ISA Action 1.17: A Reusable INSPIRE Reference Platform

(ARE3NA)

Authentication, Authorization & Accounting for Data and Services in EU Public Administrations

D1.1.2 & D1.2.2– Analysing standards and technologies for AAA

Ann Crabbé

Danny Vandenbroucke

Andreas Matheus

Dirk Frigne

Frank Maes

Reijer Copier

This publication is a Deliverable of Action 1.17 of the Interoperability Solutions for European Public Administrations (ISA) Programme of the European Union, A Reusable INSPIRE Reference Platform (ARE3NA), managed by the Joint Research Centre, the European Commission's in-house science service.

Disclaimer

Copyright notice

Bibliographic Information:

Ann Crabbé, Danny Vandenbroucke, Andreas Matheus, Dirk Frigne, Frank Maes and Reijer Copier Authentication, Authorization and Accounting for Data and Services in EU Public Administrations: D1.1.2 & D1.2.2 – Analysing standards and technologies for AAA. European Commission; 2014. JRC92555

Contents

1 TABLE OF FIGURES

2 GLOSSARY

AAA	Authentication, Authorization and Accounting
ARE3NA	A Reusable INSPIRE Reference Platform
AMF	Access Management Federation
BKG	Bundesamt für Kartographie und Geodäsie
CC	Coordination Centre
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
DRM	Digital Rights Management
DSS	Digital Signature Software
ECAS	European Citizen Action Service
EIA	European Interoperability Architecture
EIF	European Interoperability Framework
EIS	European Interoperability Strategy
EULF	European Location Framework
GIS	Geographic Information System
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IdP	Identity Provider
ICT	Information and Communication Technologies
INSPIRE	Infrastructure for Spatial Information in the European Community
ISA	Interoperability Solutions for European Public Administrations
JRC	Joint Research Centre
LDAP	Lightweight Directory Access Protocol
OASIS	Advancing Open Standards for the Information Society
OGC	Open Geospatial Consortium
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PHP	Hypertext Preprocessor

PKI	Public-Key Infrastructure
QAA	Quality of Authentication Assurance (Model)
SAML	Security Assertion Markup Language
SDI	Spatial Data Infrastructure
SOA	Service Oriented Architecture
SP	Service Provider
SSL	Secure Sockets Layer
SSO	Single-Sign-On
STORK	Secure idenTity acrOss boRders linked
TLS	Transport Layer Security
W3C	World Wide Web Consortium
WAYF	Where Are You From
WS	Web Service
XACML	eXtensible Access Control Markup Language
XCBF	XML Common Biometric Format
XML	Extensible Markup Language

1. INTRODUCTION

This report is one of the deliverables of the project *"Authentication, Authorization and Accounting for Data and Services in EU Public Administrations"* launched by the Joint Research Centre of the European Commission (Contract n°389834). The project is part of ARE3NA, one of the actions of the ISA Programme (Action 1.17), aiming to create a Re-usable INSPIRE reference platform. The general objective of the project is to assist the Joint Research Centre (JRC) of the European Commission in preparing a study, workshop and testbed on standards, technologies and best practices for the Authentication, Authorization and Accounting (AAA) of data and services to support secure data exchange by public administrations in Europe. The particular objectives for the project can be summarized as follows:

- To identify and assess the current standards and technologies that would help to guarantee secure data exchange between public administrations, with particular focus on INSPIRE data and services, as well as those relevant in the context of the ISA programme and the Digital Agenda for Europe.
- To identify and assess best practices in Europe with regard to the application of those standards and technologies for data and service sharing in order to better understand what works well, what not and what elements are missing or could be improved.
- To design, develop and deploy a AAA-testbed using open source technology, based on existing INSPIRE and SDI components in three Member States taking into account the organisational, legal and technical settings.
- To involve actively Member State representatives on the proposed AAA-architecture and testbed and to collect feedback from them.

This report "D1.1.1 & D1.2.1 – Analysing standards and technologies for AAA" covers objective 1 of the project and is one of the key deliverable of the project. As defined in the Terms of Reference, the report examines the state of play of standards and technologies to support secure data exchange between public administrations. It is based on assessment of documents and online resources describing AAA implementations and the standards & technologies they are built on, on input from experts (also through interviews) active in the field of AAA, on input from discussions during the a workshop on AAA solutions for INSPIRE held in March 2014 (organised by ARE3NA) and a similar workshop organised in Brussels in April 2014 (organised by GEANTS) focusing on the research and academic sector.

