



*moving  
services  
forward.eu*



**e-SENS white paper**  
**D3.2 Assessment on the sustainability maturity of building blocks:**  
**first and second cycle**

**Appendix 1: BBs sufficiently mature**

First assessment cycle (October to December 2013):

1. EU e-Signature Standards Framework
2. Addressing PartyIDType
3. Metadata Service Location
4. Transport ebMS3 and AS4
5. Associated Signature Container
6. Security Assertion Markup Language
7. Personal Identity Attributes
8. Quality Authentication Assurance levels

Second assessment cycle (April to June 2014 and January to February 2015):

9. Service Metadata Publishing (SMP)
10. Representational State Transfer (REST)
11. SBB Digital Signature Service (DSS)





## 1. EU e-Signature Standards Framework

### What has been assessed

The ABB EU e-Signature Standards Framework provides a framework of standards to be used for the various modules in an electronic signature solution.

### Standardisation

A number of standardisation criteria have been satisfied for SSF. Since most of the standards in the SSF are maintained or developed by ETSI or CEN, the standardisation criteria of Openness, IPR and Lifecycle management are met because ETSI fulfils these criteria in its basic policies and procedures. With respect to the Maturity standardisation criterion, not all of the sub-criteria are satisfied. According to a self-assessment of the SSF in the document that describes the Rationalised Framework for Electronic Signature Standardisation<sup>1</sup>, the development status of a subset of the standards in each of the modules needs to be improved. For details we refer to the “Rationalised Framework” document.

### Policy framework alignment

The sole purpose of the SSF is to satisfy the Mandate M460<sup>2</sup> in which it is clearly required to adhere to the EC Signature Directive<sup>3</sup>. The only remaining sub-criterion for which it is hard to determine whether it is satisfied by the SSF is around data-protection. Consequently, it is assumed that the SSF respects the data protection legislation in both originating and receiving countries. Although it seems that the SSF is useful for public administrations, citizens and businesses, no evidence is provided that the use of the SSF has a positive impact on organisational processes, administrative burden, security and privacy, financial costs etc. The same holds for possible risks of using the SSF and a solid plan for future development of the SSF.

### Business/market

The business/market criteria are fairly well met by the SSF, although some important issues are still unclear. All the basic business needs criteria are met, except for the business case, for which it is not clear whether this is positive and what the time period for the return on investment is. With respect to the Market support criteria, the main questions are still with the broad spectrum of end-uses, the willingness to pay for electronic signatures and possible competition with other solutions in member states.

---

<sup>1</sup>ETSI SR 001 604 v1.1.1 (2012-07)

<sup>2</sup> Document “The EU Mandate M460.pdf” in the zip-file submitted for assessment

<sup>3</sup><http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML>

e-SENS White Paper D3.2 Assessment on the sustainability maturity of building blocks: first and second cycle





## 2. Addressing PartyIdType

### What has been assessed

Electronic document exchanges require a mechanism for the unambiguous and machine-processable identification of business partners in business documents based on XML (or other structured formats) and in message headers. The ebCore Party ID specification specifies a mechanism for referencing party types using various international standards.

### Standardisation

The Addressing BB is an OASIS standard and fulfils the relevant and applicable criteria related to standardization. The specification provides implementation guidance and it is based on commonly used and recognized underlying standards. The specification is an open standard and has gone through the full standardization process of OASIS. It has been implemented in several projects and has likely overcome most of the potential initial problems. There are no automated conformance test mechanisms in place. The underlying technology is well proven.

### Policy framework alignment

Management for addressing schemes for party identifiers is something that is essential in most messaging formats and solutions are therefore already in place in most existing policies. However, the approaches are often tied to specific formats or communities. The Addressing BB offers a potential for convergence even though a migration may take a long time. Convergence will force member states and communities to review the existing policies/standards for addressing. Translation/Conversion between different addressing schemes may be required to bridge from existing approaches to the Addressing BB. Although the Addressing specification is mainly targeted towards businesses, it can theoretically be applied for identifying private persons. However, it is necessary to further analyse how to address this requirement.

### Business/market

The assessment team has the opinion that the Addressing BB can become an important component in eGovernment services and it has the potential to harmonize different approaches for party identification markup. The specification is in use but has not gained wide adoption compared to legacy solutions. Even though it might be seen as a competitor to other solutions, it offers a generic and standardized approach where none existed before. It is hard to assess costs and benefits as the specification only constitutes a small component in a larger infrastructural framework.



