Mapping IDABC Authentication Assurance Levels to SAML V2.0

Konstantinos MOULINOS,
Seconded National Expert

Open Standards Forum 2008: Security challenges for the Information Society

Scope of the presentation

To…

- Explore the IDABC AALs to SAML v2.0 mapping options
- Provide with pros and cons of each option
- Provide stakeholders with input when deciding on e-Government apps.

Not to…

- Compare competitive federation technologies
- Review IDABC Authentication policy
- Analyse different AAL approaches

An introduction to IDABC

- Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens
- Authentication Policy->Authentication Assurance Level.
  - based on a survey of all European government initiatives
  - provides a model which can be mapped to all existing European policies
- Each e-Government application should be mapped to a specific AAL
- 4 AALs have been defined.

Authentication Assurance Level: definition

- the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and
- the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

IDABC AAL elements

- **Registration Phase**
  - Identity proofing,
  - User registration, Token delivery
  - Retention period
- **Electronic Authentication Phase**
  - Authentication PoP
  - Token Type
  - Protection against (Application owner)

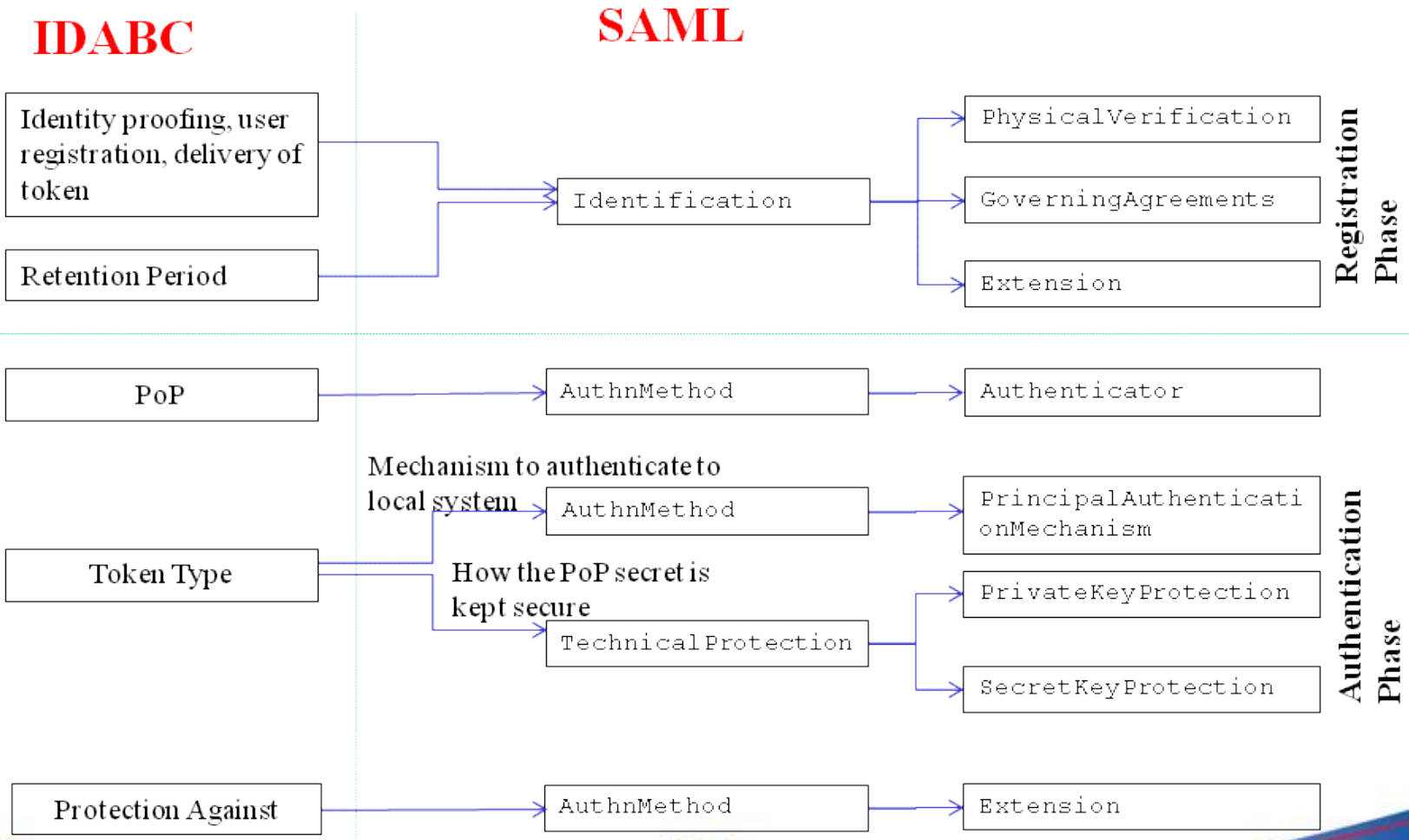
Expressing AAL with SAML

1. Mapping to existing SAML v2.0 Authentication Context (AC) classes
2. Extensions to SAML v2.0 schema
3. Extra mandatory attribute
4. Reference to external documentation

SAML AC Data Model

- Identification
- Technical Protection
- Authentication Method
- Operational Protection
- Governing Agreements

Conceptual mapping IDABC requirements to SAML v2.0 elements



1. Mapping AALs to existing ACs

IDABC AAL	Authentication Context
4	SmartCardPKI
3	SoftwarePKI, SecureRemotePassword
2	PasswordProtectedTransport, SecureRemotePassword
1	Password

- ★ **Pros**
  - ★ **Easy access control decisions**
  - ★ **Easy implementation**
- ★ **Cons**
  - ★ **Lack of expressiveness**

2a. Extensions to SAML v2.0 schema

- ENISA's focal point
- Straightforward steps
  - Disassemble IDABC AAL requirements
  - Map requirements to SAML v2.0 schema
  - Identify gaps

2b. Disassembling Requirements

ELECTRONIC AUTHENTICATION PHASE (AAL2)		
