Mapping European IDABC Authentication Levels to SAML 2.0 - Gap analysis and recommendations

Authors: Konstantinos Moulinos, Giles Hogben, ENISA (European Network and Information Security Agency)

Version: 1.0.0
Date: 2008-07-16

1 Introduction

In 2004 the European Commission (EC) launched[1] the *IDABC* (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) program to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe by means of information and communication technologies. User identification and authentication are the cornerstones of this project. Interoperability of European eID Management (eIDM) solutions is of outmost importance for the success of the project. For this reason, IDABC conducted and report on *eID Interoperability for PEGS* (Pan-European eGovernment Services) in order to analyze eID and authentication interoperability requirements. One of the objectives of this analysis was to propose and study the impact of a multi-level authentication mechanism and derive common specifications for interoperable eID in the EU This effort resulted in a series of documents setting up the *eID Interoperability Framework*[2].

One of the most important concepts of the eID Framework is the *Authentication Assurance Level* (AAL)[3] described in the *IDABC Authentication Policy*[4]. **The IDABC report is based on a survey of all European government initiatives proposing some form of authentication levels policy (there are 15 European countries which have some kind of policy). It provides a model which is intended to be mappable to all existing European policies**. Authentication Policy is considered to be a guideline which might help a governmental organization to develop a comprehensive approach for determining the appropriate level of e-authentication assurance[3] it needs and to select the best available technical solutions. At the end of this procedure, an e-Government application might be mapped to a specific AAL, in terms of identification and authentication requirements. Four AALs have been defined to describe different levels of confidence in a claimed identity and, in the consequence, engage an e-Government application. According to the AAL presented by entities (identity claimants), e-Government applications will take reasoned decisions and provide appropriate authorizations to the citizens and enterprises.

---

[1] Decision 2004/387/EC of 28 April 2004, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_181/l_18120040518en00250035.pdf.
[2] http://ec.europa.eu/idabc/en/document/6484/5644.
[3] *Authentication Assurance*: 'A measure of confidence that the security features and architecture of the Identity Management capabilities accurately mediate and enforce the security policies understood between the Relying Party and the Identity Provider', ITU-T Y.IdMsec.
Assurance Level, 'A quantitative expression of Assurance agreed between a Relying Party and an Identity Provider', ITU-T Y.IdMsec.
Relying Party: 'The recipient of a message that relies on a request message and associated assertions to determine whether to provide a requested service', Liberty Alliance.
Identity Provider: 'Kind of Service Provider (SP) that creates, maintains, and manages identity information for principals and provides authentication to other service providers within a federation, such as with web browser profiles', OASIS SAML 2.0. All the abovementioned definitions are available at:
http://wiki.enisa.europa.eu/index.php?title=Living_List_of_Identity_Management_Terminology.
[4] http://ec.europa.eu/idabc/servlets/Doc?id=18227.

Several different technologies have been suggested to integrate AALs in applications. According to [5], Security Assertion Markup Language (SAML) is a very promising technology to support IDABC Authentication Policy because it supports *federation* which is the dominant movement in identity management today. Federation refers to the establishment of business agreements, cryptographic trust, and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions. Just as web services promise to enable integration between business partners through loose coupling at the application and messaging layer, federation does so at the identity management layer – insulating each domain from the details of the others" authentication and authorization infrastructure. Key to this loose coupling at the identity management layer are standardized mechanisms and formats for the communication of identity information between the domains. Furthermore, 'identity federation' has already been addressed in the IDABC Work Programme[6] as a key element to help '…*in the establishment of common rules and semantics for sharing identity information*' under the Common Identity Management Service (CIMS) action. SAML defines just such a standard. SAML is a product of Organization for the Advancement of Structured Information Standards (OASIS) and the first release, SAML 1.0 was announced in November 2002. Since then a lot of extensions have been suggested and justifications have been proposed to keep up with technology evolution. The result of this progress is SAML v2.0 introduced in March 2005.

According to [12], 83% of the Identity Providers (IdPs[3]) surveyed would be willing to follow some technical guidance on AAL if there were any. Furthermore, standardization of authentication levels has already been recognized as one of the key elements towards the development of a pan-European eIdM system in the "Roadmap for a pan-European eIdM Framework by 2010". The goal of the current report is threefold: to explore the options available for expressing IDABC AALs using SAML v2.0 and provide stakeholders with pros and cons of each option, to document the results of ENISA's work in mapping IDABC AALs to Authentication Context[7] for OASIS SAML V2.0[8], and provide stakeholders with input when taking reasoned decisions on e-Government frameworks and applications. This report therefore serves not only as a means to provide technical guidance to stakeholders involved in IDABC initiatives but also as a tool to support European policy on electronic identity. On the other hand, in depth analysis of different AAL definitions-approaches, IDABC multilevel authentication policy review and competitive federation technologies comparison are not included within the scope of this report.

1.1 LoA definitions and approaches

Although there are excellent state of the art reviews[9] of eIDM in general, this report focuses on initiatives aiming to map the concept of AAL (or similar ones) to existing standards. The concept of Assurance Level has been used in different contexts so far, e.g. IT product evaluation and IS audit, authentication. In the context of electronic authentication, the UK Office of the e–Envoy (now the Cabinet Office e-Government Unit) was the first to introduce the concept of an 'authentication level'

[5] http://ec.europa.eu/idabc/servlets/Doc?id=29620
[6] IDABC Work Programme, Third Revision, SECTION I, Project of common interest, Horizontal measures, http://ec.europa.eu/idabc/servlets/Doc?id=25302.
[7] In some situations, an entity may want additional information to determine the level of confidence in the information in a delivered assertion. Authentication context is an XML document which permits the representation of this additional information.
[8] 'Authentication Context for the OASIS Security Assertion Markup Language', OASIS Standard, 15 March 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf. (SAML) V2.0
[9] http://wiki.enisa.europa.eu/index.php?title=Electronic_Identity_Directory

in its 'E-government Authentication Framework' guideline published in 2000[10]. Since then, several terms have been used to describe the concept of authentication level in this context: Personal Identity Verification (PIV) Authentication Level, PIV Assurance Level, Identity Assurance Level, Authentication Profile, Level of Assurance (LoA) and AAL, are some of them. In the context of this report, we will use these terms interchangeably. A widely accepted definition of the term considers assurance level as
1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued[11].

To date, the OMB/NIST LoA specification[11] remains the most comprehensive set of guidelines for IdPs to implement systems achieving a well-defined LoA and for Service Providers (SPs) to use the LoA for a fine-grained access control[12]. A number of worldwide communities have either adopted this approach or are in the process of making their approaches compatible or interoperable with the OMB/NIST LoA specification. These communities include the governments of US, UK, Australia, Canada, and EU, Higher Education (HE) federations of the US, Switzerland, Denmark, Finland, Sweden, Norway, France and Australia and New Zealand, the US National Institutes of Health (NIH), the US federal Electronic Authentication Federation (EAF) and the industry-led Electronic Authentication Partnership (EAP). IDABC has adopted an approach similar to OMB/NIST LoAs, based on risk assessment. They have defined a four levels model as proposed by the US Government Office of Management and Budget (OMB). Section 3 analyses IDABC AAL requirements for each level.

From an (authentication) policy makers' point of view, risk assessment is the most important consideration for competent authorities and/or organizations when trying to establish (define) a LoA based authentication framework. Despite the differences in assessment methodology, a risk based approach is followed when defining an Authentication Level[13]. According to this approach, each Authentication Level expresses a certain amount of potential harm or impact which an erroneous electronic authentication may cause to a specific electronic application. In order to help stakeholders to cope with identified risks (as expressed within identified Authentication Levels) involved in electronic authentication, most of the abovementioned initiatives have combined identified risks with the measures needed to mitigate these risks. Two general categories of measures have been identified so far:

a) the measures taken by IdPs to identify and register entities (identification/registration phase); and
b) the mechanisms used during the electronic authentication phase.

These initiatives differ only in the measures and mechanisms described within each category. Numbering of Authentication Levels, usually in ascending order, is another common characteristic of LoA initiatives. For instance AL0 represents a lower level of potential impact than AL1 according to UK Authentication Framework. Finally, the number of LoAs addressed within the most of the

[10] Office of the e-Envoy, Authentication Framework v1.0, Dec. 2000, http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/authentic.pdf.
[11] e-Authentication Guidelines for Federal Agencies, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.
[12] E-infrastructure Security: Levels of Assurance, Final Report, The University of Manchester, 2007, http://www.jisc.ac.uk/media/documents/programmes/einfrastructure/finalreport.pdf.
[13] According to [12] study, 92% of the IdPs surveyed would be willing to adopt the risk-based approach to access control that incorporates LoA.

existing electronic Authentication Frameworks varies between two and four (ranging from 1, least sensitive to 4 most sensitive).

On the other hand, from a stakeholders' (individuals, vendors, other organizations) point of view, the ultimate goal of every e-Government Authentication Framework is to provide them with guidance to satisfy their needs for identification and authentication in a comprehensive way. Although the implementation varies, in most of the cases, stakeholders have to follow the following steps to determine the assurance level to map a process and/or application:

- Risk assessment. In the first place, an assessment of the risks involved in the process is conducted. Risk factors are usually considered to be threats involved in the procedure, the likelihood that the threat might take place, the impact on the organization, the sensitivity (in terms of data protection) and confidentiality level of the information exchanged during specific transactions of the procedure etc. This procedure yields a measure of the severity of potential harm of adverse impacts to the system, if there is an error in identity authentication.
- Mapping identified risks to a specific AAL: the risks have been identified and stakeholders should tie the potential impact of the risks to the proper AAL to be used.
- Measures implementation: mechanisms (controls) which satisfy the registration and authentication requirements described in the already addressed AAL, might be selected and, in the consequence, implemented.