Chapter 2 describes briefly why secure access to spatial data and services is relevant in the context of INSPIRE. Chapter 3 explains the three A's of an AAA architecture with the focus in the context of the study being authentication and authorization. The existing standards and technologies are analysed and their use is explained. Chapter 4 describes a concrete case in order to better understand how the key standards make secure access possible. The fifth chapter provides more information how a secure access mechanism for INSPIRE resources could become part of similar activities under the ISA programme, e.g. STORK. In annex 1 a comprehensive overview and explanation of all the standards is given.

2. INSPIRE AND SECURE ACCESS MECHANISMS

The INSPIRE Directive entered into force on 15 May 2007. Since then, Member States have transposed the Directive into national legislation and started the implementation of its components (coordinating structure, metadata, harmonization of data, services, monitoring & reporting). This is done based on a series of implementing rules (legally binding) and technical guidelines. All public authorities are involved and in practice **thousands of organisations are providing access to thousands of spatial datasets and their metadata** through a Service Oriented based Architecture (SOA) including discovery, viewing, download, transformation and spatial data services.

2.1 Limiting public access

Although INSPIRE aims to maximize sharing of spatial data and services between public administrations and provide public access to these data and services, this **can be limited under certain conditions** which are described in the Directive. Access to discovery services can only be limited when *"such access would adversely affect international relations, public security or national defence" (Directive 2007/2/EC Art.13)*. Access to the other type of network ser-

vices and the corresponding spatial data can, in addition to the already mentioned reasons for discovery services, be limited for various other reasons, *e.g.* to protect personal data, for IPR reasons, or to protect rare species/habitats. However such limitations *"shall be interpreted in a restrictive way"* and *"the public interest served by disclosure shall be weighed against the interest served by limiting or conditioning the access" (Directive 2007/2/EC Art.13)*.

Table 1: Conditions under which public access to data and services can be limited (Directive 2007/2/EC Art.13)

Article 13[1]

1. By way of derogation from Article 11(1), Member States may limit public access to spatial data sets and services through the services referred to in point (a) of Article 11(1) where such access would adversely affect international relations, public security or national defence.

By way of derogation from Article 11(1), Member States may limit public access to spatial data sets and services through the services referred to in points (b) to (e) of Article 11(1), or to the e-commerce services referred to in Article 14(3), where such access would adversely affect any of the following:

(a) the confidentiality of the proceedings of public authorities, where such confidentiality is provided for by law;

(b) international relations, public security or national defence;

(c) the course of justice, the ability of any person to receive a fair trial or the ability of a public authority to conduct an enquiry of a criminal or disciplinary nature;

(d) the confidentiality of commercial or industrial information, where such confidentiality is provided for by national or Community law to protect a legitimate economic interest, including the public interest in maintaining statistical confidentiality and tax secrecy;

(e) intellectual property rights;

(f) the confidentiality of personal data and/or files relating to a natural person where that person has not consented to the disclosure of the information to the public, where such confidentiality is provided for by national or Community law;

(g) the interests or protection of any person who supplied the information requested on a voluntary basis without being under, or capable of being put under, a legal obligation to do so, unless that person has consented to the release of the information concerned;

(h) the protection of the environment to which such information relates, such as the location of rare species.

2. The grounds for limiting access, as provided for in paragraph 1, shall be interpreted in a restrictive way, taking into account for the particular case the public interest served by providing this access. In every particular case, the public interest served by disclosure shall be weighed against the interest served by limiting or conditioning the access. Member States may not, by virtue of points (a), (d), (f), (g) and (h) of paragraph 1, limit access to information on emissions into the environment.

