EUROSMART
The Voice of the Smart Security Industry

Position Paper

How to avoid digital signature deployment & usage difficulties for eID ?

April 2011

Disclaimer

Eurosmart has taken reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained herein or for any consequences of any use.

1. Summary of content

Digital Signature allows documents to be signed electronically in a legally binding way. This enables complete electronic processes which in turn lead to cost savings through process optimization, electronic archiving, the elimination of transport costs, reductions in cycle times, greater security and flexibility as well as localization independence. Acceptance of electronic processes by users will also increase through the avoidance of media interrupts (e.g. applications no longer have to be printed out, manually signed and sent by post)

Directive 1999/93/EC established a new legal framework on digital signature. Eleven years later, the digital signature has not been a success and it is not really used although the directive was implemented at the national level by all European Member States.

The reasons for this lack of success are listed and detailed into this position paper. With the coming digital agenda and the e-ID programs largely deployed in Europe, Eurosmart e-ID experts analysed the risks connected with e-ID. Some recommendations are made to avoid digital signature deployment & usage difficulties for coming e-ID.

2. Electronic Signature: Overview & Difficulties

2.1. Some definitions

a) **Electronic Signature**

Electronic signature is a technical term that demonstrates the authenticity of a digital document.

It is based on Public Key Infrastructure (PKI) and is the result of a cryptographic operation that guarantees signer authenticity, data integrity and non-repudiation of signed documents.

Electronic signatures are used to establish the authenticity of electronic messages and documents. They are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. The legal validity of digital signatures is governed by legislation in many countries and throughout Europe. Electronic signatures are sometimes referred to as ‘digital signatures’.

b) **Three levels of security are defined** (according to EU Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures[1])

1st level: electronic signature

2nd level: advanced electronic signature

3rd level: qualified electronic signature

c) **Profiles of digital signatures** (according to PEPPOL)

Four pillars define the profile of the signature

- eID quality, ranging from 0 to 6
- eID assurance, ranging from 0 to 7
- Hash quality, ranging from 0 to 5
- Public key quality, ranging from 0 to 5

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF

2.2 Overview

Many contributions have been made to digital signature during the last 11 years. They are related to standards, legacy, use-cases, etc. Nevertheless, it seems that digital signature is not really used and has not been a success in Europe. There are different reasons for these difficulties:

- **The many standards and notes connected with digital signature**
  Digital Signature standards are mainly driven by CEN[2] and national agencies. Nevertheless, several CEN and ETSI[3] working groups are connected with digital signature and have prepared different notes or addendums to specify specific cases or interpretations (examples are WG 16, CEN/TC224 defining the Secure Signature Creation Device). The combination of all official documents on digital signature defines what the digital signature standard is.
  The complexity of this combination opens the door to many interpretations and developments. It prevents a clear understanding of the European digital signature standard.

- **Insufficient legislation**
  The existing European Directive was a first step for digital signature. It provided the legislative framework for the Member States, but did not define the technical details. Therefore, the Member States were forced to create their own technical definitions. In the end, different interpretations were made by the Member States when the Directive was transposed into national law. For example, semantics and terminology differ from one country to another and several definitions depending on the nature of the requested digital signature exist in some Member States (examples are “date format” with a different order for day/month/year and terms like “qualified digital signature” which have different meanings in different EU Member States).
  The combination of the European standard interpretations connected with existing European and national laws is a nightmare for digital signature deployment. This ambiguity regarding the national and European legacy is a huge difficulty to be solved in the EU before re-introducing digital signature functionality as a mandatory basic function into our digital European world.

  Additionally, the application of the use cases of electronic signatures was not defined at the EU level. In some countries, the electronic signature for notaries requires authentication through a smart card and in other countries not.

  There are no clear European answers to basic questions connected with the digital signature.
  What would happen if a document from Country A was signed in Country B with a login-password combination then delivered for eServices by Country C but was hacked when Countries A or B requested a strong authentication mechanism for digital signature?

- **Digital signature uncorrelated with strong authentication**
  Strong authentication is required for doing a digital signature. As the European Directive did not mandate the authentication, there are many different authentication mechanisms in use.
  This means that digital signature can be implemented in different ways with different security levels and no operational interoperability.

