Digital Signatures: How Close Is Europe to Truly Interoperable Solutions?

Konstantinos Rantos

Digital Signatures: How close is Europe to truly interoperable solutions?

Konstantinos Rantos

Kavala Institute of Technology,
Kavala GR-65404, Greece,
krantos@teikav.edu.gr

Abstract. Digital signatures have been a hot topic in the e-government era as a key enabler for e-services provided to business and citizens, and secure exchange of e-documents. When this exchange crosses the borders of closed systems or EU's Member States, several interoperability issues arise. In EU many schemes and solutions have been proposed to overcome some problems, yet there is still more to be done. This paper provides a survey of the actions taken to promote interoperable use of digital signatures and identifies areas where EU has to invest in order to achieve the desired level of interoperability.

Keywords: Digital Signatures, interoperability, e-documents, standardisation, eGovernment services

1 Introduction

The penetration of digital signatures across EU has been noticeable the last few years, with more and more digital services adopting them to secure data authentication, integrity and non-repudiation. This flourishing period came after a long "recession" where public key cryptography and its derivatives, such as digital signatures, have been straggling to survive as a technological solution to securing e-services. European initiatives together with work programmes IDABC [15] and ISA [2] and the corresponding action plans have been the turning point that triggered EU's member states (MSs) to consider them as one of the key infrastructures in their eGovernment action plans. Nowadays, most of the countries across EU have already deployed digital signature schemes for their two main application fields:

- entity authentication, i.e. electronic identity (eid) schemes and
- data authentication and integrity, i.e. digitally signed documents.

Digital signatures have proven to be the robust solution for secure exchange of e-documents in the context of (cross-border) e-service provision. Although currently provided mainly by governments, they are anticipated to be adopted and widely deployed by other critical sectors, such as banking, to satisfy similar needs. Digital certificates and signatures are expected to be the user's e-passport to e-services.

Digital signatures are well studied and standardised by ETSI (European Telecommunications Standards Institute), CEN (European Committee for Standardisation) and other organisations and initiatives such as the EESSI (European Electronic Signature Standardisation Initiative). These standards have solved technological issues and viable and secure yet, more or less, closed solutions are already deployed and have long been tested. However, the plethora of technical standards resulted in diversified environments related to secure signature creation devices (SSCDs), certificates, and signatures, which bring more obstacles to the road towards interoperable solutions.

As a result, many activities have been taking place in EU aiming to promote digital signatures interoperability at legal, policy and technical level. Such activities include signatures related studies and projects like CROBIES (Cross-Border Interoperability of eSignatures), cross-border demonstrators and other less signature related but with a significant impact on EU's policy formulation on digital signatures, PEPPOL (Pan-European Public Procurement Online), STORK (Secure idenTity acrOss boRders linked), and SPOCS (Simple Procedures Online for Cross- Border Services) and secure documents exchange specific solutions like the Business Document Exchange Network (BUSDOX).

This paper looks at digital signatures interoperability issues and the work that is carried out in the eGovernment services field, emphasizing on e-document signing, yet ommitting application related issues. In this context, this paper provides an up to date mapping of the standards used by solutions deployed across EU and identifies the points that remain problematic and need our attention in order to strengthen weak links in the interoperability chain. It also aims to assist those that design digital signature enabled applications and have to make important interoperability decisions and those planning to develop signature generation and validation tools as the ISA programme requires.

The paper is organized as follows. Section 2 provides a quick overview of the activities that take place in EU regarding digital signatures interoperability and a thorough mapping of signature and e-document related standards. Section 3 sets the cornerstones of interoperability and defines the three levels of interoperability that seek viable solutions while section 4 identifies those areas where EU has to invest for truly interoperable solutions.

2 Current activities and standards

The EU's intentions to promote secure exchange of e-documents in the context of eGovernment services and to use electronic identities (eIDs) across all MSs, have boosted the use of digital signatures across the EU. This cross-border vision, however, has brought up many interoperability problems for digital signature enabled applications. With a plan on e-signatures in 2008 [1], Europe sets the cornerstones for the actions that have to be taken towards MSs acceptable and interoperable e-signatures. These plans are reinforced by the Commission's decision to define "interoperability of public key infrastructures (PKI)" as one

of the key activities of the ISA programme [2] defined in actions 1.8 and 1.9 regarding e-documents exchange and verification of e-signatures respectively.