3. Within this framework, and for the purposes of the application of point (f) of paragraph 1, Member States shall ensure that the requirements of Directive 95/46/EC[2] *are complied with.*

In order to implement such limitations, or to enforce certain conditions of access and use (e.g. payment for downloading certain spatial data sets), **Member States need to set-up access mechanisms** according to one or another AAA-

[1] Article 17.7 provides similar derogations regarding sharing between public authorities: "By way of derogation from this Article, Member States may limit sharing when this would compromise the course of justice, public security, national defence or international relations" (Directive 2007/2/EC Art.17.1).

[2] Also known as the Data Privacy Act

architecture using specific standards, tools and technologies. These mechanisms could become part of the broader geoRM layer which can be considered a part of the INSPIRE architecture (see figure 1). However, **there are no specific implementing rules, nor guidelines on how this can be done.** This report aims to describe the existing standards and technologies. It complements the report describing European best practices in this context (D1.3) and wants to test certain open standards and technologies with the objective to help public authorities in Member States to implement similar solutions. This will contribute to the interoperability of INSPIRE and e-Government initiatives at large. It will also stimulate the use of INSPIRE services in cross-border and cross-sector e-Government processes.

The INSPIRE approach fits well with the broader objectives of the Digital Agenda for Europe, the ICT-related flagship in the context of Europe 2020, aiming to support smart, sustainable and inclusive growth based on knowledge and innovation. The ISA programme is the major programme to realize this. ISA aims to **stimulate the development of innovative e-Government services to support the thousands of interactions that occur between public administrations, businesses and citizens** in the context of governmental business processes (policy preparation and evaluation, administrative processes, front office services to citizens and businesses). Many of those interactions require, or could potentially benefit from, the integration of location information and location based e-services. They might span multiple sectors and operate across borders, similarly to the use of spatial data to support environmental policies and policies that might have an impact on the environment. As it is the case for INSPIRE, the **ISA programme aims to improve the legal, organizational, semantic and technical interoperability at the European level**. Therefore it developed a European Interoperability Strategy (EIS) and Framework (EIF), and prepared a European Interoperability Architecture (EIA). Access to and exchange of protected data is an integral part of these efforts. In more general terms, INSPIRE developments build further on generic ICT standards and technologies. This is not different for AAA implementations.

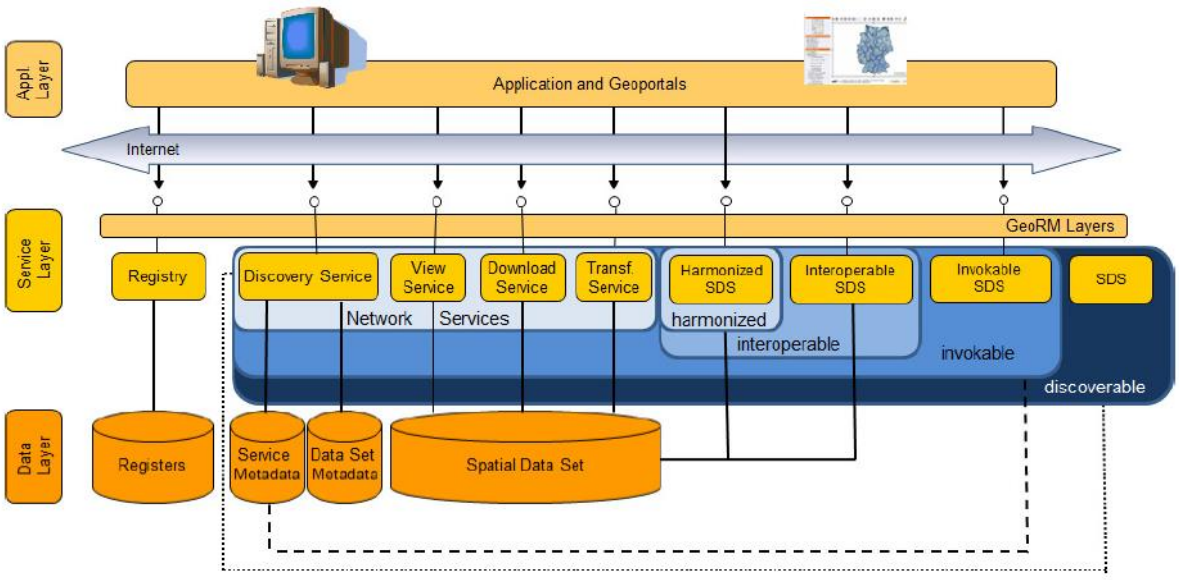

Figure 1: The Three-Tier INSPIRE Architecture

2.2 AAA in the ISA Programme

The ISA programme consists of more than 40 actions to facilitate cross-border electronic collaboration. Under the ISA programme, two particular actions aim to contribute to the improvement of European interoperability by promoting

