

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

Juan Carlos Cruellas Universitat Politècnica de Catalunya

Giles Hogben European Network and Information Security Agency

Nick Pope Thales eSecurity

ETSI (European Telecommunications Standards Institute) published the Technical Specification (TS) 101 903: “XML Advanced Electronic Signatures (XAdES)” first version in 2002. This builds on the W3C XMLSig structures adding features that are important for advanced use of digital signature particularly in the European legal framework and in support of long term validity of signatures.

It is strongly suggested that this work be taken into account in the ongoing work of W3C. In particular:

- a) It is suggest that W3C take account of technical issues identified in the appendix to this document.
- b) It is suggested that W3C note the existence of the features already defined in TS 101 903, and W3C should not re-define any features that are already addressed by TS 101 903.
- c) It is suggested that W3C work with ETSI to establish common specifications for use of XMLSignatures.

Background

The ETSI XAdES specification TS 101903 defines a set of properties, which when added to XMLSig signatures using its extension mechanisms (<ds:Object> element) allow them to fulfil a number of additional requirements, in particular those entailed by the European Commission Directive on a Community Framework for Electronic Signatures as well as other use-cases requiring long-term validity and non-repudiation. , within <ds:Object> elements.

By using XAdES, signers may incorporate certain properties into the XMLSig signature structure before computing the signature value and including them in its computation. These properties include, among others, claimed or certified information on their roles, time-stamps on the signed data objects, indication of the commitment endorsed, and explicit identification of the signature policy under which the signature is created and must be verified. Additionally, soon after the signature has been created, signers or other parties may request and incorporate a time-stamp on the signature, which provides a trusted upper boundary on the generation time.

Using XAdES, verifiers or third parties may incorporate properties encompassing the long-term lifecycle of the signature, which after their generation includes first verification, storage for several years, and auditing (which means verification of signatures considerably after (even years) their first verification). For these stages of signature's lifecycle, XAdES:

- Defines structures for incorporating references to and/or values of all the cryptographic material used in the verification process (certification path and revocation data –CRLs and OCSP responses).
- Defines structures for incorporating time-stamps on this validation material, providing trusted upper boundary for the first verification time.
- Defines structures for incorporating special nested time-stamps (archive time-stamps) computed on both the signature plus validation data directly incorporated in its structure, which counters the apparition of weaknesses on algorithms or cryptographic material as time goes on.

Today XAdES has gained a high degree of acknowledgment in Europe and is also penetrating in Japan. Several interoperability test events have been organized by ETSI in Europe and by ECOM in Japan. Some European countries mandate signing certain electronic documents with XAdES signatures (e-Invoices, accounting documents, etc).

At present, there still exist certain issues (at legal, and standardization process levels) whose resolution would improve the standard and increase its usage (and in consequence XMLSig's usage). Our position on them is summarized below. At the end of the paper, readers may also find an annex describing a technical issue whose relevance is suggested to be assessed.

Standardization position: W3C and ETSI join in maintaining and progressing XAdES

Some years ago, W3C and ETSI started negotiating the setting up of a Joint Working Group for editing XAdES as a standard of both organizations, maintaining and, if required, updating it. Nevertheless, problems not directly related with the contents of XAdES standard, like differences in IPR models, blocked the creation of such a group. As organizations may change their rules and also may change their perception of how strong they must be in their initial positions, we think that it would be worth that both organizations would keep in touch permanently so that they could identify the right moment for re-launching a negotiation process for the creation of the aforementioned ETSI/W3C Joint Working Group.

Political Position: XAdES provides an important building block for international mutual legal recognition of digital signatures.

The possibility of using digital signatures for legally binding transactions has been part of the European Legal framework since 1999. By 2004, all 25 EU Member States had implemented the general principles of the Directive [1999/93 report]. Standard formats had been produced by ETSI as specified by [TS101733], and extended to ESI-XAdes with a view to encouraging interoperability of digital signatures across Europe.

Despite this, it is commonly agreed that mutual recognition of electronic signatures between member states is a major stumbling block in roll-out of pan-European eIdentity and eGovernment services. The IDABC (Interoperable Delivery of European eGovernment Services) is currently compiling a Study on Mutual Recognition of eSignatures for eGovernment [IDA BC report]

This is especially critical in Europe considering the following:

1. The 2006 Services directive, which is a binding obligation on all EU member states by 2009 states that: *“Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.”* [Services Directive]
This makes the provision of a mutually recognised signature format and legislation to support this an especially pressing requirement.
2. The European Commission eID action plan and Large Scale Pilots: in line with the 2005 Manchester Declaration, the European Commission has initiated a 3-year programme for the rollout of cross-border interoperable eID services based on national ID cards. The majority of the work will be carried out within a pilot programme which will also look at the use of ID cards for digital signature services. The current lack of mutually recognition for eSignature formats across border is a serious obstacle to such a programme.

It is also worth noting that similar problems are being addressed in other confederations such as Asean. The e-Asean Framework agreement states an explicit intention to: *“facilitate the establishment of mutual recognition of digital signature frameworks”*

Given that standard formats are a key component in mutual recognition, the increasing migration of electronic services to a web-services model, and the fact that XAdes is the only existing eSignature standard which can operate in a web-services environment, this makes it critically important that XAdes be maintained and promoted in as wide and open a forum as possible.

ANNEX

Suggestion for defining a Distinguished Name string supporting mechanism fully reversible

XAdES signatures incorporate references to validation material allow for storing validation data common to several signatures separately from signatures themselves, thereby saving storage space .

XAdES mimics XMLSig's mechanisms implemented in the <ds:X509IssuerSerialType> element for managing Distinguished Names and referencing validation data, consisting in using their string representation computed as specified by RFC 2253 (or RFC 4514 as is currently under discussion by the W3C XML security maintenance WG). RFC 4514 states in its section 5.2 that the only fully reversible string representation for Distinguished Names is the one using dotted decimal for AttributeTypes and hexadecimal encoding for AttributeValues. Hexadecimal representations (which are human readable) for AttributeValues are not always reversible. The W3C community should assess whether both XMLSig and XAdES would benefit if a fully reversible Distinguished Names human readable string representation were defined.

In case such a specification is consider useful, several options could be considered. The first possibility is to assess the feasibility of continuing the work done in RFC 4514 and defining a compact representation in one human readable string with capabilities for containing any information required for guaranteeing full reversibility. A different approach could be based on representing the Distinguished Names as a tree of XML elements containing whatever is necessary for guaranteeing full reversibility. Work done around mechanisms for encoding ASN.1 structures with XML as XER could also be taken into account here.

References

[1999/93 report] 2006 Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures

http://ec.europa.eu/information_society/europe/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf

[TS101733] ETSI Technical Specification Electronic Signatures and Infrastructures (ESI): "CMS Advanced Electronic Signatures (CAAdES)"

[TS 101 903] ETSI Technical Specification Electronic Signatures and Infrastructures (ESI): "XML Advanced Electronic Signatures (XAdES)"

[RFC 4514] "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names". June 2006. K. Zeilenga.

<http://www.ietf.org/rfc/rfc4514.txt?number=4514>

Electronic Signature Formats Dec 2004

http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010501p.pdf

[IDABC Report] Study on Mutual Recognition of eSignatures for eGovernment

<http://ec.europa.eu/idabc/en/document/6485/5938>, which is due to be completed in 2009.

[Services Directive] Article 8 <http://eur->

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT)

[eAsean] e-Asean Framework agreement <http://www.aseansec.org/6267.htm>