Prior to start implementing EU's policy most of the MSs had justifiably designed their eID and e-services solutions considering merely their own needs and based on the applicable legal framework, usually overlooking other MSs needs and specifications. Figure 1 depicts the current status of standardisation in EU regarding digital signatures and e-documents. It is an update to the mapping published by EU [16] enhanced by the strong dependencies between those standards. The already complicated map coupled with the wide variety of options that each of these standards offers and the diversities among the adopted solutions reveal the reason why these e-signature related standards hinder the provision of interoperable solutions.

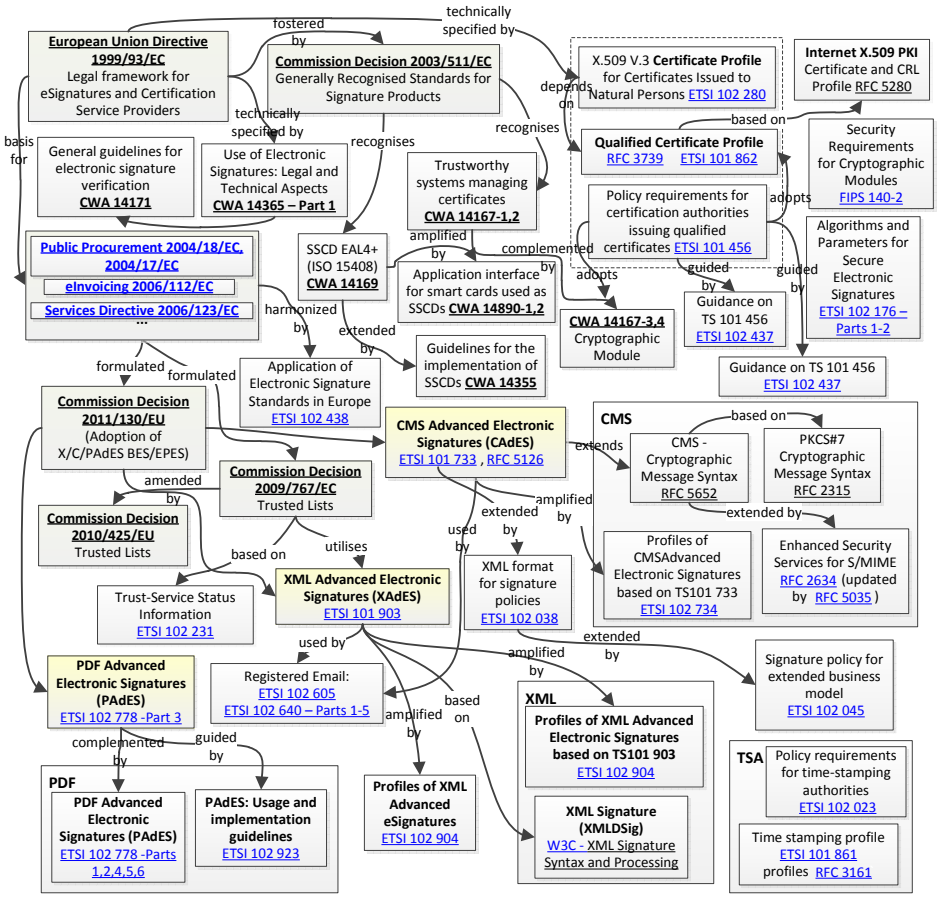

Fig. 1. E-signatures standards map

Recent activities in EU have resulted in the adoption of two significant solutions that aim to promote interoperability (both of them are the result of work carried out in the context of Directive 2006/123/EC):

- Publication of a list, namely Trust-service Status List (TSL), of supervised/accredited certification service providers (CSPs) issuing qualified certificates, to facilitate trust establishment among parties participating in a transaction (Decision 2009/767/EC [3] amended by Decision 2010/425/EU [4]). The plethora of CSPs across EU which operate under the umbrella of Directive 1999/93/EC [7] results in a chaotic situation in terms of trust among participating entitied. TSL helps verifiers establish the necessary trust relationships with foreign CSPs operating in other MSs.
  TSLs also contain mandatory information one should otherwise find on a certificate, according to the corresponding standards, e.g. information whether the certificate resides on an SSCD or not (ETSI 101 862 [9]) but the CSP did not include it in the certificate in a standardized and commonly accepted manner. Moreover, they complement digital certificates mechanism and the trust model they offer in a way that raises some questions as dependence on a list implies that user's trust circle has to be expanded to also cover mechanisms and procedures that the supervising authority employs for managing and publishing this list.
- EC has also adopted Decision 2011/130/EU [5], which defines common specifications regarding the format of signed documents to facilitate cross-border exchange within the context of service provision. These specifications promote the standardised CAdES [8], XAdES [10], and the recently ETSI adopted PAdES [14] formats for documents signed by competent authorities.
  Although these standards offer many options to cover a wide range of security concerns, only *-BES (Basic Electronic Signature) and *-EPES (Explicit Policy Electronic Signature) profiles are currently adopted by EU. These flavours have limited features and do not secure the provision of additional information required for the critical long term archiving and time of signature generation.