### 3. Metadata Service Location

#### What has been assessed

The OASIS Business Document Metadata Service Location specification is an update to, and standardizes, the PEPPOL concept of Service Metadata Location (SML), one of the key technologies supporting dynamic discovery of service metadata.

#### Standardisation

The Metadata Service Location BB is an OASIS working draft and fulfils the applicable criteria related to standardization even though it has not yet gone through all the steps in the standardization process. The specification is based on commonly used and recognized underlying standards such as the DNS system, REST and XML. The specification is to become an open standard. Profiling and further implementation guidelines will be necessary. Reference implementations exist and the PEPPOL SML, which this specification builds on, is in production and is well proven. Even though the specification builds on PEPPOL SML, it is not backward compatible with it. The specification is using well-proven underlying technology such as DNS and REST.

#### Policy framework alignment

The Metadata Service Location BB provides functionality for connecting infrastructure from different communities or countries, and it can play an important role in eGovernment services. It is used within the PEPPOL network and is the key component to create connectivity by means of the dynamic look-up functionality. It is in line with several of the underlying principals mentioned in EIF (not all are applicable). The BB must be analysed and possibly customized when adopted in new domains with less openness than the procurement domain. When adopted in a new domain, it is necessary to check whether the current functionality of the BB satisfies the specific requirements of the new domain. The assessment team has the opinion that the services described in this specification positively impact migration, security, financial costs and administrative burden. There are risks connected to the metadata services in that it becomes a very important component in an infrastructure and its availability is crucial.

#### Business/market

The assessment team has the opinion that the automatic discovery and look-up, which the BB provides, has the potential to significantly simplify access to services. The functionality has been tested in both B2G and B2B procurement, e-freight and in the construction industry processes. It helps particularly SMEs in that integration becomes more automated and routing configuration can be done without manual intervention. This is very important in domains having many-to-many connections. It is essential for cross border services. It competes with existing solutions in a limited extent because very few (if any) comparable solutions exist.



#### 4. Transport ebMS3 and AS4

##### What has been assessed

The subject of this assessment is the Transport Layer for e-Delivery ABB (ebMS3 and AS4 Profile for ebMS3). ebMS3.0 a family of XML based standards sponsored by OASIS and UN/CEFACT whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners. The ebMS standard is the messaging service component of ebXML. The AS4 specification is a profile (subset of functionality) of ebMS3.0.

##### Standardisation

The AS4 specification is a profile (subset of functionality) of ebMS 3.0. AS4 was published as an OASIS standard in 2013 and has been tested and implemented in different projects. The specification has been reviewed in due process according to the OASIS standardization process and the assessment team has the opinion that this ensures maturity. OASIS has a well-established maintenance organization and procedures.

##### Policy framework alignment

The AS4-specification is in line with several of the underlying principles of the EIFv2 (not all are applicable). Services built based on the AS4 specification can be in line with EU legal framework and policies but it must be ensured and investigated how this is best done. In e-SENS, AS4 is proposed to be used in a four-corner-model arrangement where users interconnect through gateways. This approach can help bridging, and thus overcome differences and technical incompatibilities.

The functional requirements are well described and cover typical Business-to-Government use cases. The specification has been implemented in e-Justice domain and e-government services but a more thorough investigation is required for assessing the applicability in other domains. They are compatible with other related BBs such as Addressing and Service Metadata Location. The specification, being an open standard, is independent from specific vendors. However, it uses underlying standards requiring low-level functionality not supported out-of-the-box in some platforms such as the Microsoft.Net framework.

##### Business/market

The AS4 specification offers the possibility to create services with high quality, especially cross border. There are opportunities for software and service providers to put services based on the specification into use. User groups have shown interest to adopt AS4 to complement existing solutions, such as the GS1 eCOM Technology Group. All domain specific requirements have not yet been assessed but it is envisioned that AS4 will be useful in cross border services. The AS4 specification is an international standard and it is also applicable outside Europe.



## 5. Associated Signature Container

### What has been assessed

ASiC Associated Signature Container is ETSI standard ETSI TS 102 918 v 1.1.1 (2011-04). ASiC is a container structure to bind together a number of signed objects (e.g. documents, XML structured data, spread sheet, multimedia content) with either advanced electronic signatures or time-stamp tokens into one single digital container. This uses package formats based on ZIP and supports CAdES, XAdES, detached signature(s) and the IETF RFC 3161<sup>4</sup> time-stamp protocol. ASiC-S is a simple ZIP container<sup>5</sup> to associate one or more signatures with a single data object; ASiC-E is an extended ZIP container that contains multiple data objects.