- **Lack of interoperability**
  It is very difficult to reach interoperability between several systems when they are based on different kinds of digital signatures. This is due to the different interpretations and digital signature definitions in European Member States.
  This missed interoperability stops harmonization and digital signature deployment.
  Verification of Digital signatures is not possible in neighbor countries due to different formats, key lengths etc. (there is no interconnection between CAs while more than100 CAs exist in Europe).

[2] CEN: European Committee for Standardization; www.cenorm.be
[3] ETSI: European Telecommunication Standard Institute

- **Security issues not harmonized**
  There are several interpretations of the European Directive on digital signature in terms of security. The potential security issues are still pending from the standpoint of European legislation. It is not clear how to manage such security issues in terms of legacy and responsibilities between Member States, ICT eServices providers, companies supplying ICT to the eServices sector and European citizens themselves.

- **No clear deployed use-cases**
  Digital signature could be widely used in Europe and several theoretical use-cases already exist. But reality shows that there are no concrete applications for professional users & citizens in Europe. This lack of applications based on the digital signature is probably due to the deficiency of our national legislations.
  Usage of the digital signature should be mandated by law to enable eGovernment services first, followed by other applications like eBusiness.

- **Business case for digital signature for citizens**
  There are neither motivations nor financial reasons for citizens to spend tens of euros a year for a qualified certificate.

The missing European regulation with associate legislations could explain why the digital signature is still not used in Europe. The lack of legislation stops professional and citizen uses which have no obligation to use it. This explains why there are no concrete digital signature applications for those who would like to use it.

3. e-ID: overview & challenge to solve

The EU has recognized that e-Government offers European citizens significant opportunities for improved access to better governmental services. When implemented and used correctly, e-Government offers national governmental systems substantial productivity gains and helps them cope with increasing demand for high-quality governmental services.

Interoperability is a basic requirement for systems and applications. The European e-Government world is rather scattered and uncoordinated at the moment and requires some effort to consolidate it. The first steps taken by the STORK[4] consortium are leading things in the right direction, but interoperability is not only technical, it also involves standards, security, legal and semantic issues. The current e-Government situation can be summarized as in the following subsections.

The EU funded PEPPOL project is focusing on e-signature with cross border use cases. The main application would be B2G.

Some issues with standards implementation

Although governments and smart card industries have developed the European Citizen Card (ECC) standards at CEN, EU Member States have decided to go for their own solution and the majority of them are keen to follow the ECC scheme. The lack of widely-used standards implies that standards often conflict and interoperability problems often occur. This issue is a barrier to generic and useful interoperable solutions for e-ID as it is for digital signature usage.

The ECC standard is now harmonizing existing eID standards in Europe. This is a first step for ensuring complete interoperability at the European level.

There is therefore a need to harmonize implementation choices in the EU with the involvement of government bodies.

[4] The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. https://www.eid-stork.eu/

A conflict of security level requirements

European mobility necessitates total interoperability everywhere in Europe but harmonization is not really applied to security level requirements for concrete functions such as identification, authentication, digital signature, data memory protection or privacy management. The security levels of deployed solutions may differ from one Member State to another, creating conflicts for interoperable eServices. Given that cyber criminals and terrorists will always attack the weakest link in the European defense chain, pan-European security is only achievable if all e-ID projects are equally strong. However, that is not the case for the more popular secure smart card-based approach and the purely software-based approaches used in some national infrastructures.

No European country would want to weaken national security and break down their economic efforts further to unsecured foreign choices that could introduce a major risk into their global interoperable system. Member States must therefore evaluate and compare the security levels of all national implementations.

A conflict of semantics

Generally, the interoperability of ICT systems is indispensable for efficient business processes and such interoperability for e-Services is a big challenge. Those who provide e-Services use ICT from different manufacturers from different technology generations and in Europe, from countries with different e-Service systems, languages and semantics. This means that e-Service information systems are often unable to exchange data in a meaningful way.

The eServices deployed in different European countries serve similar needs and are used for tax declarations, healthcare services, police statements, secure private or public transactions, etc. However, the implementation of such eServices differs from one country to the next, and different semantics determine that different input data is required for similar fundamental eServices in different countries. This generates conflict in terms of interoperability.