3 Defining interoperability

When implementing e-services that entail secure exchange of e-documents, or when signing documents, there are several questions that someone has to answer, including:

- What should the signed document format be?
- What types of electronic signatures (advanced, advanced based on qualified certificate, qualified) is the relying party willing to accept? In practice, what are the means that the signer has in possession and what is the risk the relying party is willing to accept in terms of signer's commitment and authorization?
- What are the acceptable key sizes, signature algorithms or hash functions?

– What additional information does the verifier need to verify and accept the provided signature, including timestamps and validation data?

The answers to these questions disclose the interoperability problems that digital signature deploying services are likely to face and can be mapped to the following interoperability levels.

3.1 Legal interoperability

The foundations of the legal framework at European level were laid by Directive 1999/93/EC [7], which defined the types of digital signatures and the requirements for the provision of certification services. Although it provided a solid basis for the use of digital signatures, it was only the basis on top of which many other structural components had to be built by MSs.

Since Directive 1999/93/EC several enhancements took place by corresponding decisions and plans for the wider deployment of e-services supported by the use of electronic services. Many studies have been conducted within the IDABC programme regarding legal interoperability [15], the details of which are out of the scope of this paper.

3.2 Interoperability at policy level

Although law is one of the factors that will affect the validity of a signature, policy restrictions is another and is related to the security considerations of the service for which signatures are deployed. For instance, while an advanced signature based on a qualified certificate might suffice for a document used within a specific service, the same document for a different type of service might require a qualified signature, i.e. the one based on a SSCD [7].

Policy restrictions should be considered by the verifier prior to accepting a digital signature and could include issues related to certificate validity, certificate suitability (e.g. requirements for trust establishment, use of SSCDs, acceptable SSCDs, CSP's auditing), signature validity (e.g. algorithms and key sizes, timestamps) and document signature properties (e.g. signature format, signature placement).

Current practices and EU adopted mechanisms do not secure policy requirements satisfaction leaving verifiers with the difficult task of collecting the necessary information or deciding ad-hoc about the acceptance or not of a signed document (assuming that the verifier has policy requirements).

3.3 Technical interoperability

Legal and policy restrictions might affect technical decisions on document, signature and certificate formats and characteristics. If signer and verifier cannot support the same algorithms, protocols and mechanisms, signature verification is bound to fail. Technical interoperability problems typically can be bypassed if solutions, algorithms and mechanisms adhere to specific standards and alternatives are narrowed down to a limited set of options.

4 Areas where EU should invest

In this section key areas that are anticipated to play an important role in future e-services seeking maximum interoperability are defined.

4.1 Time stamping

Time stamps are the means to provide assurances about the existence of data before a particular time [11]. While in some transactions is important to mark the time of data receipt, e.g. in e-procurement services, there are other examples where time-stamps have to be provided by the signer, e.g. a certificate issued by a competent authority some time in the past, in which case the verifier has to establish a trust relationship with the time-stamping authority (TSA) to accept both the time-stamp and the signature.

According to Directive 1999/93/EC and ETSI 102 023 [11] a TSA can be considered as a CSP which issues time stamp tokens. Based on EU's trust model, solid trust relationships between TSA and verifier can only be established if the TSA is a qualified one and therefore, supervised/accredited by the MS's competent authority and if the services are listed in the MS's TSL, given that these are included in a voluntary basis [3].

Trust establishment is essential for the verifier to be assured about the procedures, practices and the security measures taken by the authority to provide this service. Otherwise the validity of the time stamp is jeopardized. Time-stamping is a service that has to be put into the picture to enhance digital signature enabled services.

4.2 Signatures with validation data and long term archiving

Although currently adopted formats of *-BES and *-EPES seem satisfactory for a very basic exchange of signed e-documents, they do not suffice for stronger requirements set by the receiving entity in a transaction.

Verification information, all or part of it, as previously mentioned, can be provided by the signer, which bears the risk of deploying non-interoperable solutions. To avoid this unpleasant situation various solutions adopt alternatives for secure signature validation, such as validation points proposed by Decision 2011/130/EU [5] and used by large scale pilots, such as PEPPOL and SPOCS. Such ad hoc approaches however do not provide robust solutions to signed document validation.