the sharing and re-use of technical solutions based on spatial data and services. The European Location Framework (EULF) aims to provide guidance (e.g. by promoting Best Practices, guidelines, …) for generating innovative location based e-services through the better integration of location information in e-Government, improved alignment of policies and strategies, and the use of open standards. The second initiative is A Reusable INSPIRE Reference Platform (ARE3NA) which aims to support Member States by sharing and re-using common open source components (e.g. through pilot projects) for the implementation and exploitation of INSPIRE's spatial data sets and services. One of the activities of ARE3NA is to detect missing components that could help to foster this goal. Currently there are no technical provisions for implementing an AAA layer for INSPIRE. The AAA study, of which this report is part, aims to fill this gap. Several other actions are relevant to AAA implementations. ISA action 1.4 – "EU-wide interoperability of electronic identities (ECAS-STORK integration) focusses on authentication, as well as ISA action 1.5 – "An interoperable solution for electronic identities (eIDs)", while action 1.18 – "Federated Authorisation Across European Public Administrations (common services)" focusses on authorization. This report describes the activities and relevant experience in the last chapter of this report.

3. AAA: AUTHENTICATION, AUTHORIZATION AND ACCOUNTING

The large number of data providers and resources affected by the INSPIRE Directive can be controlled and managed using the AAA concept. To help frame this concept and distinguish the different terms, the following definitions, taken from the OGC Geospatial Digital Rights Management Reference Model [1], are used:

- **Access control** – a combination of authentication and authorisation.
- **Authentication** – verification that a potential partner in a conversation represents a person or organisation.
- **Authorisation** – determination whether a subject is allowed to have the specified type of access to a particular resource. Usually, authorisation is applied in the context of authentication. Once a subject is authenticated, it may be authorised to perform different types of access.
- **Accounting or rights management** – tracking and controlling the use of content, rights, licences and associated information.

Access control and rights management are inter-related in many ways, but should be considered separately when a technical solution is concerned. **The focus on this work is on the first two A's, authentication and authorization**, rather than accounting. Any attempt to further control of access and use of content, such as when data sets are downloaded, stored and used on local machines and/or mobile devices falls under Digital Rights Management (DRM) mechanisms, where the focus is on usage control. We are not to dealing with DRM in this work.

3.1 Access Management Federation [2] [3]

For establishing access control across public authorities in Europe participating in INSPIRE, this work proposes **federated authentication and local authorization**, also referred to as an Access Management Federation (AMF).

An access management federation is a network of organizations that trust each other for the means of sharing protected resources among each other. Worldwide, many academic AMFs are available for the purpose of sharing information and services between academic institutions such as Universities and Research Organizations. In academia, some of the well-known AMFs are UK Access Management Federation (United Kingdom) [4], In Common (USA) [5], Belnet of which KU Leuven is a member (Belgium) [6], and DFN-AAI (Germany) [7].

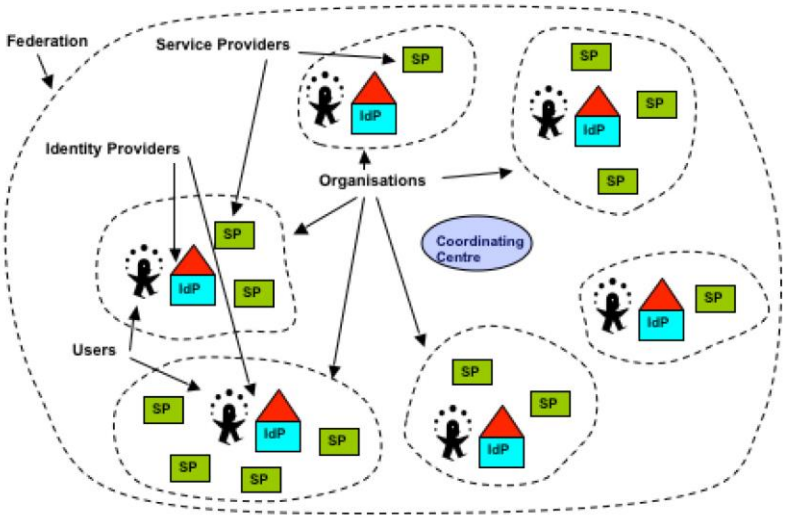

Figure 2: Access Management Federation [2]