### Standardisation

ASiC is a relatively new standard developed in ETSI and has room for maturing. However, it is usable right now. The plug test event in 2012<sup>6</sup> had relatively high participation rate, which is indicating existence of many interests for implementations. The European Commission has developed a software tool DSS<sup>7</sup> for TSL signing, which supports the ASiC-S (but not the ASiC-E) format. The Estonian digital signing format BDOC<sup>8</sup> is fully compliant with ASiC (including ASiC-E). There is open source software Digidoc<sup>9</sup> for signing documents with eID of several countries. Further detailing of the ASiC standard is ongoing. ASiC includes excellent support for A2A services.

### Policy framework alignment

ASiC is compliant with the European Interoperability Framework. ASiC especially relates to underlying principle 5 on Security and Privacy and underlying principle 10 on Openness. ASiC is in line with the conceptual model for public services as defined in the EIF. ASiC is aligned with national frameworks of the participating countries and use of ASiC will avoid potential incompatibilities between Member States.

### Business/market

The adoption of the ASiC will positively impact organisational processes: for example signing documents digitally in ASiC format allow Eltel Networks to save 1,380 Euros per month and the University of Tartu to save 11,500 Euros per month<sup>10</sup>. The biggest savings would be achieved on workforce costs, and the costs of printing and postage.

---

<sup>4</sup>IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

<sup>5</sup>PKWARE ".ZIP Application Note". Available at <http://www.pkware.com/support/zip-application-note>

<sup>6</sup><http://www.etsi.org/plugtests/ASiC/Home.htm>

<sup>7</sup><https://joinup.ec.europa.eu/software/sd-dss/release/release202>

<sup>8</sup><http://www.id.ee/public/bdoc-spec21.pdf>

<sup>9</sup><http://e-estonia.com/components/digidoc>

<sup>10</sup><http://sk.ee/en/useful/digitalsigning>



## 6. Security Assertion Markup Language

### What has been assessed

This ABB refers to the framework proposed to be used by the different Member States for exchanging messages with authentication and authorization data into the Electronic Identification (e-ID) process over SAML 2.0 standard.

### Standardisation

The SAML ABB was successfully used in several projects where different pilots were conducted among different Member States performing a set of use cases such as Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery or Change of Address.

A complete set of management, decision-making process, formal review process documents and guidelines are available for this ABB on the STORK1.0 and STORK2.0 web sites. The underlying technology is SAML2.0 that is a well proven and documented standard endorsed by OASIS. All software resources related to this ABB are available in the JOINUP portal under EUPL license. The life cycle support for this ABB was provided by STORK1.0 (2008- 2011), the ISA Work Programme 2011 (2010 - 2012) and STORK 2.0 (2012-2015). Maturity, openness, intellectual property rights and lifecycle management criteria are fulfilled by this ABB.

### Policy framework alignment

The SAML ABB is in line with the European Interoperability Framework, in particular with Principle n°4 Security and Privacy, Principle n°9 Openness and Principle n°11 Technological neutrality and adaptability. EU Data Protection Legislation is fully respected by this ABB. Electronic government is promoted by this ABB where cross-border authentication is provided. This implies an important level of applicability in different areas. The impact of this ABB is considerable since citizen, public and private organizations are interested in using electronic services among different European security domains with just one electronic identification. Basic alignment with existing policies, applicability and potential criteria are fulfilled by this ABB.

### Business/market

Potential change in the quality of the service delivered to the citizen/business by the administration before and after adopting this ABB is guaranteed. This ABB provides a federation id key and allows citizens to authenticate securely using their national credentials in their home European countries to get access to services offered by administrations/business in other European countries. It is hard to assess costs and benefits due to only a small set of pilots having been developed so far. These pilots are not final products and they were conducted to prove capabilities in different use case scenarios among different Member States. No competing solutions are available in Member Countries.





## 7. Personal Identity Attributes

### What has been assessed

Personal identity attributes are defined by STORK as a set of attributes that can be queried about the subject of an authentication, being a citizen authenticated in his home country.

### Standardisation

Implementation guidelines, documentation for the implementation of STORK, decision making process, formal review process, relevant documentation of the development and approval process of STORK, life cycle policies/processes/procedures for STORK, executed plans and procedures, are available in STORK1.0<sup>11</sup> and STORK2.0<sup>12</sup> web sites. However, the documentation is about STORK not just about Personal Identity Attributes ABB. All software resources related to this ABB are available in STORK website. Life cycle support for this ABB was provided by STORK1.0 (2008- 2011), ISA Work Programme 2011 (2010 - 2012) and STORK 2.0 (2012-2015). Maturity, openness, intellectual property rights and lifecycle management criteria are fulfilled by this ABB.