In the context of digital signatures there are semantic issues as well:

- The validity of certificates can be interpreted wrong (yyyy-mm-dd or dd.mm.yy)
- Family name formats (country specific characters, length)

If EU Member States want to achieve cross-border eServices and, in the long run, an internal market for eServices, such interoperability issues need to be solved at the international level.

A conflict of legislation

Various national-level regulations on signature could create legal conflicts for cross-border signature applications.

Although the European Union requires all Member States to legislate to ensure that citizens have a right to privacy through means such as Directives 95/46, national data privacy laws still vary greatly across Europe. This means that privacy concerns are often viewed as a barrier, and there is a complex landscape of privacy within Europe which could have a very negative impact on European interoperability. Even if privacy issues are seen as generally more difficult to tackle than technical issues, it is nonetheless critical to focus on them. There is currently no clear procedure governing the response to the loss of privacy in one country by a citizen from another country using eServices from a third country.

It is critical that Europe-wide legislation be implemented.

4. Eurosmart proposals for the EU

Referring to existing projects that have been deployed in mass production within Europe such as electronic Passports, and the above technical analysis of comparisons between data-base and Smart secure devices, Eurosmart recommends the use of e-ID smart cards to benefit from their portability, high security and performance. The Smart secure device represents an ideal storage media for personal data in accordance and respect of EU recommendations and privacy protection.

Eurosmart recommendations on **digital signature** are as follows:

1. The European standard should be simplified with a limited number of documents

2. Legislation connected with digital signature should be more detailed in the next version of the European directive

3. Security, privacy and interoperability should be defined and detailed at the European level for a common understanding between Member States. Strong authentication should be part of the European digital signature directive

4. All running digital signature card programs in EU Member States (e.g. Finland, Sweden, Belgium, Portugal, Spain, Italy, Estonia, Austria, Germany, Lithuania, Monaco, and The Netherlands) should be analyzed in terms of used signature quality and cryptographic quality

5. The European Commission must implement a roadmap for further semantic definitions for digital signature

6. A harmonized scheme for digital signature quality in the European Economic Area should be a target

7. Create daily use killer eGovernment applications for Digital signature

8. Definition of an eSignature classification A security and legal framework should be defined by law. However, there should not be more than two levels of signatures: the first one should be considered an acknowledgement; the second one should be considered a binding commitment, preventing the repudiation of transactions

9. Create attractive business models for citizens in the context of expensive signature cards

10. Electronic identity management at the EU level through the creation of a European eID Agency.

All recommendations listed above should be taken into account within the scope of eID programs.

Experiences with digital signature must be transferred to national eIDs in order to avoid similar difficulties.

Sources

- ETSI TS 101 456, v1.4.1, 2006
- ETSI TR 102 038, v1.1.1, 2002
- ETSI TS 101 903, v1.3.2, 2006
- ETSI TR 102 045, v1.1.1, 2003
- ETSI TS 102 176-1, v2.0.0, 2007
- ETSI 102 231, v2.1.1, 2006
- CWA 14890, 2004
- CWA 14170, 2004
- CWA 14167_1, 2003
- CWA 14167_2, 2002
- CWA 14169, 2002
- CWA 141170, 2004
- CWA 14171, 2004
- CWA 14172, 2004
- CWA 14355, 2004
- CEN TC 224 WG15

Glossary

CEN	European Committee for Standardization
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
CWA	**C**EN **W**orking Group **A**greement
ECC	**E**uropean **C**itizen **C**ard
STORK	**S**ecurity Iden**t**ity Acr**o**ss Bo**r**der Lin**k**ed
PEPPOL	**P**an-**E**uropean **P**ublic **P**rocurement **O**n**l**ine
CPS	**C**ertificate **P**ractice **S**tatement
LCP	**L**ightweight **C**ertificate **P**olicy
NCP	**N**ormalized **C**ertificate **P**olicy
QCP	**Q**ualified **C**ertificate **P**olicy
SSCD	**S**ecure **S**ignature **C**reation **D**evice

EUROSMART
The Voice of the Smart Security Industry

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work in dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Brussels
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email: eurosmart@eurosmart.com