All these federations are using the same setup, as illustrated in figure 2:

- **Service Providers** (SP) host protected resources that can be used by authenticated and authorized users of the federation.
- **Identity Providers** (IdP) provide the login and the authentication of organizational user accounts.
- A **Coordination Centre** (CC) controls the technical compliance with policies and procedures of the federation and thereby establishes the trust between members of the federation.

Member organisations participating in a federation operate identity providers for their users and any number of service providers to expose their protected resources[3]. An organization can join the federation by applying to the coordination centre as a service provider, an identity provider or both. For the legal act of accepting the organization – i.e. it becomes a trusted party – the CC checks technical compliance according to the policies and procedures of the federation. These policies and rules are defined by the federation and therefore can vary. Usually they include some general rules applicable to all members, and more specific rules that apply to IdP and SP. As an example, some of the rules of the UK Access Management Federation for Education and Research are listed in table 2 [8]. After being evaluated successfully, the CC will add the organization's credentials to the federation metadata.

[3] An organisation can have one or more service providers to expose their protected resources. How many instances of a Service Provider an organization provides depends on both technical details and organisational constraints. Usually, one Service Provider instance is sufficient when all hosted protected resources fall under the same security policy.

UK Access management Federation for Education and Research

Rules of Membership

Rules which apply to all Members

1 The Member warrants and undertakes that:
- All and any Data, when provided to the Federation Operator or another Member (as the case may be), are accurate and up-to date and any changes to Metadata are promptly provided to the Federation Operator;
- It will use its reasonable endeavours to comply with the Technical Specifications;
- It will observe Good Practice in relation to the configuration, operation and security of the System;
- It will observe Good Practice in relation to the exchange and processing of any Data and in the obtaining and management of the DNS names, digital certificates and private keys used by the System;
- It holds and will continue to hold all necessary licences, authorisations and permissions required to meet its obligations under these Rules.

2 The Member will not act in any manner which damages or is likely to damage or otherwise adversely affect the reputation of the Federation.

3 The Member may use the Federation logo in accordance with the Federation logo usage rules located at http://www.ukfederation.org.uk/WebsiteInfo as may be updated by the Federation Operator from time to time.

4 The Member grants the Federation Operator the right:
- To publish and otherwise use and hold the Metadata for the purpose of administering the operation of the Federation;
- To publish the Member's name for the purpose of promoting the Federation.

5 The Member must give reasonable assistance to any other Member investigating misuse. In particular, if the Member uses outsourced identity providers, it must cooperate with the identity provider to investigate and take action in respect of such misuse.

Rules applying to Service Providers

1 The Service Provider must not disclose to third parties any Attributes supplied by End User Organisations other than to any data processor of the Service Provider or where the relevant End User has given its prior informed consent to such disclosure.

2 The Service Provider will only use the Attributes for the following purposes:
- Making service access control or presentation decisions and only in respect of the service for which the Attributes have been provided;
- Generating aggregated anonymised usage statistics for service development and/or for other purposes agreed in writing from time to time with the End User Organisation.

3 The Service Provider acknowledges that it is responsible for management of access rights to its services or resources and the Federation Operator will have no liability in respect thereof.

- The **federation metadata** is an XML file hosted online by the CC that defines the circle of trust of the federation. It includes a listing of standard compliant network endpoints of IdPs and SPs. The circle of trust is asserted by the CC for a certain time by including an expiration date and by adding a digital signature to avoid tampering.

The procedure for logging in using an electronic ID card (eID) or token is the same. In this case, the (local) government sets up an IdP and the federation includes this IdP as a trusted party in the metadata [9].