### Policy framework alignment

The e-ID Interoperability Framework especially relates to underlying principle 4 on Security and Privacy and underlying principle 9 on Openness. The Personal Identity Attributes ABB is originated from SAML 2.0 and the SAML 2.0 ABB is especially in line with Principle nº4 Security and privacy, principle nº9 openness and principle nº11 technological neutrality and adaptability. Thus, the ABB is also in line with principles that are in line with SAML2.0. There are limitations to what an authentication framework and its attribute profile can do to handle incompatibilities between member states need for attributes. The current set may not be sufficient to deal with such incompatibilities. Basic alignment with existing policies, applicability and potential criteria manage to be fulfilled by this ABB.

### Business/market

STORK's Pilots prove SAML2.0 ABB guarantees an ID key which it makes possible for citizens to authenticate securely using their national credentials in their home European countries to get access to services offered by administrations/business in other European countries. Conversely, The ABB is not applicable but we may assume that the Personal Identity Attribute ABB is used in the same way as SAML 2.0. Basic business need and market support criteria are not yet fulfilled by this ABB.

---

<sup>11</sup><http://www.eid-stork.eu>.

<sup>12</sup><http://www.eid-stork2.eu>.





## 8. Quality Authentication Assurance levels

### What has been assessed

QAA Level definitions to describe a set of requirements used to determine to which level an authentication solution belongs.

### Standardisation

The QAA ABB was successfully used in several projects where different pilots were conducted among different Member States performing a set of use cases such as Cross-Border Authentication for Electronic Services, Safer Chat, Student Mobility, Electronic Delivery or Change of Address.

Implementation guidelines, documentation for the implementation of QAA, decision making process, formal review process, relevant documentation of the development and approval process of QAA ABB, life cycle policies/processes/procedures for QAA ABB, executed plans and procedures, are available in STORK1.0 and STORK2.0 web sites. No underlying technologies are under this mapping. All software resources related to this ABB are available in STORK website. Life cycle support for this ABB was provided by STORK1.0 (2008- 2011), ISA Work Programme 2011 (2010 - 2012) and STORK2.0 (2012-2015). Maturity, openness, intellectual property rights and lifecycle management criteria are fulfilled by this ABB.

### Policy framework alignment

The QAA ABB is in line with the European Interoperability Framework, in particular with principle n°2 User-centricity, principle n°04 Security and Privacy, Principle n°6 Administrative simplification and Principle n°9 on Openness. EU Data Protection Legislation is fully respected by this ABB. e-Government is promoted by QAA ABB where cross border authentication is provided. In addition, QAA does not impose a single e-ID solution. This makes it easier to implement e-Government solutions however; common specifications for mutual recognition of national electronic identities (e-ID) between participating countries and administrations should be tested and developed. Basic alignment with existing policies, applicability and potential criteria are fulfilled by this ABB.

### Business/market

The e-ID Framework will make it possible for citizens to authenticate using their national credentials in their home European countries to get access to services offered by administrations/business in other European countries. Moreover, the security and privacy of information is guaranteed both at authentication as well as during transfer through the e-ID framework. In addition that a functional trust framework for e-authentication is a requirement for successful and large-scale cross-border interoperation of such services is being taken into account. Basic business need and market support criteria are fulfilled by this ABB.





## 9. ABB Service Metadata Publishing (SMP)

### What has been assessed

Service Metadata Publishing specification is a method for publishing the metadata of services made available via the web.

### Standardisation

Service Metadata Publishing (SMP) is in a mature level of developing and production. It was used for the PEPPOL project and it has been standardized in OASIS. The specification is based on commonly used and recognized underlying standards such as REST and XML. All sub-criteria under the standardisation criteria have been satisfied for SMP. Criteria regarding IPR are fulfilled.

### Policy framework alignment

The SMP BB provides functionality for connection of infrastructures from different communities or countries, with different maturity- and ambition levels, thereby enhancing flexibility and scalability. It can play an important role in e-Government services. It is used in production within the PEPPOL network and is the key component to create connectivity by means of the dynamic capability look-up functionality. PEPPOL infrastructure, addresses the Organisational, Semantic and Technical interoperability layers of the European Interoperability Framework (EIF) version 2.03 and SMP is compliant with public services concept as defined in EIF. SMP is currently in production in connection with AS2 and START for message exchange and using PKI as a trust model, but should be piloted with different message exchange protocols and other trust models. In countries where PEPPOL is used, SMP is aligned with national frameworks. SMP fulfils most of the Applicability criteria, but there are items that might be considered for improvement.