Following a similar approach, IDABC has proposed to sectoral application owners six steps to follow in order to develop their own Authentication Policy:

Step 1: Conduct a rapid risk assessment of the sectoral application or system,
Step 2: Map Identified Risks to the Applicable Authentication Assurance level,
Step 3: Select procedures and technology that, at a minimum meets the technical requirements for the required level of assurance,
Step 4: Sign a Mutual Recognition Agreement between involved parties,
Step 5: Validate that the implemented system has achieved the required assurance level; and
Step 6: Periodically reassess the system to determine technology refresh requirements.

The reader may find more information, concerning determination of IDABC AAL, at[14].

1.2 IDABC AAL Requirements

The IDABC model has four AALs, layered according to the severity of the impact of damages that might arise from misappropriation of a person identity:

1. Level 1: Minimal Assurance
2. Level 2: Low Assurance
3. Level 3: Substantial Assurance
4. Level 4: High Assurance

Regardless of the strength of the mechanisms proposed by each AAL, the authentication of an entity consists of two main phases, according to [4]:

1. The Registration phase, which is the process by which a user gains a credential such as a username or digital certificate for subsequent authentication. The registration is generally made of the following steps:

i. The Identity Proofing, during which the real-world identity of the claimant is verified;
ii. The claimant's details registration and the Token Delivery; and
iii. The delivery of Electronic Credentials;

2. The Electronic Authentication phase, also called Proof of Possession (or PoP), during which the electronic identity of the claimant is verified. Depending on the chosen architecture, an additional

[14] http://ec.europa.eu/idabc/en/document/6484/5644

process called "assertion delivery" involving a trusted entity called "Relying Party[3]" (RP) may also occur during this phase. Since assertion delivery is not included in standard IDABC AAL specifications, the report will make no further reference to this process.

Requirements for each specific AALs are described in Table 2 (pp. 11), Table 5 (pp. 16), Table 8 (pp. 22) and Table 11 (pp. 31) respectively. Each table is logically divided into two major areas; each one represents one of the two main AAL phases (registration and authentication) already described. Each area consists of three columns; the first column refers to the step within the relevant phase while the second to the requirement itself. The third column refers to the capacity of SAML v2.0 to express the specific requirement and will be further described in the following sections. The reader may notice that references to previous AAL levels also appeared in the third column from time to time. When such a reference is appeared this means that the requirement has already been satisfied at a higher AAL and there is no need to describe it again at the specific AAL. Finally, to facilitate referencing at later stages, each requirement is accompanied with a number at the end. This number is used to refer to the specific requirement during the gap identification section for each AAL.

1.3 Other possible technologies

The first effort to put the LoA-linked access control concept into software implementation was made by the FAME-PERMIS project15. The project developed middleware extensions for the Shibboleth (supported by SAML) infrastructure to facilitate multifaceted authentication and LoA-linked fine-grained access control. The FAME system integrates a wide range of authentication services, supporting the use of different token types, and derives levels of authentication assurance in conformance with the NIST standard[12].

There are two dominant protocols in federation for e-Government applications developed so far[16]:

1. SAML has been adopted by many security frameworks (e.g. Shibboleth, E-Authentication Federation and Liberty Alliance) for communicating security and identity information. LoA value can also be conveyed as part of one of the attributes in a SAML assertion. In addition, SAML v2.0 Authentication Contexts can be used to provide a SP with additional information about an authentication process performed by an IdP, such as identity vetting process that was used to initially associate a subject and their identity, credential management and storage, authentication method, mechanisms for minimizing compromise of credentials, credential renewal frequency, etc. Such rich information about the authentication process can be used by the SP to put the level of authentication assurance into a risk management context. SAML 2.0 has the concept (originally defined in Liberty Alliance ID-FF) of Authentication Context. Authentication Context provides a set of related mechanisms by which IdPs and SPs can discuss the details behind an Authentication Statement. The IdP is able to provide details beyond the mere fact of authentication, and the SP is able to indicate its requirements for such details.
2. WS-Federation is an identity federation specification which defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms[17]. It is part of what is called Web Services Security framework – a framework developed by several companies[18] for providing Web services with security.

[15] The FAME-PERMIS project, http://www.fame-permis.org.
[16] Other important protocols addressing the functionality of identity management are OASIS' eXtensible Access Control Markup Language (XACML), Service Provisioning Markup Language (SPML) and eXtensible Resource Identifier (XRI).
[17] Web Services Federation Language (WS-Federation), Version 1.1 December 2006.
[18] IBM, Microsoft, RSA Corp. and Verisign are some of them.

To the best of our knowledge, WS-* does not provide any way of modeling contextual aspects of authentication mechanisms suitable for specifying authentication policy as SAML does. An exhaustive comparison between these two frameworks (SAML and WS-Federation) is provided at 'eID Interoperability for PEGS, Report on assessment of eIDM technical solution'. According to this study these protocols are mostly similar although a small advantage is given to SAML. This is explained by the fact that, the WS-Federation has several dependencies to other WS-* standards (link to WS-Trust is the most important one) and at the same time SAML 2.0 protocol does not have any dependencies to other standards. This makes the implementation of the SAML 2.0 standard more robust and explains the fact that currently we are seeing more and more implementations of SAML 2.0 standard without any other dependencies (e.g. Liberty).

1.4 Bindings between LoA's and SAML

There are currently several approaches to how LoA information can be represented in SAML v2.0:

1. Instead of presenting AAL in a format like the one described in the document containing OASIS Authentication Context, many initiatives[19] have adopted an extra mandatory attribute which is used to express the level for easy processing. The `<AssuranceLevel>` attribute which provides the SP an indication of how strongly the user was authenticated. In the case of IDABC, numeric values (1, 2, 3, and 4) will be assigned to the attribute. Below is given a hypothetical example representation of the assurance level attribute:

```
<saml:Attribute
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="europa:eu:saml:attribute:AssuranceLevel">
<saml:AttributeValue xsi:type="xs:string" >2</saml:AttributeValue>
</saml:Attribute>
```

In this case, the `<AssuranceLevel>` attribute is communicated between IdP and SP via the `<RequestedAuthnContext>` element. Whenever this approach is adopted, LoA is part of the authorization process. For example, authorization decisions would be made based on the following tuple: (Subject, Target, Action, LoA), rather than the traditional (Subject, Target, Action), where *Subject* is the entity accessing the resource, *Target* is the resource itself, and *Action* describes what action the entity is allowed to perform on the target resource.
The major advantages of this approach are the easiness in terms of taking access control decisions-only based on the comparison of the numeric values expressing the authentication level-and the simplicity of implementation –all that is needed is a numeric value to represent an AC. On the other hand, intitiatives adopted this approach define also an extra mandatory attribute which is used to tell the assurance level for easy processing. The use of an extra attribute may be problematic for many software products to handle because commercial implementations may not work with them.
2. Some initiatives have tried to map the proposed LoAs to existing SAML v2.0 authentication context classes. In the case of IDABC, an example is given in the following table.

IDABC AAL	Existing Authentication Context Reference
4	SmartcardPKI
3	SoftwarePKI
2	PasswordProtectedTransport
1	Password

Table 1: Mapping IDABC AALs to existing SAML v2.0 AC classes

[19] i.e. eAuthentication initiative: http://www.cio.gov/eauthentication/index.cfm, DK-SAML: http://www.oiosaml.info/

Similarly to the abovementioned opition, the main advantages of this approach are the ease of taking access control decisions based only on a check if the presented AC class is included or not in a predefined set of approved AC classes (as defined in the local authentication policy,) - and the simplicity of implementation. Several ready-to-use AC classes covering a wide range of authentication context use cases have already been provided by OASIS. On the other hand, the main disadvantage of this approach is the lack of expressiveness in semantically rich environments involved, especially during the registration phase of authentication.

The IDABC multilevel authentication framework is such an environment. According to our analysis, we have identified several points of mismatch between IDABC AALs requirements and existing AC classes. For example, in order to express the AAL 3 registration requirements we have identified seven required extensions (see Table 10) to the existing XML schema. Furthermore, the electronic authentication phase (or PoP) suffers from similar, albeit less severer, expressivess problems in describing the registration phase.

SAML's conceptual model (see Figure 1) distinguishes technical protection of the secret key used for PoP from the PoP phase which is not the case for IDABC authentication model. That is why, OASIS has mainly focused on the PoP and principal authentication mechanism aspects of authentication phase leaving the technical protection element unspecified, in most of the cases,. As a result, only seven out of twenty five classes, incorporate specifications referring to the technical protection element.

3. To bridge the gaps identified when adopting the previous option, provideXML-based extension data structures for requirements not satisfied by the existent data model, thus redefining the existing SAML v2.0 AC schema. This approach results in four (one for each IDABC AAL) SAML v2.0 AC classes. Examples of such classes are described in [Section 3. Gap Analysis]
4. In order to circumvent the problems introduced by the abovementioned approaches, recent initiatives[20] tend to adopt a different solution; instead of using the full expressiveness of the authentication context schema, each level class is characterized by a URI, and the body of the context class simply contains a reference to the external documentation that defines the LoA scheme[21] in a natural language format. For example, such a URI may link to a hypothetical location such http://ec.europa.eu/idabc/loa/idabc-loa1.pdf where the specifications of IDABC AAL 1 may be found in a .pdf file (one such file should be delivered for each AAL).This is the approach which has been used in the draft proposal [[22]].There are two limitiations when using this approach[20]:

a) the URIs representing the levels must be hard-wired into every system in the deployment, and the ordering of the URI levels must be decided and configured out-of-band;
b) the authentication assertions carrying these LoA authentication context URIs do not convey any details about the authentication event, although such details are implied by the level indicated by the URI.