Operational use of the federation requires that the user authenticates with his organization and not with each service provider. Once authenticated, **Single Sign-On** ensures that the user gets a session established with all service providers of the federation when required and is thus not required to re-authenticate. Authorization is established at the

side of the service provider and is typically based upon user attributes asserted by the identity provider. However, other pieces of information such as IP addresses or geo-location could be taken in account in addition to the user attributes.

- **Attribute**: characteristic of a subject, resource, action or environment [10]. Attributes consist of variable name / value pairs, some examples: 'user-id:set@user.example.com', 'group:developers', 'role:expert[4]', *etc.*

An important note is that the use of attributes that are considered Personal Identifiable Information (PII) should be avoided and can only be used with the explicit consent of the user.

An Access Management Federation for spatial data and services (**GeoAMF**) can be established leveraging the same architecture, roles and organizational principles. The main differences are, that a service provider hosts OGC Web Services instead of or next to regular web resources such as HTML pages and that the client is a desktop GIS or a web browser based geo-application such as an OpenLayers based client. In the context of the testbed the focus of the controlled access will be on INSPIRE type of network services consumed by these desktop and browser based applications.

3.2 Authentication and Authorization Standards

In this section we describe the relevant standards for setting up and managing controlled access mechanisms with focus on authentication and authorization. Other standards that might be relevant in geoRM are mentioned in a separate section but will not necessarily be implemented in the context of the testbed.

3.2.1 Secure communication

Secure communication is important to prevent unwanted modification of the information while in transit between computer systems. This project will leverage main stream IT technology to secure communication over the Internet: combining the standard communication protocol HTTP (IETF RFC 2616) with an encryption protocol – either SSL (Secure Sockets Layer; IETF RFC 6101; deprecated) or its successor TLS (Transport Layer Security; IEF RFC 6176) – results in HTTPS (IETF RFC 2818). The use of HTTPS for all communication renders other security standards unnecessary. HTTPS is a widely used international standard and relatively 'simple' to implement.

3.2.2 Authentication

In the framework of an access management federation, the process of authentication involves more than the action of logging in to a system. It entails the redirection to the appropriate identity provider, the actual logging in at this identity provider and, in case of a successful login, the passing on of a set of appropriate attributes to a service provider.

The Security Assertion Markup Language (SAML) [11] is an XML-based protocol for communicating user authentication, entitlement, and attribute information between business entities (service providers and identity providers). It was developed and continues to be advanced by the Security Services Technical Committee of the open standards consortium, OASIS (Organization for the Advancement of Structured Information Standards). SAML 2.0 was ratified as

[4] Roles are usually based on the function/position/task in the organization, or in case of SDI's in the network. E.g. ICT administrator, GI developer, GI expert, GI user, etc.

an OASIS Standard in March 2005[5], replacing SAML 1.1. SAML allows business entities to make assertions (a package of information) regarding the identity, attributes, and entitlements of a user to other entities.

The actual login happens at the identity provider and is therefore controlled / managed by the hosting party. The other two actions deal with authentication in a federated system and are made possible by the SAML protocol. It is a main stream IT Standard (OASIS) with a lot of existing implementations, based on Open Standards and Open Source Software. SAML is scalable, although not easy to implement. But this can be resolved by using one of the many toolkits to support implementation.

Metadata is a key concept in SAML. Metadata is typically kept at a coordination centre and mainly contains a 'white list' of trusted service providers and identity providers as well as their SAML compliant network endpoints, public keys to validate signatures from trusted partners, *etc*. The metadata kept at the coordination centre forms the basis of the trust relation between the asserting party (the IdP) and the relying party (the SP).

- **Endpoint**: the point where the communication takes place between entities. It is a location on the web, represented by an URL. Each entity in the federation has two types of endpoints leveraging the HTTPS protocol: Endpoints that are mandated to be compliant with the SAML standard which vary depending if it is an IdP or a SP; and endpoints that are used for login (IdP) or to execute protected services (SP). The SAML compliant endpoints get configured when you configure an IdP or SP of the federation and aggregated in the federation metadata. The IdP endpoints for login are not disposed publically; the IdP itself only knows them. The SP endpoints of data services are not part of the SAML metadata either. For discovery purposes, they may get registered in a catalogue.

