat Politécnica de Cataluña
cruellas@ac.upc.edu
Giles Hogben – European Network and Information Security Agency
Giles.Hogben@enisa.europa.eu
Nick Pope – Thales eSecurity Nick.Pope@thales-esecurity.com
Historical background

  – Defines Advanced Electronic Signatures as those ones that:
    • Are uniquely linked to the signatory
    • Are capable of identifying the signatory
    • Are created using means that the signatory may maintain under his sole control
    • Are linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
Historical background

- ETSI (European Telecommunications Standardization Institute) starts developing standards for electronic signatures aligned with European directive.


- February 2003, W3C acknowledges a submission based on XAdES v1.1.1 as W3C Note.
Historical background

• An interoperability event is organized by ETSI at November 2003.
• April 2004 publishes XAdES v1.2.2.
• Interoperability event in May 2004.
• March 2006 publishes XAdES v1.3.2
Technical background: generalities

• XAdES signatures build on XMLDSig signatures.

• XAdES signatures use XMLDSig extension capabilities (ds:Object).

• XAdES standardizes:
  – A number of new properties that further qualify XMLDSig signatures with information able to fulfil a number of common requirements (long term validity, non-repudiation, alignment to European Directive, etc)
  – Mechanisms to incorporate the aforementioned properties.
Technical background: generalities

- Defines a number of so-called “XAdES forms” as signatures that incorporate specific combinations of properties.
Technical background: properties

• XAdES properties may:
  – Qualify the signature itself, the data to be signed or the signatory.
  – Be incorporated to the signature by the signer before actually produce the digital signature value it and be secured by the signature itself (signed properties).
  – Be incorporated by the signer, the verifier or another party after the generation of the digital signature value (unsigned properties).
Technical background: XAdES and signature lifecycle

- XAdES forms (specific combinations of properties) are designed to encompass signatures life-cycle.

- This specially includes long-term signatures, where XAdES forms provides mechanisms covering from their creation to their auditing long time after their creation and first verification.
**Signer**

(1) Incorporates properties

(2) Generates Signature

(3) Requests, gets and incorporates signature time-stamp

**Storage service**

(4) Adds references to verification data

**Verifier**

(5) Verifies signature

(6) Requests, gets and incorporates time-stamp on signature and references

(7) Adds verification data

(8) Requests, gets and incorporates archive time-stamp
Technical background: properties overview

• Signed properties.
  – Incorporated by the signer before actually computing the digital signature value.
  – Secured by the digital signature value.

• SigningCertificate:
  – Reference to the signing certificate and optionally to the certificates in the certpath. References incorporate identifiers and also digest values of the certificates.
  – Secures signer certificate reference.
Technical background: properties overview

• SignerRole:
  – Indication of the role played by the signer when generating the signature. They may be claimed or certified (certificate attributes).

• CommitmentTypeIndication:
  – Commitment endorsed by the signer when producing the signature (proof of origin, proof of receipt, etc).
Technical background: properties overview

• SignatureProductionPlace:
  – Indication of the claimed place where the signature is produced.

• SigningTime:
  – indication of the claimed time when the signature is produced.

• Data object time-stamps:
  – Time-stamps on the to-be-signed data objects may also be incorporated.
Technical background: properties overview

• Signature policy identifier:
  – Reference to a set of rules followed when generating the signature and that also must be met when verifying it in order to consider the signature valid. This reference also includes a digest value computed on an electronic form of the signature policy document.
XAdES-EPES

Signature

SignedInfo

SignatureValue

Object

SignedProperties

SignedSignatureProperties

SigningCertificate

SignerRole

SignedDataProperties

UnsignedProperties

UnsignedSignatureProperties
XAdES-BES
Technical background: properties overview

• Unsigned properties:
  – Generated after the production of digital signature value.
  – Generated by the signer, verifier or other parties.
  – Usually data that help verifiers and auditors to assert the validity of the signature even long time after it was generated.
Technical background: properties overview

• SignatureTimeStamp:
  – Time-stamp on the signature that proves that the electronic signature was actually generated before that time.

• CompleteCertificateRefs:
  – References (including identifiers and digest values) to all the certificates in the certpath (but the signing certificate) that whose status verifiers must check while verifying the signature.
XAdES-T
Technical background: properties overview

• **CompleteRevocationRefs:**
  - References (including identifiers and digest values) of certificate status data (CRLs, OCSP responses, etc) that verifiers get while verifying the electronic signature.

• **Time-stamp on signature and references:**
  - Time-stamp securing signature and references to the material used by the verifier. It proves that at that time, a first verification of the signature took place and used the cryptographic material time-stamped. This may be assessed time after the verification.
Technical background: properties overview

• The next three properties are used when a long-term signature is required that incorporates all the cryptographic material used in its verification:

• CertificateValues:
  – All the certificates required in its validation.

• RevocationValues:
  – All the CRLs and/or OCSP required in its validation.
Technical background: properties overview

- **ArchiveTimeStamp:**
  
  - Time-stamp securing all the material in the signature including the values of the certificates and revocation data, to counter weakness of algorithms and cryptographic material signature-related as time goes by.
  
  - Nesting allowed to counter weaknesses in algorithms and cryptographic material in previous time-stamps.
XAdES current deployment

- XAdES signatures are nowadays being deployed in European countries for a variety of environments: electronic invoicing, digital accounting, Registered Electronic e-mail, etc.

- In certain countries, laws require use of XAdES signatures for certain transactions.

- ETSI has issued TS 102 904 “Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)”, defining XAdES profiles for e-invoicing, e-government, and also a baseline profile.
Position

• XAdEs provides a relevant building block for international mutual legal recognition of electronic signatures. This is a critical issue in areas like European Union (3-years programme for rollout of cross-border interoperable e-ID services) and Asia (e-Asian Framework agreement, to “facilitate the establishment of mutual recognition of digital signature frameworks”)

Position

• It is suggested that W3C notes the existence of the features already defined in ETSI TS 101903, and does not re-define any features already addressed there.

• It is suggested that W3C works with ETSI to establish common specifications for use of XML-based signatures.
Position

• It is suggested that W3C takes account of the lack of reversibility between ASN.1 and string representation for Distinguished Names as stated in XMLDSig and produces a reversible way (XAdES uses these mechanisms for identifying cryptographic validation material).
References

• W3C Note on XAdES. At http://www.w3.org/TR/XAdES/

• TS 101 903: “XML Advanced Electronic Signature (XAdES)“

• ETSI TS 102904: “Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)“

• ETSI Standards may be downloaded at: http://pda.etsi.org/pda/queryform.asp