Despite these limitations, we consider that both the highest degree (unlimited actually) of expressiveness and the simplicity of implementation-a URI for each AAL is needed, making this approach the most well promising for expressing the IDABC multilevel authentication policy.

[20] Level of Assurance Authentication Context Profiles for SAML 2.0, Working Draft 01, OASIS.
[21] Level of Assurance Authentication Context Profiles for SAML 2.0, http://www.oasis-open.org/committees/download.php/28706/sstc-saml-loa-authncontext-profile-draft-01.pdf.
[22] http:// www.oasis-open.org/committees/down**loa**d.php/28706/sstc-**saml**-**loa**-authncontext-profile-draft-01.pdf

Although it is quite obvious that all these approaches are valid and could be accepted, there is still a lot of controversy about which is the most favorable. Each approach presents specific advantages and disadvantages, highlighted in this report.

2 Gap Analysis

2.1 Mapping AAL requirements to SAML v2.0 Authentication Context

SAML v2.0 Authentication Context data model is categorized in the Authentication Context schema as follows[8]:

1. Identification - Characteristics that describe the processes and mechanism the authentication authority uses to initially create an association between a subject and the identity (or name) by which the subject will be known.
2. Technical Protection - Characteristics that describe how the "secret" (the knowledge or possession of which allows the subject to authenticate to the authentication authority) is kept secure.
3. Operational Protection - Characteristics that describe procedural security controls employed by the authentication authority (for example, security audits, records archival).
4. Authentication Method - Characteristics that define the mechanisms by which the subject of the issued assertion authenticates to the authentication authority (for example, a password versus a smartcard).
5. Governing Agreements - Characteristics that describe the legal framework (e.g. liability constraints and contractual obligations) underlying the authentication event and/or its associated technical authentication infrastructure.

All this information is encapsulated in a SAML v2.0 element named `<AuthenticationContextDeclaration>` declared in the following way in the SAML v2.0 AC schema.

```
<xs:element name="AuthenticationContextDeclaration"
type="AuthnContextDeclarationBaseType">

<xs:complexType name="AuthnContextDeclarationBaseType">
     <xs:sequence>
          <xs:element ref="Identification" minOccurs="0"/>
          <xs:element ref="TechnicalProtection" minOccurs="0"/>
          <xs:element ref="OperationalProtection" minOccurs="0"/>
          <xs:element ref="AuthnMethod" minOccurs="0"/>
          <xs:element ref="GoverningAgreements" minOccurs="0"/>
          <xs:element ref="Extension" minOccurs="0"
     maxOccurs="unbounded"/>
     </xs:sequence>
     <xs:attribute name="ID" type="xs:ID" use="optional"/>
</xs:complexType>
```

Note that, for brevity's sake, `AuthnContextDeclarationBaseType` will be omitted whenever we referred to one or more of its sub elements, for the rest of this report. On the contrary, referencing will always be in place for the six basic sub elements and their subordinate elements and/or their possible extensions. `AuthnContextDeclarationBaseType` is considered to be the parent element of all the elements presented in Figure 1.

The following figure is a (proposed) reference model for mapping IDABC AAL requirements (see § 1.2) with SAML v2.0 specifications.

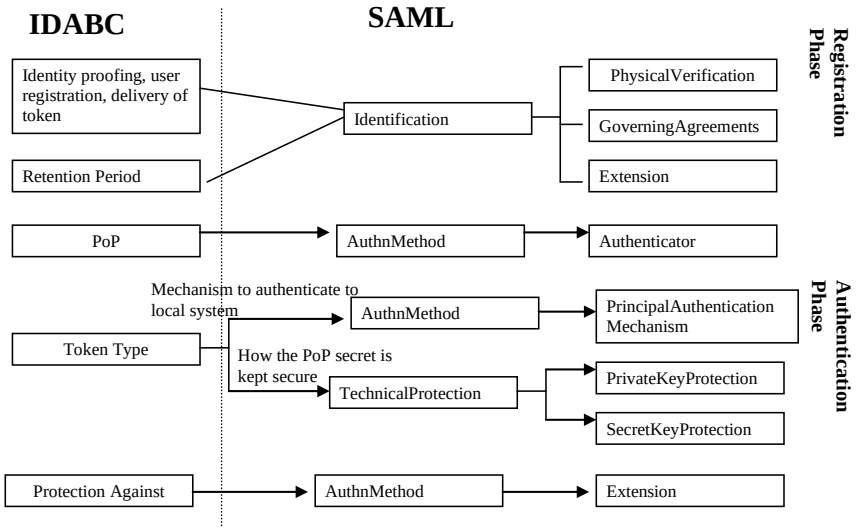

Figure 1 Conceptual mapping IDABC requirements to SAML v2.0 elements

Note that IDABC does not refer to elements which could be categorized neither under 'Operational Protection' element (e.g. audits, records archival etc) or Governing Agreements (e.g. liability constraints etc) element. I.e. there are some elements of Authentication Context which are not covered by the IDABC model.

The following sections (one per AAL) provide a detailed analysis of the mapping between IDABC AAL requirements to SAML v2.0 AC classes. Each section is further divided into three major subsections:

1. *IDABC Requirements*: a detailed presentation of relevant requirements written in IDABC Authentication Policy document[4]. More information on this subsection has already been provided in § 1.2.
2. *Gaps:* a) a mapping table between IDABC AAL requirements and existing SAML v2.0 elements; and b) a mapping between relevant IDABC AAL requirements and proposed extensions to existing SAML v2.0 AC[23]; the first column is the requirement number, the second is a possible position[24] for the extension to take place within existing SAML v2.0 AC and the third is the proposed XML based representation of the relevant data structure.
   IDABC requirements may or may not be represented using existing SAML v2.0 elements. This information is summarised in the third column of IDABC AAL requirements description tables (Table 2, Table 5, Table 8, and Table 11). A value of 'expressible' means that the requirement can be expressed using the SAML v2.0 elements as described within the already existing SAML v2.0 AC[25] while a value of 'not expressible' means that the requirement cannot be expressed using the existing SAML v2.0 elements and an extension

[23] The authentication context declaration schema has well-defined extensibility points through the <Extension> element. Interested parties can use this element to insert additional authentication context details for the SAML assertions. These additional elements MUST be in a separate XML Namespace to that of the authentication context declaration base or class schema that applies to the declaration itself.

[24] The reader might have in mind that the proposed position actually refers to the `<Extension>` element of the corresponding data model element. For example when 'Identification' is referred as a proposed extension position then the `<Extension>` element of the `<Identification>` element is meant.

[25] saml-schema-authn-context-2.0.xsd

should be provided. Note that the term 'expressible' is used to describe only the fact that SAML v2.0 has identified a specific element which corresponds approximately to an element of the IDABC model. There are cases where the proposed by OASIS elements/values might NOT be suitable to express the requirement in the most accurate, concise and comprehensive way. Appropriate comments are provided in these cases. The required SAML v2.0 elements (either existing or extensions) are described in detail in the corresponding paragraphs.

3. *Suggested AC class*: the proposed XML schema for the corresponding AAL. Each schema is logically divided into two areas determined by a `<redefine>` element: the first area is devoted to the proposed extension elements while the second is the description of the proposed data model (see also footnotes 23 and 24).
4.

Specific notation is used whenever an existing SAML v2.0 element is referenced. For example, *Identification->Governing Agreements* is pointing to the `<Governing Agreements>` sub-element of `<Identification>` element. *AuthnMethod->PrincipalAuthenticationMechanism->*{Smartcard, ActivationPin} means that `<PrincipalAuthenticationMechanism>` sub-element of `<AuthnMethod>` element may take the values of (either) `Smartcard` and(or) `ActivationPin`.

We have used a straightforward naming scheme to map authentication levels to class names. For example, the declaration of AAL1 namespace might be `targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelOne"`.

Finally, the IDABC allows RPs to rely on any authentication whose assurance level is greater than or equal to the assurance level required by the RP. In other words, higher-level credentials can be used at lower assurance level RPs – significantly enhancing credential re-use. For example, an assurance level 1 RP can rely on an assurance level 2 authentication. Another example is an assurance level 2 RP can rely on a level 4 authentication. This functionality is left to the implementation of application vendors.

2.2 IDABC Authentication Level 1 (Minimal Assurance)

2.2.1 Requirements description-analysis

Level 1 registration is appropriate for application transactions in which damages that might arise from misappropriation of real world identity would have a Negligible or Low impact[26]. The registration is purely claims based. This registration level is heavily used by lots of Internet applications (webmails, on-line, auctions, etc.).

REGISTRATION PHASE	IDABC REQUIREMENT	EXPRESSIBLE/NOT EXPRSESSIBLE IN SAML V2.0 EXISTING CONTEXT

[26] According to Impact Severity Scaling described in 'Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms', http://ec.europa.eu/idabc/servlets/Doc?id=29622.

Procedure for identity proofing, user details registration, delivery of token and credentials	The RA **(1)**	expressible
	can be any entity whose authentication methods are accepted in an eGovernment application. There is no requirement to prove the identity or maintain a record of the facts of registration. Identity assertions of claimants are accepted. **(2)**	expressible
	Only the e-mail address must be unambiguous and valid. There is no specific requirement for delivery of the token or credential. **(3)**	expressible
Retention period for registration data	**None**	-
ELECTRONIC AUTHENTICATION PHASE		
Authentication Protocol for Proof of Possession (PoP)	Most of the time, Challenge-reply password PoP **(4)**	expressible
	However, according to risk assessment, could also be: Tunelled password PoP	See AAL2
	One-time (or strong) Password PoP	See AAL3
	Symmetric Key PoP	See AAL4
	Private Key PoP	See AAL4
Token Type	Most commonly Password or PIN tokens will be chosen. **(5)**	expressible
	All token types are acceptable.	See AAL2, AAL3, AAL4
Requires the application owner to implement protection against	Replay **(6)**	Not expressible
	On-line guessing **(7)**	Not expressible

Table 2: IDABC AAL 1 requirements description

Most AAL1 requirements are either expressible using existing SAML v2.0 elements or left for clarification in the next AALs description. This is due to: a) minimal registration requirements; and high rate of reusability of stricter AALs credentials.

