# Open Smart Card Infrastructure for Europe

# v2


## Volume 4: Public Electronic Identity, Electronic Signature and PKI

## Part 8: Executive summary of White paper on Advanced Electronic Signature

**Authors: Smart-IS A.M. and eESC/TB12 AES**

# 1 Executive Summary

The realm of authentication and e-signature is vast, complex and consists of varied and divergent requirements seen from very different perspectives. It is also constantly evolving with new approaches proposed and new product offerings introduced. This White paper is concerned with a definition of and a proposed solution for authentication & electronic signature within the context of the **Open Smart Card Infrastructure for Europe** (**OSCIE) Vol 4 Public Electronic Identity, Electronic Signature and PKI.** It is in accordance with the Directive 1999/93/CE decided by the European Council and voted by the European parliament presenting the legal framework for the use of Electronic Signatures (13/12/1999) and the Directive 95/46/CE decided by the European Council related to the protection of Personal Information (24/10/1995).

There are four basic functions of signatures which are recognised – identification signatures, authentication signatures, signatures as declaration of knowledge, and signatures as declaration of will.

The issue of identification is complex and has political and social ramifications. It is also a fundamental issue and a core element of civil society in general and of security in particular.

Authentication is the process or ability to identify a person, resource, or system that is requesting access to another person, resource or system. Without authentication there can be no security, as even the strongest security measures are rendered irrelevant if one person can easily assume the identity of any other person.

Electronic signature signifies knowledge of, authorisation for and/or acceptance of an agreement where the agreement is explicitly associated with the signature. The European Directive definition of 'advanced electronic signature' is an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory
(b) it is capable of identifying the signatory
(c) it is created using means that the signatory can maintain under his sole control
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

All systems used in the authentication process must be interoperable and all systems used must be rendered secure.

The White paper contains a proposal for the Public Electronic Identity functional description and implementation specifications for e-Authentication (NAME) and for advanced Electronic Signature (NAME-ES) using smart cards via open public networks (the Internet). It is based upon supporting analysis and details of the underlying telecommunication industry and terminal manufacturer requirements for multi-platform access to services. End to end interoperability and security issues are dealt with. The specifications include the following elements: security (key management, certification procedures), services (payment protocols, loyalty, e-trading, data-transfer) and applications. NAME and NAME-ES could be implemented on multi-function cards issued by network operators based on international standards (EMV, SET, WAP, UMTS,…), for secure access to interoperable services through open infrastructures and International standard secure readers.

A description of the process that was used to obtain consensus on the proposed definitions and solutions is given. Issues concerning authentication & electronic signature for the three principal vectors of the e-economy: E-business, E-government and E-work are analysed and the business legal, functional and technical perspectives treated.

In order to facilitate consultation of the White paper by the expert and by the non-expert alike, a section of the White paper is specifically Expert oriented. To facilitate understanding the explanatory texts are to be found in the annexe. Amongst these are included:

- Glossary of Terms and Abbreviations Used
- List of referenced Standards
- List of International working groups
- List of Contributors
- Security Requirements
- Legal Requirements
- Security Solutions Review.

The annexe also contains a brief history of the European project SMART-IS A.M. Their contribution to the White paper includes the following documents of which the White paper is a summary:

- NAME , NAME-ES, Telco user requirements, smart card terminal manufacturers requirements and the Security solutions review. All of these documents were submitted to a RFC (Request For Comment) process.

It has been necessary to exclude from this White paper, certain non-technical areas of discussion and to focus upon the technical issues of generically acceptable solutions to identity and e-signature which include:

- Technical specifications for the implementation of the authentication and electronic signature modules on various types of terminals.
- Comparison with other types of solutions and comparative economic impacts.
- Tracking, referencing and collating economic and investment analysis research concerning interoperability technologies.
- Constraints, success factors and alternative solutions to the use of NAME and NAME.ES modules by terminal manufacturers.

The recommendations made are a basis for moving towards a technical standard. However the recommendations do not replace the need to formalise the process through the channel of acceptable standards organisations which is outside the scope of this White paper.

Interoperability can only be guaranteed where the solutions implemented are according to established standards. Therefore, only technically stable and acceptable market solutions have been fully considered. The market recommendations dealt with concern existing smart card standard technology and network security standards and the corresponding application areas. Although advances in biometrics are considered to be a market evolution, this technology is not mentioned in the European Directive and is, therefore, considered out of scope for the present White paper.

All subjects dealt with in the OSCIE common specification Volumes 1 to 10 (except for volume 4) are considered to be out of scope. Specifically within volume 4 data encryption methods, physical network security, are all out of scope for this White paper. All non-technical aspects such as organisational aspects (contracts, procedures, roles and responsibilities) and service aspects (such as certificate authorities, service providers, Certificate Policy, Certificate Practice Statement, Certificates management, Card Management System etc) are out of scope.