SAML has emerged as the gold standard for federations, and even though other standards are available, only one other major protocol exists: OpenID. Both standards are open and both need proper implementation as to avoid security risks. The major difference is that SAML is based on an explicit 'trustee list' and OpenID is not, as a consequence, it has been stated often that OpenID is more vulnerable for authentication flaws [12] [13]. Table 2 provides a comparison between SAML (supported by Shibboleth) and OpenID. Some AAA implementations exist using one or both of these standards (see D1.2 – Analysing Best Practices)

Table 2: Comparison of different authentication standards (based on Chadwick, [13])

Standard	SAML / Shibboleth	OpenID
Complexity	Complex • Configuration needed, supported by implementation tools	Simple • Fewer options, out of the box implementation
WAYF[6] service	Needed • WAYF service with list of IdPs	Not needed • Uses the user's URL or XRI
IdPs and SPs	Dependency IdP and many SPs • Often IdP is home institution with high availability • Many SPs	Dependency IdP and few SPs • Dependency on OpenID provider to run service 24/7 • Many IdPs, but few SPs that want to

[5] Approved Errata for SAML V2.0 was last produced by the SSTC on 1 May 2012 (http://saml.xml.org/saml-specifications).

[6] WAYF – Where Are You From

		give access to services
Security issues	More reliable • Almost always linked to a real person • Trust infrastructure • Some privacy protection: SP cannot track users between sessions • re-allocation of ID's can be done • Very susceptible to phishing unless users scrutinize X.509 certificates carefully • Not susceptible to Cross Site Request Forgery	Many security weaknesses: • No assurance of who the user is • No trust infrastructure • No privacy protection: IdP and SP can track users between sessions • re-allocation of ID's can be done, but not designed to be life-long • Very susceptible to phishing • Susceptible to Cross Site Request Forgery

3.2.3 Authorization

Authorization is established at the side of the service provider and consists of managing access to a specific resource, based on access rights. These rights are based on the secure exchange of information (attributes) between the identity provider and service provider, made available by the SAML protocol. It is important to note that it is fundamental that the SP can trust the information received from the IdP, as the SP itself has no user accounts to verify.

Before discussing this mechanism further, first a couple of definitions are given [10], in order to clarify concepts:

- **Rule**: a condition: only selected individuals can view a particular dataset (e.g. given users, given users for set period of time, given users in set location or conditions specific to a subset of the data)
- **Policy**: a set of rules
- **Policy decision point** (PDP): the system entity that evaluates the applicable policy and renders an authorization decision.
- **Policy enforcement point** (PEP): the system entity that enforces the decisions made by the PDP.

The choice of standards and technology is up to the service provider. However, this does not lead to interoperability problems because of the federated approach: the authorization part is handled separately from the authentication mechanism which is handled centrally. Examples of widespread authorization standards are XACML, GeoXACML and OAuth. A short overview of these standards and their pros and cons are given in Section 3.

XACML (eXtensible Access Control Markup Language) defines an access control policy language encoded in XML and a processing model describing how to evaluate access requests according to the rules defined in policies. XACML is an attribute-based access control (ABAC) system: attributes associated with a user, the request context or system state serves as input to the decision whether a given user may access a given resource in a particular way. Role-based or location based access control can also be implemented as it is a special case of attribute-based access control [10].

GeoXACML (Geospatial eXtensible Access Control Markup Language) adds a few very specific components to the XACML 2.0 [14] standard: the definition of the geometry data type and the definition of geo-specific functions (e.g. test of topologic relations), [15].

This project's use cases are built on GeoXACML. The INSPIRE requirement analysis reveals the potential need for having support for geographical criteria[7]. It is only in cases where this is necessary that Geo-XACML must be used, in all other cases one can make use of XACML.

Table 3: Comparison of different authorization standards

Standard	What?	Pro	Con
XACML	XML-based open standard by OASIS	General purpose and widely used	Complexity
GeoXACML	Geo-extension to XACML	As XACML but with ability to index Rules and Policies based on geospatial conditions	Complexity
OAuth	Category or scoped based decisions	Enable to act "on behalf of"	Simplicity may not support complicated rights

It is important to note that the concepts of (Geo)XACML and OAuth are fundamentally different and, therefore, their applicability depends on the overall use case, architecture and access constraints. In the context of the testbed XACML/GeoXACML is to be favoured because of its geo-extension.