2.2.2 Gaps

2.2.2.1 Existing Authentication Context

The following information summarizes elements within SAML v2.0 Authenticaton Context class which CAN map to AAL1 requirements.

Req. No	SAML v2.0 AC Element
1	OrganizationType
2, 3	Identification->Governing Agreements
4	AuthnMethod->Authenticator->{SharedSecretChallengeResponse}
5	AuthnMethod->PrincipalAuthenticationMechanism->{Password}

Table 3: Mapping IDABC AAL1 requirements to existing within SAML v2.0 AC class elements

Note thehe `<OrganizationType>` element actually is not defined in Authentication Context but in theSAML v2.0 Metadata[27] schema. For this reason an `<import/>` element is needed in the proposed AAL1 Context class. This also holds true for the rest of the proposed AAL Context classes. The rest of the registration requirements are mapped to `Identification->Governing` Agreements elements.

`The SharedSecretChallengeResponse` element expresses the challenge reply PoP. This type of authenticator makes use of symmetric cryptography. At this point, the IDABC requirement is not very prescriptive with regards to the use of encryption or not. Non-cryptographic challenge reply protocols have not identified in the existing SAML v2.0 AC.

2.2.2.2 Proposed Extensions

The IDABC level 1 requirement: ”protection must be provided against...”, is the only requirement at this AAL which may not be addressed using the elements in the existing SAML v2.0 AC class. That is why an extension to the `<AuthnMethod>` extension element is suggested. This element also, though enhanced with other addressed attacks, is also required for the rest of the AAL specifications.

Req. No	SAML AC Element – Extension Point	Proposed Elements
6,7	AuthnMethod	<element name="AttacksAddressed" type="AttacksAddressedType"/> <xs:annotation> <xs:documentation> The AuthnMethod Extension MUST NOT occur any other place than in the Extension element of the AuthnMethod Element within the AuthnContextDeclarationBaseType element within an Authentication Context declaration. </xs:documentation> </element> <xs:simpleType name="AttacksAddressedType "> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="Replay" minOccurs=”0”/> <xs:enumeration value="Online Guessing” minOccurs=”0”/> </xs:restriction> </xs:simpleType>

Table 4: Proposed SAML v2.0 extensions for IDABC AAL1

2.2.3 Suggested IDABC AAL1 Context Class

The following is a proposed SAML v2.0 schema, suitable to express the requirements of IDABC AAL1.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelOne"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelOne"
finalDefault="extension"
blockDefault="substitution"
version="2.0">
```

[27] saml-schema-metadata-2.0.xsd

```
<import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="saml-
schema-metadata-1.0.xsd"/>

<redefine schemaLocation="sstc-saml-context-ext-IDABC-L1.xsd">

<xs:annotation>
      <xs:documentation>This redefine section sets conditions on the extensions
in sstc-saml-context-ext-IDABC-L1.xsd so that they comply with IDABC level 1.
      </xs:documentation>
</xs:annotation>

<xs:element name="IssuingOrganization" type="OrganizationType"/>

<xs:simpleType name="AttacksAddressedType ">
      <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="Replay" minOccurs="1"/>
      <xs:enumeration value="Online Guessing" minOccurs="1"/>
      </xs:restriction>
</xs:simpleType>

</redefine>

<redefine schemaLocation="saml-schema-authn-context-types-1.0.xsd">
            <xs:annotation>
                  <xs:documentation> This section requires that extensions are
placed in the right section of the schema.
                  </xs:documentation>
</xs:annotation>
<xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnContextDeclarationBaseType">
                  <xs:sequence>
                        <xs:element ref="Identification" minOccurs="0"/>
                        <xs:element ref="TechnicalProtection" minOccurs="0"/>
                        <xs:element ref="OperationalProtection" minOccurs="0"/>
                        <xs:element ref="AuthnMethod"/>
                        <xs:element ref="GoverningAgreements" minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="ID" type="xs:ID" use="optional"/>
            </xs:restriction>
</xs:complexContent>

</xs:complexType>
      <xs:complexType name="AuthnMethodBaseType">
            <xs:complexContent>
                  <xs:restriction base="AuthnMethodBaseType">
                        <xs:sequence>
                              <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
                              <xs:element ref="Authenticator"/>
                              <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
                              <xs:element ref="Extension" minOccurs="1"/>
                        </xs:sequence>
                  </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
```

```
      <xs:complexContent>
            <xs:restriction base="PrincipalAuthenticationMechanismType">
                  <xs:sequence>
                        <xs:element ref="Password"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthenticatorBaseType">
                  <xs:sequence>
                        <xs:element ref="SharedSecretChallengeResponse"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentificationType">
      <xs:complexContent>
            <xs:restriction base="IdentificationType">
                  <xs:sequence>
                        <xs:element ref="GoverningAgreements"/>
                        <xs:element ref="Extension" minOccurs="0"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

