European Federated Validation Service Study

Solution Profile – MOA Signature Verification software

July 2009

This report / paper was prepared for the IDABC programme by:

Author's name: Indicated in the solution profile below, under '*contact information*'

Coordinated by: Hans Graux (time.lex), Christian Staffe (Siemens), Eric Meyvis (Siemens)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/7764

Executive summary

The European Federated Validation Service (EFVS) Study was initiated by IDABC in order to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature verification functionality. As a first step in the EFVS Study, information has been collected on twenty existing solutions that already provide all or some of the functionalities associated with European signature verification functionality, or that could provide valuable insights on how such an EFVS could be organised.

This has been done by drafting standardised profiles of the identified solutions, focusing specifically on how each of these solutions (a) determine the validity of signature certificates; (b) verify electronic signatures created using these certificates; and (c) provide specific guarantees to their customers on the outcomes of these processes.

The present document contains the solution profile for: MOA Signature Verification software.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	Project Management and Quality Plan (EFVS SC14 PMQP)
[RD2]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD3]	Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications http://ec.europa.eu/idabc/en/document/6485/5938

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: 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; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Solution Profile – MOA Signature Verification software

General identification information

Name and organisation
The "Module for Online Application (MOA) – Signature Verification (German: Signatur-Prüfung), referred to as "MOA-SP" is issued by: Federal Chancellery - Bundeskanzleramt
Reference (on-line source)
Federal Chancellery: http://www.bka.gv.at/site/3327/Default.aspx Project website (mostly German): http://moa-idspss.egovlabs.gv.at/
Contact information
Federal Chancellery – Bundeskanzleramt Ballhausplatz 2 1014 Vienna Austria Tel.: +43/1/53115-0 email: post@bka.gv.at Send questions related to this questionnaire to: Herbert.Leitold@egiz.gv.at

Scope of the solution

Services offered
(What services does the solution offer to a relying party? This should include most notably the three basic services above – validation of certificates, verification of the signature, and ensuring trustworthiness and legal liability – but may also cover additional services – e.g. semantic services, archiving of documents/signatures, maintenance, time stamping, security/reliability metrics for the security level of the signature and the certificate,… *Services that are not currently available but which are planned for the future may also be indicated.)* MOA-SP is an open source framework that provides the means for signature verification including certificate validation of XML or CMS based signatures. MOA-SP has been launched in 2002 and is part of a more comprehensive framework consisting of multiple modules for signature creation as well as for identification. MOA-SP aims at facilitating automated processes by completely taking over the signature verification tasks. Thus, SOAP webservice and JAVA API interfaces are provided. **Basic Services:** The basic service that MOA-SP provides is Signature Verification. The framework may be used by API as well as via SOAP web service interface. Currently the following signatures are supported: • XAdES BES based XML-DSig • CMS Signatures Apart from a cryptographic verification the signature verification also involves the validation of the underlying certificate chain (cryptographic integrity as well as trust including revocation checking). **Existing Additional services:** Apart from the basic services mentioned above MOA-SP provides the following additional services: • Examination of the signing certificate for QC statements in order to determine qualified signatures. • Examination of the signing certificate for private extensions containing special object identifiers indicating official signatures from public authorities. • Historical verification of signatures (certificates are validated according to the signing

time retrieved from the signed document)

- Optional archival of signature revocation information.

Future additional services:

The following extensions are planned in the medium term:

- Integration of Trusted Lists (TSL as defined related to the Service Directive)

Application domain (e.g. sector or application types)

(Is the solution usable in any sector or application field (i.e. is it generic in scope), or is it currently limited to a specific sector, application or domain? If it is currently restricted, would it be possible to extend the solution to other sectors, applications or domains? What would need to be changed?)

Basically the solution may operate in any sector or application field as far as the signatures that have to be verified are either XAdES BES XML-DSig- or CMS-based and the underlying certificates are X.509 certificates.

Since MOA-SP offers a SOAP interface the solution may be used by arbitrary applications. Since MOA-SP is open source software support for signatures other than the above mentioned may be added anytime.

CAs covered by the solution

(How many CAs are presently covered by the solution, and which ones? Do they include CAs established in multiple countries or states?)

The default configuration comes with Austrian CAs:

- A-TRUST (http://www.a-trust.at/)
- Main Association of Social Security Institutions (http;//www.hauptverband.at)

Technically new CAs may be immediately installed, registering specific trust anchors. The most common hash/signature algorithms (including RSA and ECDSA based algorithms, SHA-1, SHA-2 and RIPEMD160, respectively) are supported.

Extensibility of the solution

(Can additional CAs be integrated into the solution? If so, are there restrictions? Have such

extensions been done in the past yet, or are any extensions currently planned?)

Additional CAs can be quickly registered. The only restriction may be imposed by the underlying signature algorithms. But since the most common algorithms have been implemented no problems should occur in case of CAs following common standards.