Moreover, long-term archiving data are needed for the verification of signer's signature at a time when the signer's certificate might be revoked or will have expired. The aforementioned reliable timestamping is much related to the information that supplements the signature for long-term archiving. Such data will prove essential in the long run when governments go all digital, hence all archives are in digital form. In that case keeping all the necessary verification information with the signed document will be vital.

4.3 Policy restrictions

As the number of e-services is anticipated to grow in the years to come, more diversified and open environments will come into picture with their own requirements and restrictions regarding signature generation and validation. Currently accepted standards allow the signer only to disseminate his/her signature policy using the *-EPES format. This approach, although straightforward for the signer, requires the verifier to adapt his/her requirements on what the signer provides and decide about the validity on an ad-hoc basis. It does not consider the verifier's requirements regarding signature and, as a result to that, document acceptance.

A more appropriate solution would also allow the verifier provide his/her own requirements and establish a kind of agreement with the signer on the corresponding needs prior to signer's commitment. EU should elaborate on the formulation of an EU wide policy format and MSs must formulate their policies on e-signatures based on this for all cross-border services considering the following.

- Signer's policy adopted format should be unambiguously interpretable by the verifier, and automatically processed to relieve the end user from this very complicated task. ETSI 102 038 [12] and ETSI 102 045 [13] standards can form the basis towards this achievement.
- Promote policies recording and mapping based on commonly accepted standards to achieve the much desirable interoperability at policy level.
- Work on schemes that will facilitate policy agreements between signer and verifier prior to signer's commitment.

4.4 Commonly adopted standards for certificate formats

Current standards provide robust solutions for certificates and facilitate unambiguous interpretation of the type of certificate, its properties and security characteristics. However, not all of them are adopted by CSPs who issue qualified certificates, leaving critical information out of the certificate or included in a non standardized manner.

Adoption of commonly accepted profiles based on specific standards, such as those included in Figure 1, would allow certificates to carry all the necessary information that is now "delegated" to other schemes. Such an approach would help overcome the aforementioned problem caused by the issuance of certificates by different CSPs under different procedures, specifications and with a different perspective on the format that a certificate should have. CROBIES has already proposed an interoperable certificate profiles that can be adopted by the EU [6].

Although adoption of common profiles is not an easy task, it will secure the wide acceptance of certificates and convert them to the e-passport that EU envisioned and tries to promote through corresponding plans and actions.

5 Conclusions

The wide variety of standards on digital signatures complemented by the large number of options they offer, have resulted in many cross-border interoperability problems in EU.This paper provided an up to date mapping of digital signature and e-documents related standards and identified the key areas that still need to be considered by the EU in order to achieve truly interoperable solutions. In contrast to EU's approach of introducing new ad-hoc mechanisms and solutions to old problems the paper suggests the use of existing standards assuming that the options they offer are narrowed to a commonly accepted subset, an approach that is also adopted by Decision 2011/130/EU [5]. Adopting a more strict set of rules will simplify this complicated environment and will pave the way to a wider deployment of digital signatures, even for digitally analphabetic users.

References

1. Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM(2008) 798.
2. Decision 922/2009/EC on interoperability solutions for European public administrations (ISA).
3. Commission Decision 2009/767/EC, Setting out measures facilitating the use of procedures by electronic means through the "points of single contact" under Directive 2006/123/EC. Corrigendum, November 2009.
4. Commission Decision 2010/425/EU: Amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.
5. Commission Decision 2011/130/EU, Establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC, February 2011.
6. CROBIES: Interoperable Qualified Certificate Profiles, Final Report, 2010.
7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
8. ETSI TS 101 733. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). `www.etsi.org`.
9. ETSI TS 101 862. Qualified Certificate profile. `www.etsi.org`
10. ETSI TS 101 903. XML Advanced Electronic Signatures (XAdES). `www.etsi.org`.
11. ETSI TR 102 023. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities. `www.etsi.org`
12. ETSI TR 102 038. TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies. www.etsi.org.
13. ETSI TR 102 045. Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model. `www.etsi.org`.
14. ETSI TS 102 778-3. Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES); PAdES Enhanced – PadES-BES and PAdES-EPES Profiles. `www.etsi.org`.
15. IDABC Work Programme 2005-2009, `http://ec.europa.eu/idabc/`
16. Mandate M460, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.