</xs:redefine>
</xs:schema>
```

2.3 IDABC Authentication Level 2 (Low Assurance)

3.2.1 Requirements description-analysis

Level 2 registration is appropriate for application transactions in which damages that might arise from misappropriation of real world identity would have a Medium impact. In many cases the Level 2 registration can be accomplished online and immediately.

REGISTRATION PHASE	**REQUIREMENT**	**EXPRESSIBLE/NOT EXPRSESSIBLE IN SAML V2.0 EXISTING CONTEXT**
Procedure for identity proofing, user details registration, delivery of token and credentials	The token/credential must be issued by a body **(1)**	expressible
	which is subject to a specific government agreement or under government supervision. **(2)**	expressible

	No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification. The assertions must undergo a basic validation, either by cross-referencing the provided assertions (i.e. the claimed attributes which allow the unique identification of the claimant) with an official identity source or identity database from a neutral and trustworthy source such as a bank, insurance agency or government department, or implicitly (e.g. by sending credentials to the official registered domicile of the claimant or by requiring the token/credentials to be collected personally by the claimant during which identity documents must be provided to validate the assertions). **(3)**	expressible
	3. Delivery The token/credential must be sent out by two separate mailings, at least one of which must be by physical mail (not e-mail) to the official address of the claimant as shown in an official identity database in which the physical address was registered. **(4)**	expressible
	Or The token/credential may be downloaded directly by the claimant following the registration procedure, by following a link which was sent to an e-mail address communicated by the claimant during the registration process; in this case, the e-mail link may not be valid for more than 24 hours. **(5)**	expressible
Retention period for registration data	A record of the facts of registration shall be maintained by the CSP or its	Not expressible

	representative. The suggested minimum retention period for registration data for Level 2 credentials is 5 years beyond the expiration or revocation (whichever is later) of the credential. **(6)**	
ELECTRONIC AUTHENTICATION PHASE		
Authentication Protocol for Proof of Possession (PoP)	Most of the time Tunneled **(7)**	expressible
	or One-time Password PoP.	See AL3
	However, according to risk assessment, could also be: - Symmetric Key PoP - Private Key PoP	See AL4
Token Type	All tokens are acceptable except the sole use of user chosen passwords. At a minimum a randomly generated password or PIN token is acceptable; preferably a One-time password device token should be used. **(8)**	expressible
Requires the application owner to implement protection against	Eavesdropper **(9)** Replay **(10)** On-line guessing **(11)**	Not expressible

Table 5: IDABC AAL 2 requirements description

3.2.2 Gaps

2.2.3.1 Existing Authentication Context

The following table maps the abovementioned IDABC AAL2requirements to SAML v2.0 existing elements.

Req. No	SAML v2.0 AC Element
1	OrganizationType
2,3,4,5	Identification->Governing Agreements
7	AuthnMethod->Authenticator->{RestrictedPassword}
8	AuthnMethod->PrincipalAuthenticationMechanism->{Token}

Table 6: Mapping IDABC AAL2 requirements to existing within SAML v2.0 AC class elements

Tunnelled PoP representation is similar to the `<PasswordProtectedTransport>` AC[28] class which is applicable when an entity authenticates to an authentication authority through the presentation of a password over a protected session. These requirements are expressed by restricting `Authenticator` to `RestrictedPassword` and `AuthenticatorTransportProtocolType` to one of {`SSL`, `MobileNetworkRadioEncryption`, `MobileNetworkEndToEndEncryption`, `WTLS`, `IPSec`} protocol values.

[28] Described in saml-schema-authn-context-srp-2.0.xsd.

Current AAL2 specification dictate that the token type should be either randomly generated password (soft) or one time password device (hard) token. This fact produces difficulties in defining the following elements:
a) PrincipalAuthenticationMechanismType: randomly generated password could be expressed by restricting `PrincipalAuthenticationMechanismType` to `RestrictedPassword` , albeit with deviations in the meaning, while one time password by restricting the same element to `Token` value. Due to the fact that `PrincipalAuthenticationMechanismType` is a `sequence` element instead of a `choice`, this requirement suffers from lack of expressiveness. A restriction of `PrincipalAuthenticationMechanismType` element to `choice` might be proved adequate to express this specific requirement.
b) KeyStorageType: in this particular case, this element would express contradictory values (soft/hard) for a token. To this end, no restriction of TechnicalProtectionBaseType element is an option.

IDABC AAL2 Token type is an ambiguous requirement with regards to SAML v2.0 in that it only defines that the token should be hardware. Details regarding the length, in bits, of the random seed used in the time synchronization token (SeedLength element) and the portability of the token (DeviceInHand element) are not provided. Furthermore, no documentation (e.g. what is its usage) is provided by OASIS with regards to DeviceInHand element.

2.2.3.2 Proposed Extensions

Requirements not expressible within SAML v2.0 AC are represented in the following table along with the proposed extensions.

Req. No	**SAML AC Element – Extension Point**	**Proposed Element**
6	Identification	<xs:element name="RegistrationDataRetention"> <xs:annotation> <xs:documentation> This element indicates the length of time for which secondary registration data is stored. The RegistrationDataRetention element MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> <xs:attribute name=”retentionPeriod” type="xs:duration" use="required"/> </xs:element>
9,10,11	AuthnMethod	<element name="AttacksAddressed" type="AttacksAddressedType"/> <xs:annotation> <xs:documentation> The AuthnMethod Extension MUST NOT occur any other place than in the Extension element of the AuthnMethod Element within the AuthnContextDeclarationBaseType element within an Authentication Context declaration. </xs:documentation> </element> <xs:simpleType name="AttacksAddressedType "> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="Eavesdropper" minOccurs=”0”/> <xs:enumeration value="Replay" minOccurs=”0”/> <xs:enumeration value="Online Guessing” minOccurs=”0”/> </xs:restriction> </xs:simpleType>

Table 7: Proposed SAML v2.0 extensions for IDABC AAL2

A new extension has appeared in this class and is related to the retention period for registration data. This requirement, though assigned to different numeric values, is also present in the rest of the authentication contexts. Finally, "Eavesdropper" attack has been added to the `AttacksAddressedType` suggested element.

3.2.3 Suggested IDABC AAL2 Context Class

The following XML schema is proposed to express IDABC AAL2 requirements.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelTwo"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelTwo"
finalDefault="extension"
blockDefault="substitution"
version="2.0">

<import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="saml-
schema-metadata-2.0.xsd"/>

<redefine schemaLocation="sstc-saml-context-ext-IDABC-L2.xsd">

<xs:annotation>
      <xs:documentation>This redefine section sets conditions on the extensions
in sstc-saml-context-ext-IDABC-L2.xsd so that they comply with IDABC level 2.
      </xs:documentation>
</xs:annotation>

<xs:element name="IssuingOrganization" type="OrganizationType"/>

<xs:complexType name="RegistrationDataRetentionPeriodType">
      <xs:attribute name=" retentionPeriod " type="xs:duration" use="required">
            <xs:restriction base="xsd:duration">
                  <xsd:minInclusive value="P05Y"/>
            </xs:restriction>
      </xs:attribute>
</xs:complexType>

<xs:simpleType name="AttacksAddressedType">
      <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="Eavesdropper" minOccurs="1"/>
      <xs:enumeration value="Replay" minOccurs="1"/>
      <xs:enumeration value="Online Guessing" minOccurs="1"/>
      </xs:restriction>
</xs:simpleType>

</redefine>

<redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
            <xs:annotation>
                  <xs:documentation> This section requires that extensions are
placed in the right section of the schema.
                  </xs:documentation>
</xs:annotation>

<xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnContextDeclarationBaseType">
                  <xs:sequence>
                        <xs:element ref="Identification" minOccurs="0"/>
```

```
                        <xs:element ref="TechnicalProtection" minOccurs="0"/>
                        <xs:element ref="OperationalProtection" minOccurs="0"/>
                        <xs:element ref="AuthnMethod"/>
                        <xs:element ref="GoverningAgreements"minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="ID" type="xs:ID" use="optional"/>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnMethodBaseType">
                  <xs:sequence>
                        <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
                        <xs:element ref="Authenticator"/>
                        <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="1"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorTransportProtocolType">
      <xs:complexContent>
            <xs:restriction base="AuthenticatorTransportProtocolType">
                  <xs:sequence>
                        <xs:choice>
                              <xs:element ref="SSL"/>
                              <xs:element ref="MobileNetworkRadioEncryption"/>
                              <xs:element ref="MobileNetworkEndToEndEncryption"/>
                              <xs:element ref="WTLS"/>
                              <xs:element ref="IPSec"/>
                        </xs:choice>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                        </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthenticatorBaseType">
                  <xs:sequence>
                        <xs:element ref="RestrictedPassword"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
            <xs:restriction base="TechnicalProtectionBaseType">
                  <xs:sequence>
```

```
                        <xs:choice>
                              <xs:element ref="SecretKeyProtection"/>
                        </xs:choice>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
            <xs:restriction base="PrincipalAuthenticationMechanismType">
                  <xs:sequence>
                        <xs:element ref="Token"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
            <xs:restriction base="SecretKeyProtectionType">
                  <xs:sequence>
                        <xs:element ref="KeyActivation"/>
                        <xs:element ref="KeyStorage"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyStorageType">
      <xs:complexContent>
            <xs:restriction base="KeyStorageType">
                  <xs:attribute name="medium" use="required">
                        <xs:simpleType>
                              <xs:restriction base="mediumType">
                                    <xs:enumeration value="token"/>
                                    <xs:enumeration value="MobileDevice"/>
                              </xs:restriction>
                        </xs:simpleType>
                  </xs:attribute>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentificationType">
      <xs:complexContent>
            <xs:restriction base="IdentificationType">
                  <xs:sequence>
                        <xs:element ref="GoverningAgreements"/>
                        <xs:element ref="Extension" minOccurs="1"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

</xs:redefine>
</xs:schema>
```

Comment [KDM1]: Should we transform it to a choice: token ? RestrictedPassword

Comment [KDM2]: Any possible other acceptable values?
memory - the key is stored in memory.
smartcard - the key is stored in a smartcard.
token - the key is stored in a hardware token.
MobileDevice - the key is stored in a mobile device.
MobileAuthCard - the key is stored in a mobile authentication card.

Notes

In contrast with the previous class, minimum value of `<Extension>` elements in `<IdentificationType>` element has been set to '1'. This is due to the fact that an extension (`RegistrationDataRetention`) has been addressed for this AC class.

2.4 IDABC Authentication Level 3 (Substantial Assurance)

4.2.1 Requirements description-analysis

Level 3 registration is appropriate for application transactions in which damages that might arise from misappropriation of real world identity would have a High impact.

REGISTRATION PHASE	**REQUIREMENT**	**EXPRESSIBLE/NOT EXPRSESSIBLE IN SAML V2.0 EXISTING CONTEXT**
Procedure for identity proofing, user details registration, delivery of token and credentials	The token/credential must be issued by a body. **(1)**	expressible
	which is subject to a specific government agreement or under government supervision. **(2)**	expressible
	Personal appearance is required. **(3a)**	Not expressible
	During registration, the claimant must present an official identity document such as an identity card, passport or drivers license. **(4a)**	Not expressible
	Or alternatively (5)	Not expressible
	provide third party corroboration from at least two neutral and trustworthy sources such as bank, insurance agency or government department. **(4b)**	Not expressible
	Or alternatively (6)	Not expressible
	No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and	Not expressible

	which are signed using a qualified signature, which the RA validates. **(3b)**	
	3. Delivery At a minimum: The token/credential must be sent out by registered mail after prior validation of the claimed address against an official identity database in which the physical address was registered **(7)**	expressible
Retention period for registration data	A record of the facts of registration shall be maintained by the CSP or its representative. The suggested minimum retention period for registration data for Level 3 credentials is 7 years beyond the expiration or revocation (whichever is later) of the credential. **(8)**	Not expressible
ELECTRONIC AUTHENTICATION PHASE		
Authentication Protocol for Proof of Possession (PoP)	Preferably One-time Password PoP **(9)**	expressible
	Symmetric Key PoP **or** Private Key PoP	See AL4
Token Type	At a minimum, Level 3 requires the use of a soft crypto token or one-time password device token. Preferably, a Soft crypto token is used.**(10)**	expressible
Requires the application owner to implement protection against	Eavesdropper **(11)**	Not expressible
	Replay **(12)**	Not expressible
	On-line guessing **(13)**	Not expressible
	Verifier Impersonation **(14)**	Not expressible
	Man-in-the-middle **(15)**	Not expressible
	Session Hijacking **(16)**	Not expressible

Table 8: IDABC AAL 3 requirements description

Several new requirements have arisen at this authentication level. Apart from the 'protection against specific attacks', the rest of the 'not expressible' within the existing SAML v2.0 AC requirements are related with the claimant's registration.

4.2.2 Gaps

2.2.4.1 Existing Authentication Context

One time password PoP is expressed by restricting the `Authenticator` element to `RestrictedPassword` or `ZeroKnowledge` values while control of soft crypto token is expressed by restricting `PrincipalAuthenticationMechanism` to a token (`Token` element) activated by a PIN (`ActivationPin` element).

Req. No	SAML v2.0 AC Element
1	OrganizationType
2	Identification->Governing Agreements

7	Identification->GoverningAgreements
9	AuthnMethod->Authenticator-> {SharedSecretChallengeResponse}
10	AuthnMethod->PrincipalAuthenticationMechanism->{Token, ActivationPin}

Table 9: Mapping IDABC AAL3 requirements to existing within SAML v2.0 AC class elements

`RestrictedPassword` and `ZeroKnowledge` elements do not accurately express the One time PoP property of this AAL; the first element is referred actually to passwords not selected by users while the second emphasize on the fact that password transmission is not encrypted. On the other hand `SharedSecretChallengeResponse` element is also not accurate; if we do not describe a specific challenge response algorithm then challenge response algorithms which are not one time password PoP may be implied while on the other hand, if we specify a specific algorithm there are plenty of them which are left outside. IDABC AAL3 requirements are very generic and do not specify something on this aspect.

In addition, current AAL3 specifications dictate that the token type should be either soft crypto token or one time password device token. This fact could be expressed by restricting `PrincipalAuthenticationMechanismType` to `Token` with `ActivationPin` or `Token` values respectively. Due to the fact that `PrincipalAuthenticationMechanismType` is a `sequence` element instead of a `choice`, this requirement suffers from lack of expressiveness. A restriction of `PrincipalAuthenticationMechanismType` element to choice might be proved adequate to express this specific requirement.