Business model/cost model of the solution

(How is the solution funded? Is it envisaged as a for-profit model? Who pays contributions, and for what type of services? What profits (if any) are made with the services provided by the solution? Upon request of the correspondent, any communicated price information or other commercially sensitive information will not be disclosed.)

The framework is open source under the Apache 2.0 licence and may be used free of charge. It is funded by the Federal Chancellery in order to equip small and medium-sized businesses with a secure and easy tool to handle signature verification/creation solutions.

Technical approach

Validation approach
(Does the solution validate signature certificates, electronic signatures based on a hash value of the signed document(s), or signed documents with embedded signatures (attached signatures - enveloping or enveloped signatures – detached signatures)? *What is the maturity of the solution i.e. can it be classified as a known technical approach, such as a trusted list, bridge, or validation platform?)* Upon signature verification the underlying signing certificate (including each certificate of the complete chain up to a trusted root certificate) is also validated. The service supports enveloping, enveloped and detached signatures. MOA-SP can be used • by API • or by SOAP interface based on HTTP/HTTPS Using the SOAP interface, requests and responses are defined as XML structures with defined content. The user builds up a request (either by using the API or by creating an XML based request) and sends it to MOA-SP. The response of MOA-SP has to be evaluated (API) or interpreted (XML based response received via SOAP) respectively by the invoking application. Requests and responses consist of some mandatory and some optional elements. The specification of the XML structures (request and response) may be retrieved from the open source web site (refer to the title page of this questionnaire).
With regard to certificates
(How does the validation of certificates work – based on OCSP, CRLs, or both? What certificate profiles are supported by the solution?) Certificates are being validated in context of signature verification. Both approaches OCSP and CRLs are being supported. Which type revocation information service is used depends on the certificate. The preferred order (in case of certificates with multiple revocation information) depends on the configuration of the verification service. The service distinguishes between qualified and non-qualified certificates/signatures.

Independent from the quality of the underlying certificate the service indicates official signatures (special signatures from authorities indicated by a certain private extension).

The overall status of a certificate validation is either

- "trusted": if there is a certificate chain from the signing certificate up to a trusted root certificate and if each certificate of this chain was valid at the given time.
- or not "trusted": if the service was not able to build a valid certificate chain up to a trusted root certificate or although the service was able to build up a certificate chain up to a trusted root certificate at least one of the certificates of the chain was either revoked, on-hold, the validity period did not match the time given or the revocation status could not be determined.

With regard to signatures

(What signature formats are supported by the solution - PKCS #7, CMS, XML signatures, PDF signatures, XAdES, CAdES, or others?)

MOA-SP supports CMS and XAdES BES based XML-Signatures.

Multi-signatures

(Is the solution capable of validating multiple signatures on a document? Does it support independent signatures (co-signatures) and/or overall countersignatures?)

MOA-SP does not support multiple signatures, but can be/is used for it. The service has to be invoked multiple times for the verification of multiple signatures (each time referencing another signature).

Logging and auditing

(Is the use of the solution logged, and if so, to what extent? Do users of the solution have the possibility to perform audits or to gain access to independent auditing reports?)

Depending on the configured log level all steps are being logged, including parsing of XML based requests and download of certificate revocation information (LDAP), OCSP or CRLs.

Auditing depends on the practice of the service provider operating MOA-SP. Customers do not have access to logs.

Restrictions imposed on CAs

(What technical requirements are imposed on CAs, e.g. with regard to standards, formats or certificate profiles that they need to adopt? This includes e.g. the inclusion of certain information in signature certificates that is necessary in specific sectors.)

MOA-SP exclusively supports X.509 certificates. CRL distribution points and authority information are taken from the certificate. QC statements and key usages are evaluated and included in the signature verification response.

Usage of the solution by relying parties

(How do relying parties use the solution? Are there software components which they need to integrate into their own systems, is it a web service, etc.)

MOA-SP provides the verification service either as a SOAP web service or as a Java API. While the API approach requires a J2SE (minimum version 1.4.x) and the integration of the corresponding Java libraries into the specific application the SOAP interface may be used from any type of application on any platform. The SOAP interface which is naturally based on HTTP can be secured by SSL, allowing the server to authenticate against the clients.

Technical flexibility

(Given the technical characteristics outlined above, could the technical requirements of the solution be changed to increase its flexibility (e.g. by supporting other signature standards, validation methods, certificate profiles, etc...))?

The solution has been implemented in a very generic and modular way, so that future enhancements can be easily conducted.

Status of the project/Actual usage of the solution

(What is the status of the project (e.g. in development, prototyped, in production, etc.).

What is the actual usage of the solution (e.g. in terms of relying parties adopting the solution to validate electronic signatures) and what are the impacts of its use? How many transactions, how many certificates does it handle?)

MOA-SP which is fully operational is used by a large number of applications, many of them in the domain of e-government, and some of them in private sectors. Usually companies or public authorities use their own instance of MOA-SP to provide signature verification for the applications they are operating.