### Business/market

Adoption of SMP supports flexible quality of service delivered to the citizen/business by the administration, by automatic discovery and look-up that has the potential of simplifying access to services. The development of SMP was initiated by the PEPPOL project. It is used in the e-Procurement domain by all partners of OpenPEPPOL. Implementations in the e-Health and CISE domain are being initiated. It is important to further develop these implementations and to involve more industry partners of other domains so that the SMP building block really has a stable implementation base to be a generic BB in e-Delivery and is universally applicable in other domains.



## 10. Representational State Transfer (REST)

### What has been assessed

Representational State Transfer (REST) is a style of architecture based on a set of principles that describe how networked resources are defined and addressed.

### Standardisation

Representational State Transfer (REST) is a style of architecture based on a set of principles that describe how networked resources are defined and addressed. REST has gained widespread acceptance across the Web as a simpler alternative to SOAP and WSDL. Sub-criteria under the Maturity and Openness criteria have been satisfied for REST. There are several tools for testing REST services like cURL or Google Advanced REST client, but there were no certification found. REST is widely used in production environment by several large scale service providers.

### Policy framework alignment

REST is a software architecture style consisting of guidelines and best practices for creating web services that does not violate any principles of EIF v 2.0. As a software architecture style it is in line with principles of EIF v 2.0 and thus facilitates interoperability between public administrations. REST services can be used for A2A and B2B integration and can contribute to public services development. REST services do not contradict the EU legal framework on data protection or electronic signature and has a neutral impact on the national frameworks of the participating countries. It is a software architecture style consisting of guidelines and best practices for creating web services widely used thus does not introduce incompatibilities between Member States. The PEPPOL SMP REST usage is a proof that the validity of information exchanged across borders is maintained. REST's goal is "to improve server scalability by eliminating any need for the server to maintain an awareness of the client state beyond the current request"[2] thus it facilitates the development of web services and implicitly e-Government services. There are items that might be considered for improvement. The "Recommendations for improvement" section below comprises some policy related suggestions.

### Business/market

REST ensures user-perceived performance, network efficiency, scalability and reliability thus the quality of the service delivered to the citizen/business is positively influenced. REST architecture is widely used in production environment by several large-scale service providers (Google, Yahoo, Amazon, etc.). REST can help public partners in achieving their missions, by providing guidelines and best practices for creating scalable web services and can be useful in the development of e-Government cross-border services by providing guidelines and best practices for creating scalable web services. REST has already a large market adoption rate and provide lower costs over time.



## 11. Digital Signature Service (DSS)

### What has been assessed

Java Applet specification, based on the underlying open source framework, to create or verify electronic signatures. Only, the specifications have been assessed, not the actual implementation of the web service and its interface.

### Standardisation

For the SBB DSS the majority of the standardisation criteria have been satisfied. The SBB is described in sufficient detail, consistency and has been developed for a sufficient period to overcome most of the initial problems. Furthermore DSS version 4.x is based on proven and stable technology, DSS is being used or planned to be used by 12 member states. A few standardisation criteria have not been satisfied. There is no planned mechanism specified to assess the conformity of the installed version of DSS. Furthermore not all information about the maintenance of DSS is openly available. There is for instance no information published on the operation of the maintenance and the decision-making process, including reviewing, for a new version of DSS is not open. Next to this no information is provided on how Member States which parts of the implementation can be reused when migrating from DSS to another solution and there is no clear procedure specified for the development, documentation and execution of the disposal of DSS. The software that is created and available is published as open source under the LGPL license and is royalty-free. The European Commission is responsible for the maintenance of DSS and also provides a helpdesk.

### Policy framework alignment

Only one policy criteria has not been satisfied by the DSS solution, this is the criteria on the specification of the functional and non-functional requirements which have not been fully specified. All other policy criteria, both on the basis alignment with existing policies criteria and the applicability criteria have been satisfied. On the potential criteria, only the evidence criteria have not been met. The submitter of the SBB DSS provided too little information about the evidence criteria of the SBB to do a proper assessment on the criteria that relate to this.

### Business/market

The business/market needs criteria are all satisfied by the SBB DSS, except for the criterion that the business case. Furthermore, there is no evaluation of costs and benefits of using DSS in a member state provided. All other criteria have been met and SD DSS is in use or planned to use in 12 member states and implemented by different contractors. However, a point of attention is that some browser suppliers, such as Google, do not support the implementation in the form of Java Applets. Due to the limited scope of DSS there are no competing solutions identified and the European Commission makes sure that there is support available for the implementation and use of DSS.