Finally, the `PhysicalVerification` lack of `Extension` element hinders the expression of such a rich as AAL3 identification environment. For example, the 'in person qualified ignature issuance' requirement is hard to express using the existent `PhysicalVerification` element structure (an extension is needed). Furthermore, the standard (SAML v2.0) does not provide further information with regards to the alternative values of this element (`primary`, `secondary`).

2.2.4.2 Proposed Extensions

Non expressible requirements are represented in the following table. Most of the proposed extensions are taking place at the `Identification` element of the proposed class.

Req. No	SAML AC Element – Extension Point	Proposed Elements
3a	Identification	<xs:complexType name="PhysicalPresenceType"> <xs:element ref="DocumentaryEvidenceChoice"/> <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/> </xs:complexType>
3b	Identification	<element name="InPersonQualifiedSignature" type="xs:boolean"/> <annotation> <documentation> This element indicates that identification has been performed on line using a qualified digital signature issued in person. The InPersonQualifiedSignature element MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation>
4a	Identification	<element name="GovernmentIssuedDoc" type=" GovernmentIssuedDocType"/> <xs:annotation> <xs:documentation> The GovernmentIssuedDoc Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> </element> <xs:complexType name="GovernmentIssuedDocType">

		<xs:sequence> <xs:element ref="IssuingOrganization" minOccurs="1"/> <xs:element ref="Photo" minOccurs="1"/> <xs:element ref="Signature" minOccurs="1"/> </xs:sequence> <xs:choice> <xs:element ref=”IdentityCardID”/> <xs:element ref=”PassportNo”/> <xs:element ref=”DrivingLicenseID”/> <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/> </xs:choice> </xs:complexType> <element name="IssuingOrganization" type="OrganizationType"/>
4b	Identification	<element name="ThirdPartyCorroboration" type="ThirdPartyCorroborationType"/> <xs:annotation> <xs:documentation> The ThirdPartyCorroboration Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> </element> <xs:complexType name=" ThirdPartyCorroborationType"> <xs:choice minOccurs="2" maxOccurs="unbounded"> <xs:sequence> <xs:element ref="OrganizationName"/> <xs:choice> <xs:element ref=”BicCode” minOccurs="1"/> <xs:element ref=”InsuranceAgencyRN” minOccurs="1"/> <xs:element ref=” GovernmentIssueID” minOccurs="1"/> </xs:choice> </xs:sequence> </xs:choice> </xs:complexType>
5	Identification	<xs:group name="DocumentaryEvidenceChoiceGroup"> <xs:annotation> <xs:documentation> The DocumentaryEvidence Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </element> <xs:choice> <xs:element ref=”GovernmentIssuedDoc”/> <xs:element ref=”ThirdPartyCorroboration”/> </xs:choice> </xs:group>
6	Identification	xs:group name="RegistrationChoiceGroup"> <xs:annotation> <xs:documentation> The RegistrationChoice Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </element> <xs:group name="RegistrationChoiceGroup"> <xs:choice> <xs:element ref="PhysicalPresence"/> <xs:element ref="QualifiedSignature"/> </xs:choice> </xs:group>

8	Identification	<xs:element name="RegistrationDataRetention"> <xs:annotation> <xs:documentation> This element indicates the length of time for which secondary registration data is stored. The RegistrationDataRetention element MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> <xs:attribute name=”retentionPeriod” type="xs:duration" use="required"/> </xs:element>
11, 12, 13, 14, 15, 16	AuthnMethod	<element name="AttacksAddressed" type="AttacksAddressedType"/> <xs:annotation> <xs:documentation> The AuthnMethod Extension MUST NOT occur any other place than in the Extension element of the AuthnMethod Element within the AuthnContextDeclarationBaseType element within an Authentication Context declaration. </xs:documentation> </element> <xs:simpleType name="AttacksAddressedType "> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="Eavesdropper" minOccurs=”0”/> <xs:enumeration value="Replay" minOccurs=”0”/> <xs:enumeration value="Online Guessing” minOccurs=”0”/> <xs:enumeration value="Verifier Impersonation” minOccurs=”0”/> <xs:enumeration value="Man-in-the-middle" minOccurs=”0”/> <xs:enumeration value="Session Hijacking" minOccurs=”0”/> </xs:restriction> </xs:simpleType>

Table 10: Proposed SAML v2.0 extensions for IDABC AAL3

There is a slight change in the normal numbering procedure when referring to ‘Documentary evidence’ and ‘physical presence’ requirements: the first one is related to the documents needed on behalf of the claimant to present to the authentication authority to prove his identity. The other one is related to the need of claimant’s physical presence when identifying himself to the authentication authority. Each one may further separated to two more specific requirements.

4.2.3 Suggested IDABC AAL3 Context Class

The IDABC AAL3 would then be expressed as a SAML Authentication Context Class using the above extensions as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelThree"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelThree"
finalDefault="extension"
blockDefault="substitution"
version="2.0">

<import namespace="urn:oasis:names:tc:SAML:2.0:metadata"
schemaLocation="saml-schema-metadata-2.0.xsd"/>

<redefine schemaLocation="sstc-saml-context-ext-IDABC-L3.xsd">

<xs:annotation>
      <xs:documentation>This redefine section sets conditions on the extensions
in sstc-saml-context-ext-IDABC-L3.xsd so that they comply with IDABC level 3.
      </xs:documentation>
</xs:annotation>
```

```
<xs:element name="IssuingOrganization" type="OrganizationType"/>
<xs:element name="Photo" type="xs:boolean"/>
<xs:element name="Signature" type="xs:boolean"/>
<xs:element name="IdentityCardID" type="xs:boolean"/>

<xs:complexType name=" GovernmentIssuedDocType ">
      <xs:sequence>
            <xs:element ref="IssuingOrganization" minOccurs="1"/>
            <xs:element ref="Photo" minOccurs="1"/>
            <xs:element ref="Signature" minOccurs="1"/>
      </xs:sequence>
      <xs:choice>
            <xs:element ref=”IdentityCardID”/>
            <xs:element ref=”PassportNo”/>
            <xs:element ref=”DrivingLicenseID”/>
      </xs:choice>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
</xs:complexType>

<xs:element name="GovernmentIssuedDoc" type="GovernmentIssuedDocType"/>

<xs:complexType name="ThirdPartyCorroborationType">
      <xs:choice minOccurs="2" maxOccurs="unbounded">
            <xs:sequence>
                  <xs:element ref="IssuingOrganization"/>
                  <xs:choice>
                        <xs:element ref=”BicCode” minOccurs="1"/>
                        <xs:element ref=”InsuranceAgencyRN” minOccurs="1"/>
                        <xs:element ref=”GovernmentIssueID” minOccurs="1"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:choice>
            </xs:sequence>
      </xs:choice>
</xs:complexType>”

<xs:group name="DocumentaryEvidenceChoiceGroup">
      <xs:choice>
            <xs:element ref=”GovernmentIssuedDoc”/>
            <xs:element ref=”ThirdPartyCorroboration”/>
      </xs:choice>
</xs:group>

<xs:element name="DocumentaryEvidenceChoice"
type="DocumentaryEvidenceChoiceGroup"/>

<xs:complexType name="PhysicalPresenceType">
      <xs:element ref="DocumentaryEvidenceChoice"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
</xs:complexType>

<element name="InPersonQualifiedSignature" type="xs:boolean"/>

<xs:element name="PhysicalPresence" type="PhysicalPresenceType"/>

<xs:group name="RegistrationChoiceGroup">
      <xs:choice>
            <xs:element ref="PhysicalPresence"/>
            <xs:element ref="InPersonQualifiedSignature"/>
      </xs:choice>
</xs:group>
```

```
<xs:complexType name="RegistrationDataRetentionPeriodType">
      <xs:attribute name=" retentionPeriod " type="xs:duration" use="required">
            <xs:restriction base="xsd:duration">
                  <xsd:minInclusive value="P07Y"/>
            </xs:restriction>
      </xs:attribute>
</xs:complexType>

<xs:simpleType name="AttacksAddressedType">
      <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="Eavesdropper" minOccurs=”1”/>
            <xs:enumeration value="Replay" minOccurs=”1”/>
            <xs:enumeration value="Online Guessing” minOccurs=”1”/>
            <xs:enumeration value="Verifier Impersonation” minOccurs=”1”/>
            <xs:enumeration value="Man-in-the-middle" minOccurs=”1”/>
            <xs:enumeration value="Session Hijacking" minOccurs=”1”/>
      </xs:restriction>
</xs:simpleType>

</redefine>

<redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
            <xs:annotation>
                  <xs:documentation> This section requires that extensions are
placed in the right section of the schema.
                  </xs:documentation>
</xs:annotation>
<xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnContextDeclarationBaseType">
                  <xs:sequence>
                        <xs:element ref="Identification" minOccurs="0"/>
                        <xs:element ref="TechnicalProtection" minOccurs="0"/>
                        <xs:element ref="OperationalProtection" minOccurs="0"/>
                        <xs:element ref="AuthnMethod"/>
                        <xs:element ref="GoverningAgreements" minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="ID" type="xs:ID" use="optional"/>
            </xs:restriction>
</xs:complexContent>
</xs:complexType>
      <xs:complexType name="AuthnMethodBaseType">
            <xs:complexContent>
                  <xs:restriction base="AuthnMethodBaseType">
                        <xs:sequence>
                              <xs:element ref="PrincipalAuthenticationMechanism"
minOccurs="0"/>
                              <xs:element ref="Authenticator"/>
                              <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
                              <xs:element ref="Extension" minOccurs="1"/>
                        </xs:sequence>
                  </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
            <xs:restriction base="TechnicalProtectionBaseType">
```