Authentication Protocol for Proof of Possession (PoP)	Most of the time Tunneled	expressible
	or One-time Password PoP.	AAL3
	However, according to risk assessment, could also be: - Symmetric Key PoP - Private Key PoP	AAL4
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.	expressible
Requires the application owner to implement protection against	Eavesdropper Replay On-line guessing	Not expressible

2c. Mapping requirements to SAML v2.0 schema

An 'expressible' example

Tunneled PoP

```
<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>
```

A 'not expressible' example

AttacksAddressed

```
<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>
```

2d. Identifying gaps

- **Non-cryptographic challenge reply protocols have not been identified in the SAML v2.0 AC**
- **IDABC hardware token: no details are provided (e.g. seed length, portability)**
- `RestrictedPassword` **and** `ZeroKnowledge` **elements do not accurately express the One time PoP property**
- **Lack of** `Extension` **at** `PhysicalVerification` **element**
- **and more…**

2e. Extensions to SAML v2.0 schema

- Pros
  - Straightforward
  - Expressiveness
- Cons
  - Gaps between IDABC requirements and SAML semantics

3. Extra attribute

```
<saml:Attribute

NameFormat="urn:oasis:names:tc:SAML:2.0:att
    rname-format:basic"

Name="europa:eu:saml:attribute:AssuranceLev
    el"

<saml:AttributeValue xsi:type="xs:string”>2
</saml:AttributeValue>

</saml:Attribute>
```

- ★ **Pros**
  - ★ Easy access control decisions
  - ★ Easy implementation
- ★ **Cons**
  - ★ Extra mandatory attribute

4. Reference to external documentation

- **URI**

http://ec.europa.eu/idabc/loa/idabc-loa1.pdf

- **'Natural language format'**

- **Pros**
  - Easy implementation
  - Highest level of expressiveness
- **Cons**
  - Every system configured with the URIs

Conclusions

- Revision of SAML AC documentation element
- Gaps between SAML v2.0 specs and IDABC requirements have been identified
- Machine vs human readable format
- External documentation reference gains momentum
  - Structure of such a document?
  - Global convergence and the role of OASIS eGovernment Member Section and ENISA
- IDABC generic requirements specification

Contact

Konstantinos MOULINOS

Seconded National Expert in Security Policies

Mail: Konstantinos.Moulinos@enisa.europa.eu

Tel: +30 2810 391363

Fax: +30 2810 391895