Legal approach

Relationship with the CAs[3]
(What requirements does a CA need to meet before being able to accede to the solution? Specifically, which processes and procedures have been foreseen to 'vet' CAs? What kind of agreements are put in place with the CAs, and what are the main issues addressed in these agreements?) Since companies and public authorities use MOA-SP for their own applications and services they usually run their own instances. That allows them to individually configure trust anchors and individually include CAs. Therefore the requirements for CAs are up to the specific company or authority.
Relationship with the relying parties
(How does a relying party get the right to use the solution? What kind of agreements are put in place in relation with the relying parties, and which services can be offered to the relying parties via these agreements?) The framework is released under the Apache 2.0 licence. Relying parties that want to use the solution do not have to meet any agreements in excess to the licence terms.
Reliability of the signature certificates
(What procedures does the solution put in place to determine the reliability of signature certificates? Are certificate policies checked? Are supervision/accreditation schemes considered? Have specific security criteria been defined, and does the solution support multiple levels of reliability? If so, can the solution distinguish between qualified and nonqualified signature certificates?) Certificate policies are not explicitly checked. The solution is able to determine and distinguish between qualified and non-qualified signature certificates (by evaluating QC statements). Finally the specific certificate is being evaluated with regard to official signatures. Official signatures are based on advanced or qualified certificates containing a special object identifier as a private extension. Official signatures are used to sign official documents issued by authorities.

[3] Within the EU, the term 'CA' should be taken to mean a certification service provider as defined in article 2.11 of the eSignatures Directive (Directive 1999/93/EC) and outside the EU, this means a Certification Authority in the technical sense, i.e. an entity issuing signature certificates to third parties.

Legal value of the signatures

(Can the solution make a statement on the legal value of signatures? If so, what factors are taken into account? If multiple degrees of validity are supported by the system (i.e. a statement on the reliability of the signature as a whole is provided), then how are these 'reliability levels' defined and communicated to the relying party? Can the solution identify if a signature can be considered a qualified signature (i.e. if it is an advanced electronic signature based on a qualified certificate created by using a secure signature creation device, as defined in the eSignatures Directive)? Finally, if the certificate policies contain restrictions on the use of the signatures (e.g. limitation to transactions of a certain amount or exclusion of certain sectors), then are these restrictions taken into account when communicating the legal value of the signature?)

As noted above the solution is able to distinguish between qualified and non-qualified certificates. There are two degrees of validity provided by the system: trusted and not trusted. Since certificate policies are not explicitly evaluated possible restrictions are not taken into account.

Liability of the solution provider

(What liability (if any) does the solution provider accept with regard to its services? Specifically, if the signatures rely on qualified certificates as defined under the European eSignatures Directive (if this is applicable to the solution), then how does the solution address its liability for providing guarantees to the public in relation to such certificates?)

No specific liability rules in excess to the law (e.g. Signature Law or Civil Code).

Quality of service and availability

(Does the solution provide any guarantees with regard to the quality of its service (i.e. the reliability of the information it provides) and its availability to relying parties, other than already mentioned above?)

As noted above MOA-SP is usually operated by companies or authorities by themselves for serving their own applications. Any guarantees in terms of quality of service is up to the specific company or authority.

Independence of the solution

(Is the solution fully unaffiliated (legally unrelated) with all of the CAs that are integrated into the solution? If not, then how is trust created towards the relying party for affiliated CAs?)

As mentioned above MOA-SP is usually operated by companies or authorities by themselves. The MOA-SP default configuration only involves the integration of A-TRUST CA, which can be removed or complemented by the operating party if needed.

Compliance with the provisions of the eSignatures Directive

(Does the solution support signatures from CAs established in countries that are not subjected to the provisions of the eSignatures Directive (Directive1999/93/EC)? If so, how are they integrated and how does the solution address their legal value?)

The default configuration only involves Austrian CAs. Which further CAs are to be integrated is up to the operating service provider.

Suitability of the solution at the European level

Assessment of the solution owner
(Does the solution owner feel that the solution could be adapted to operate at the European level – not applicable if the solution already functions at the European level?) The solution can be easily adapted to operate at the European level.
Issues to be addressed
(Which issues does the solution owner feel would still need to be addressed before the solution could be made to operate at the European level?) Additional CAs should be integrated in order to operate at the European level. If XML-DSig signatures other than XAdES BES based ones are to be verified, these type of signatures has to be integrated.
Integration with other validation solutions
(Is there any strategy to allow the solution to interoperate with other validation solutions, i.e. can the solution connect to other 'islands of trust'?) The interoperation with other validation solutions is conceivable but currently not planned.
Market Impacts
(How could the solution impact or influence the European market?) The solution is aimed at companies and authorities. Since the document formats being supported (XML-DSig, CMS) are based on common standards a cross-border operation is conceivable. A free of charge signature verification solution for companies and authorities may be helpful in terms of dissemination.
Any other comments?

(The solution owner can provide any other comments that (s)he feels were not adequately covered elsewhere)

No further comments.