```
                  <xs:sequence>
                        <xs:choice>
                              <xs:element ref="SecretKeyProtection"/>
                        </xs:choice>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
            <xs:restriction base="PrincipalAuthenticationMechanismType">
                  <xs:sequence>
                        <xs:element ref="Token"/>
                        <xs:element ref="ActivationPin"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthenticatorBaseType">
                  <xs:sequence>
                        <xs:element ref="SharedSecretChallengeResponse"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="SharedSecretChallengeResponseType">
      <xs:complexContent>
            <xs:restriction base="SharedSecretChallengeResponseType">
                  <xs:attribute name="method" type="xs:anyURI"
                  fixed="urn:ietf:rfc:2945"/>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
            <xs:restriction base="SecretKeyProtectionType">
                  <xs:sequence>
                        <xs:element ref="KeyActivation"/>
                        <xs:element ref="KeyStorage"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyActivationType">
      <xs:complexContent>
            <xs:restriction base="KeyActivationType">
                  <xs:sequence>
                  <xs:element ref="ActivationPin"/>
                  </xs:sequence>
            </xs:restriction>
```

```
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyStorageType">
      <xs:complexContent>
            <xs:restriction base="KeyStorageType">
                  <xs:attribute name="medium" use="required">
                        <xs:simpleType>
                              <xs:restriction base="mediumType">
                                    <xs:enumeration value="token"/>
                                    <xs:enumeration value="memory"/>
                                    <xs:enumeration value="MobileDevice"/>
                              </xs:restriction>
                        </xs:simpleType>
                  </xs:attribute>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentificationType">
      <xs:complexContent>
            <xs:restriction base="IdentificationType">
                  <xs:sequence>
                        <xs:element ref="GoverningAgreements"/>
                        <xs:element ref="Extension" minOccurs="2"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

</xs:redefine>
</xs:schema>
```

Notes

Note that, despite the fact that seven proposed extensions have already been described at the relevant table (see), the `<Extension>` sub element minimum value of `<IdentificationType>` element has been set to '2'. This is due to the fact that `DocumentaryEvidenceChoiceGroup`, `PhysicalPresenceType`, `InPersonQualifiedSignature`, `GovernmentIssuedDoc` and `ThirdPartyCorroboration` elements are sub elements of `RegistrationChoiceGroup` element. This last one along with the RegistrationDataRetention element comprises the set of the proposed extensions. Finally, due tothe element lack of expressiveness in the the Physicalverification element, we decided to restrict the `Identification` element only to `GoverningAgreements` and `Extension and to put the extra expressiveness in these elements`.

2.5 IDABC Authentication Level 4 (High Assurance)

5.2.1 Requirements description-analysis

Level 4 registration is appropriate for application transactions in which damages that might arise from misappropriation of real world identity would have a Very high impact. Level 4 identity proofing is distinct in that it directly or indirectly requires in-person identity proofing of official identity documents.

REGISTRATION PHASE	**REQUIREMENT**	**EXPRESSIBLE/NOT EXPRSESSIBLE IN SAML V2.0 EXISTING CONTEXT**

Procedure for identity proofing, user details registration, delivery of token and credentials	The token/credential must be issued by a body. **(1)**	expressible
	which is subject to a specific government agreement or under government supervision. **(2)**	expressible
	The RA shall ensure that the subscriber's identity information is verified and checked in accordance with the stated registration policy. **(3)**	expressible
	Personal appearance is required. **(4a)**	Not expressible
	During registration, the claimant must present an official identity document such as an identity card, passport or drivers license which contains a photo and signature, and which is verified by the RA before a token/credential can be issued; **(4b)**	Not expressible
	Or alternatively (5)	Not expressible
	No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and which are signed using a qualified signature, which the RA validates. **(4c)** Note that Level 4 security requires that the token/credential must be delivered to the claimant in person, so that it is impossible to obtain Level 4 authentication methods without personal identification.	Not expressible
	The token/credential may only be given to the claimant in person after validation of his identity using an official identity document. **(7)**	expressible
Retention period for registration data	A record of the facts of registration shall be maintained by the CSP or its representative. The suggested minimum retention period for	Not expressible

	registration data for Level 4 credentials is 10 years beyond the expiration or revocation (whichever is later) of the credential. **(8)**	
ELECTRONIC AUTHENTICATION PHASE		
Authentication Protocol for Proof of Possession (PoP)	Symmetric Key PoP **(9)**	expressible
	Private Key PoP **(10)**	expressible
Token Type	Only Hard crypto tokens can be accepted at Level 4. **(11)**	expressible
Requires the application owner to implement protection against	Eavesdropper **(12)**	Not expressible
	Replay **(13)**	Not expressible
	On-line guessing **(14)**	Not expressible
	Verifier Impersonation **(15)**	Not expressible
	Man-in-the-middle **(16)**	Not expressible
	Session Hijacking **(17)**	Not expressible

Table 11: IDABC AAL 4 requirements description

As with the AAL 3 requirements description, the requirements are indexed according to alternative possibilities (4a, 4b) etc… In the AAL 4 case, this is in order to distinguish between the need for the claimant's physical verification by the IdP or not.

5.2.2 Gaps

2.2.5.1 Existing Authentication Context

To address the Symmetric or Private key PoP property we have included all possible and available by SAML v2.0 AC values.

Req. No	SAML v2.0 AC Element
1	OrganizationType
2	Identification->Governing Agreements
3	Identification->GoverningAgreements
7	Identification->GoverningAgreements
9,10	AuthnMethod->Authenticator-> {DigSig, ZeroKnowledge, SharedSecretChallengeResponse, SharedSecretDynamicPlaintext, AsymmetricDecryption, AsymmetricKeyAgreement}
11	AuthnMethod->PrincipalAuthenticationMechanism-> {Smartcard, ActivationPin}

Table 12: Mapping IDABC AAL4 requirements to existing within SAML v2.0 AC class elements

Hard crypto token possession and a control requirement may be expressed by restricting `PrincipalAuthenticationMechanism` to a smartcard (possession) with a PIN (control) values. According to IDABC Hard crypto token specifications, they shall not be able to export authentication keys. There is no element in SAML v2.0 to address this requirement.

2.2.5.2 Proposed Extensions

Non expressible requirements are represented in the following table. Most of the proposed extensions are to the `Identification` element of the proposed class.

Req. No	SAML AC Element – Extension Point	Proposed Elements
4a	Identification	<xs:complexType name="PhysicalPresenceType"> <xs:element ref="GovernmentIssuedDoc"/> <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/> </xs:complexType>

4b	Identification	<element name="GovernmentIssuedDoc" type=" GovernmentIssuedDocType"/> <xs:annotation> <xs:documentation> The GovernmentIssuedDoc Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> </element> <xs:complexType name="GovernmentIssuedDocType"> <xs:sequence> <xs:element ref="IssuingOrganization" minOccurs="1"/> <xs:element ref="Photo" minOccurs="1"/> <xs:element ref="Signature" minOccurs="1"/> </xs:sequence> <xs:choice> <xs:element ref=”IdentityCardID”/> <xs:element ref=”PassportNo”/> <xs:element ref=”DrivingLicenseID”/> </xs:choice> </xs:complexType> <element name="IssuingOrganization" type="OrganizationType"/>
4c	Identification	<element name="InPersonQualifiedSignature" type="xs:boolean"/> <annotation> <documentation> This element indicates that identification has been performed on line using a qualified digital signature issued in person. The InPersonQualifiedSignature element MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation>
5	Identification	xs:group name="RegistrationChoiceGroup"> <xs:annotation> <xs:documentation> The RegistrationChoice Extension MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </element> <xs:group name="RegistrationChoiceGroup"> <xs:choice> <xs:element ref="PhysicalPresence"/> <xs:element ref="QualifiedSignature"/> </xs:choice> </xs:group>
8	Identification	<xs:element name="RegistrationDataRetention"> <xs:annotation> <xs:documentation> This element indicates the length of time for which secondary registration data is stored. The RegistrationDataRetention element MUST NOT occur any other place than in the Extension element of the Identification Element within an Authentication Context declaration. </xs:documentation> </xs:annotation> <xs:attribute name=”retentionPeriod” type="xs:duration" use="required"/> </xs:element>
12, 13, 14, 15, 16,17	AuthnMethod	<element name="AttacksAddressed" type="AttacksAddressedType"/> <xs:annotation> <xs:documentation> The AttacksAddressed Extension MUST NOT occur any other place than in the Extension element of the AuthnMethod Element within the AuthnContextDeclarationBaseType element within an Authentication Context declaration.

		</xs:documentation> </element> <xs:simpleType name="AttacksAddressedType "> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="Eavesdropper" minOccurs="0"/> <xs:enumeration value="Replay" minOccurs="0"/> <xs:enumeration value="Online Guessing" minOccurs="0"/> <xs:enumeration value="Verifier Impersonation" minOccurs="0"/> <xs:enumeration value="Man-in-the-middle" minOccurs="0"/> <xs:enumeration value="Session Hijacking" minOccurs="0"/> </xs:restriction> </xs:simpleType>

Table 13: Proposed SAML v2.0 extensions for IDABC AAL4

5.2.3 Suggested IDABC AAL4 Context Class

The IDABC Level 4 would then be expressed as a SAML Authentication Context Class using the above extensions as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelFour"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:IDABCLevelFour"
finalDefault="extension"
blockDefault="substitution"
version="2.0">

<import namespace="urn:oasis:names:tc:SAML:2.0:metadata" schemaLocation="saml-
schema-metadata-2.0.xsd"/>

<redefine schemaLocation="sstc-saml-context-ext-IDABC-L4.xsd">

<xs:annotation>
      <xs:documentation>This redefine section sets conditions on the extensions
in sstc-saml-context-ext-IDABC-L4.xsd so that they comply with IDABC level 4.
      </xs:documentation>
</xs:annotation>

<xs:element name="IssuingOrganization" type="OrganizationType"/>
<xs:element name="Photo" type="xs:boolean"/>
<xs:element name="Signature" type="xs:boolean"/>
<xs:element name="IdentityCardID" type="xs:boolean"/>

<xs:complexType name="GovernmentIssuedDocType">
      <xs:sequence>
            <xs:element ref="IssuingOrganization" minOccurs="1"/>
            <xs:element ref="Photo" minOccurs="1"/>
            <xs:element ref="Signature" minOccurs="1"/>
      </xs:sequence>
      <xs:choice>
            <xs:element ref="IdentityCardID"/>
            <xs:element ref="PassportNo"/>
            <xs:element ref="DrivingLicenseID"/>
      </xs:choice>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
</xs:complexType>

<xs:element name="GovernmentIssuedDoc" type="GovernmentIssuedDocType"/>

<xs:complexType name="PhysicalPresenceType">
```

```
      <xs:element ref="GovernmentIssuedDoc"/>
      <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
</xs:complexType>

<element name="InPersonQualifiedSignature" type="xs:boolean"/>

<xs:element name="PhysicalPresence" type="PhysicalPresenceType"/>

<xs:group name="RegistrationChoiceGroup">
      <xs:choice>
            <xs:element ref="PhysicalPresence"/>
            <xs:element ref="InPersonQualifiedSignature"/>
      </xs:choice>
</xs:group>

<xs:complexType name="RegistrationDataRetentionPeriodType">
      <xs:attribute name=" retentionPeriod " type="xs:duration" use="required">
            <xs:restriction base="xsd:duration">
                  <xsd:minInclusive value="P10Y"/>
            </xs:restriction>
      </xs:attribute>
</xs:complexType>

<xs:simpleType name="AttacksAddressedType">
      <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="Eavesdropper" minOccurs=”1”/>
            <xs:enumeration value="Replay" minOccurs=”1”/>
            <xs:enumeration value="Online Guessing” minOccurs=”1”/>
            <xs:enumeration value="Verifier Impersonation” minOccurs=”1”/>
            <xs:enumeration value="Man-in-the-middle" minOccurs=”1”/>
            <xs:enumeration value="Session Hijacking" minOccurs=”1”/>
      </xs:restriction>
</xs:simpleType>

</redefine>

<redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

<xs:annotation>
      <xs:documentation> This section requires that extensions are placed in the
      right section of the schema.
      </xs:documentation>
</xs:annotation>

<xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnContextDeclarationBaseType">
                  <xs:sequence>
                        <xs:element ref="Identification" minOccurs="0"/>
                        <xs:element ref="TechnicalProtection" minOccurs="0"/>
                        <xs:element ref="OperationalProtection" minOccurs="0"/>
                        <xs:element ref="AuthnMethod"/>
                        <xs:element ref="GoverningAgreements" minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
                  <xs:attribute name="ID" type="xs:ID" use="optional"/>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>
```

```
<xs:complexType name="AuthnMethodBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthnMethodBaseType">
                  <xs:sequence>
                        <xs:element ref="PrincipalAuthenticationMechanism"
                  minOccurs="0"/>
                        <xs:element ref="Authenticator"/>
                  <xs:element ref="AuthenticatorTransportProtocol"
            minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="1"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="TechnicalProtectionBaseType">
      <xs:complexContent>
            <xs:restriction base="TechnicalProtectionBaseType">
                  <xs:sequence>
                        <xs:choice>
                              <xs:element ref="PrivateKeyProtection"/>
                              <xs:element ref="SecretKeyProtection"/>
                        </xs:choice>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="PrincipalAuthenticationMechanismType">
      <xs:complexContent>
            <xs:restriction base="PrincipalAuthenticationMechanismType">
                  <xs:sequence>
                        <xs:element ref="Smartcard"/>
                        <xs:element ref="ActivationPin"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="AuthenticatorBaseType">
      <xs:complexContent>
            <xs:restriction base="AuthenticatorBaseType">
                  <xs:sequence>
                        <xs:choice>
                              <xs:element ref="DigSig"/>
                              <xs:element ref="ZeroKnowledge"/>
                              <xs:element ref="SharedSecretChallengeResponse"/>
                              <xs:element ref="SharedSecretDynamicPlaintext"/>
                              <xs:element ref="AsymmetricDecryption"/>
                              <xs:element ref="AsymmetricKeyAgreement"/>
                        </xs:choice>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>
```

```
<xs:complexType name="PrivateKeyProtectionType">
      <xs:complexContent>
            <xs:restriction base="PrivateKeyProtectionType">
                  <xs:sequence>
                        <xs:element ref="KeyActivation"/>
                        <xs:element ref="KeyStorage"/>
                        <xs:element ref="Extension" minOccurs="0"
                  maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="SecretKeyProtectionType">
      <xs:complexContent>
            <xs:restriction base="SecretKeyProtectionType">
                  <xs:sequence>
                        <xs:element ref="KeyActivation"/>
                              <xs:element ref="KeyStorage"/>
                              <xs:element ref="Extension" minOccurs="0"
                        maxOccurs="unbounded"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyActivationType">
      <xs:complexContent>
            <xs:restriction base="KeyActivationType">
                  <xs:sequence>
                        <xs:element ref="ActivationPin"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="KeyStorageType">
      <xs:complexContent>
            <xs:restriction base="KeyStorageType">
                  <xs:attribute name="medium" use="required">
                  <xs:simpleType>
                        <xs:restriction base="mediumType">
                              <xs:enumeration value="MobileAuthCard"/>
                              <xs:enumeration value="smartcard"/>
                              <xs:enumeration value="token"/>
                        </xs:restriction>
                  </xs:simpleType>
                  </xs:attribute>
            </xs:restriction>
      </xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentificationType">
      <xs:complexContent>
            <xs:restriction base="IdentificationType">
                  <xs:sequence>
                        <xs:element ref="GoverningAgreements"/>
                        <xs:element ref="Extension" minOccurs="2"/>
                  </xs:sequence>
            </xs:restriction>
      </xs:complexContent>
```

```
</xs:complexType>

</xs:redefine>
</xs:schema>
```