In order to have a trusted system, these aspects have to be dealt with in order to begin a practical implementation. If a Certificate Authority does not trust a certificate issued by another, neither interoperability nor a common signature have any interest.

Legal considerations for National/State legislation and Civil liberties and citizens rights although summarised are out of scope. In order to enforce cross-border acceptance of authentication and e-signature existing legislation must be applicable. The European legislation gives electronic signatures the same legal validity as traditional paper signatures and explicitly forbids the denial of an electronic agreement simply because it is not in "writing." To prevent conflicting state level approaches, the European legislation further forbids any state statute or regulation that limits, modifies, or supersedes this in a manner that would discriminate for or against a particular technology. The directive affirmatively requires the Member States to give legal effect to "advanced electronic signatures" that are based on "qualified certificates" and that are created by "secure signature creation devices".

The International, Industry & European work groups concerned with authentication & electronic signature issues and solutions and which are listed in the annexe have also been consulted in producing this White paper. However due to the difficulty with respect to national security issues, National work groups dealing with these areas have not been consulted and National standards bodies have not been specifically informed.

The International standards bodies have also been informed of the progress on the White paper and where appropriate, have contributed to the discussion.

The White paper has been produced with the help of Trailblazer 12 of the eEurope Smart Card (eESC) initiative which was launched by the European Commission in December 2000 as an immediate outcome of the eEurope initiative. The eEurope Smart Cards initiative gathered a wide community of industry experts, users, operators, academics with the objective of accelerating and harmonising the development and use of smart cards across Europe by building a consensus for system interoperability and the security of transactions. Twelve trailblazers were proposed to focus on the different issues and offer guidelines and best practices for meeting user requirements in order to integrate smart cards based infrastructures

across sectors. Trailblazer 12 focused upon the authentication measures and the Smart-Is project contributed specifically to this.

The eEurope Smart Card initiative has led to the production of a set of common specifications CSV2 containing guidelines, best practices, technical specifications and requirements for political, legislative or technical action.

An attempt has been made to forecast future developments and important initiatives have been anticipated by international organisations who are considering the implementation of the NAME & NAME-ES recommendations in the near future.

There are many barriers to take-up and most of these have been briefly documented:
The cost of rolling out authentication and e-signature applications nationally across an open network is prohibitive. Except for pilot schemes this has only been done with a fairly limited population (Finland for the national ID card, France for the medical profession).

A certain inhibition exists amongst national schemes because of the high cost and lack of a best practice solution. Although out of scope of this project, the legal and regulatory aspects when crossing national borders are even more complex due to the different national legislatures and the differing requirements for citizen protection & privacy as much within a national population as within a working or other community.

E-work (working at a distance) has not yet evolved to encompass the improved security aspects of PKI & smart card use, due to lack of ubiquitous card readers and the cost of implementation which has no obvious associated return on investment.

Certificate authorities at this moment in time do not have working agreements in place to accept/reject certificates issued elsewhere other than specific to the certificate issuing authority.

The following suggestions have been made in order to better anticipate future issues for organisations who wish to follow the White paper recommendations:

- Support a CEN/ISSS workshop on the NAME & NAME-ES modules dealing especially with the interoperability issues of specifications and requirements between cards, card readers, middleware and applications.
- Encourage national initiatives on interoperability (such as the Attica initiative -- prime minister's office -- in France) to work together.
- Within a European context but at national level, a regulatory authority could be set up, similar to the telecommunications regulators. The authority will deal with legal, regulatory and other implementation issues. In order to do this a full study on the existing framework for legislation needs to be carried out together with relevant recommendations.
- Encourage multinationals to implement e-working using smart card based authentication and e-signature.
- Encourage and support national initiatives in the ID and health domains.

- Encourage insurance companies to introduce lower cost policies linked to the acceptance of the reduced risk which is inherent to the use of smart card based schemes.

The full text of the White paper on authentication and e-signature is available on http://www.smartis.org/ and on http://www.eeurope-smartcards.org

**Bibliographic Reference for this extract is**

| | |
|---|---|
| Title: | Final White Paper: Deliverable D8.1 Whole project from 1 June 2000 to 18 December 2002 |
| Version: | 4 |
| Date: | 14 March 2003 |
| Author: | Alan Husselbee |
| Approved by: | N. Lipszyc – Smart-IS Marketing |
| Project: | Smart-IS A.M. IST Project n° 1999-13114: Smart-IS AM, Accompanying Measure for accelerating Electronic Business and New Transactional Information Systems |
| Co-ordinator: | Eurosmart |
| Participants : | Axiome, Cyber-COMM, Euralia, Magicaxess, Meta Group, Smart-IS Marketing, Telefonica I&D |