Notes

Similarly with AAL 3, the gaps addressed with regard to `Physicalverification` element is also true for the present AAL. Due to lack of expressiveness of this particular element, we decided to restrict the Identification element only to GoverningAgreements and Extension.

3 Conclusions and recommendations

This report represents ENISA's work on expressing IDABC multilevel authentication policy in a machine readable format using the OASIS SAML v2.0 standard. The main goal of this report is to provide stakeholders with documented technical information in terms not only in terms of gap analysis but also of guidance for the implementation of IDABC AALs in real-world eGovernment applications. To accomplish this, the LoA concept is expressed as a definition of a series of authentication context classes and alternative semantics for the representation SAML-based mechanisms has also been reported (see § **Error! Reference source not found.**). Each class defines a proper subset of the full set of authentication contexts. Schema elements have been chosen as representative of the practices and technologies proposed by IDABC AALs, and provide asserting and relying parties convenient shorthand when referring to IDABC authentication context issues. The most important conclusions of this report may be summarised in the following points:

- A standardized model and semantics of authentication mechanisms is vital to achieve interoperability of authentication level descriptions. This model may either be human readable or machine readable. SAML Authentication Context is a primary candidate for standardizing a model and semantics of authentication mechanisms in machine-readable form. This report makes the following conclusions about the use of SAML AC as a basis for standardizing a model and semantics of authentication mechanisms:
    1. SAML AC provides inadequate documentation on the meaning of its elements. The <documentation> element of the AC XML schema is the only explanation provided of the meaning of its elements and this is often missing or inadequate.
    2. Although nowadays SAML v2.0 is widely used in the federation field, SAML AC would need revising in order to provide a complete, accurate and usable model. The specific elements in need of revision are described in [Mapping AAL requirements to SAML v2.0 Authentication Context].
    3. If a machine-readable version is to be provided, it should be expressed in a form which facilitates machine reasoning and semantic extensibility such as OWL [[29]].
    4. Given the fact that processing on-the-fly revisions to authentication context descriptions is widely seen to be unfeasible from a performance and combinatoric point of view, we suggest that a machine-readable model of authentication mechanism is in fact inappropriate. Machine processing will in practice be limited to the matching agreed URI's pointing to human readable policies. This suggests therefore that a machine-readable format for AC is not appropriate.
    5. If it is decided that such a model is better expressed in human-readable format then it makes little sense to continue using the complex syntax of SAML AC as a container for such metadata. Instead it would make more sense to standardize the model and semantics within a group such as the OASIS eGovernment TC. The 'Natural language format' has important advantages among different authentication context information representations (using the SAML federation framework) when it comes to expressing

[29] http://www.w3.org/2004/OWL/#specs

IDABC multilevel authentication policy. This is due to the fact that this alternative may be easily implemented by vendors while at the same time maintaining an adequate (unlimited) level of authentication context information expressiveness for the users. Authentication Policy mapping is only one part of an authentication framework standardization procedure. eGovernment authentication schemes have been designed with a limited scope in mind i.e. within the limits of a federation, a country etc. Interoperability problems may arise when organizations with different underlying authentication schemes trying to communicate. That is why, actions striving for global convergence should be taken up and apart from vendors, organizations like ENISA and OASIS eGovernment Member Section may have a role to play towards this direction.

- IDABC authentication requirements proved in a few cases cases to be vague and contradictory when trying to translate them using a formal description language like XML. The simultaneous presence of soft crypto token and one time password device (hard crypto token) at AAL 3 as a token type requirement is such an example. This suggests that a standardized