3.2.4 Other standards

Figure 3 illustrates the grouping of security standards but also shows their more general fit with main stream IT. It shows the many standards involved and the categories associated with them. It is therefore possible to separate the realization of secure communication into Network/Layer Binding and Application Layer security. For the first kind of systems, the use of HTTP + SSL or TLS is mandatory. However, there is the limitation that only computer-to-computer communication can be secured. In systems based on an enterprise service bus, where secured messages are sent between system endpoints and eventually get routed, the use of TLS may no longer be sufficient. In these cases, XML messages can become secured to ensure integrity or confidentiality by applying the Web Services Security (WS-Security) standard. With the SAML standard, the XML Digital Signature and XML Encryption standards (W3C) may get used to protect assertions as well as SOAP binding specific message. XML Digital Signatures is used to protect the federation metadata and to associate the metadata with the CC.

The standards of the Policy Layer and Licensing are outside the scope for this project. For completeness, the interested reader can read more about the other standards in Annex 1.

[7] See also *"D2.4 - Results of the Workshop: 'AAA-Architectures for INSPIRE', 16-17 March, Leuven".*

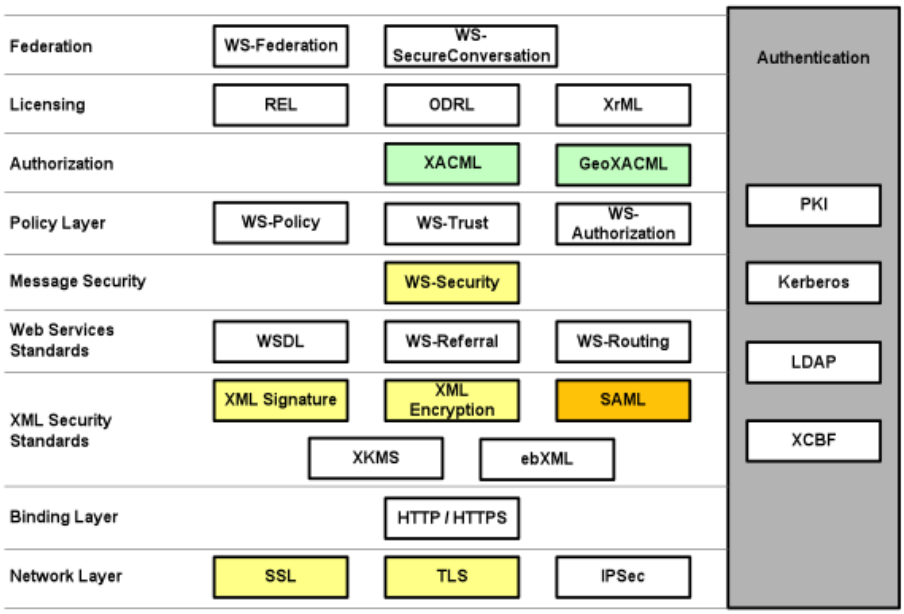

Figure 3: Schematic overview of AAA and related standards

3.3 Authentication and Authorization Technologies

The choice of technology is broader and more open, and will largely depend on existing software environments of the organisations that will implement the AAA mechanism. For authentication, information regarding usernames, passwords and a set of user attributes can be stored on different platforms: LDAP, Kerberos, PKI, XCBF or different types of databases such as MySQL db. For authorization each entity (SP and IdP) needs a SAML 2.0 endpoint built on top of the local technology.

Many tools exist to implement SAML and other authentication standards, some are open source, others are proprietary. We first give an overview, than discuss Shibboleth used in many implementations in more detail.

3.3.1 Tools for implementing SAML and other AAA standards

The Kantara initiative (see *https://kantarainitiative.org/*) aims at testing interoperability in different domains, including for SAML and other implementations of authentication/authorization standards. The initiative studied commercial and open source solutions for implementing security standards such as SAML. They analysed products and tools for different SAML actors (IdP, SP, Discovery Service[8] and Metadata services). Table 3 illustrates the broad spectrum of products that exist. The table was based on the work done by the Kantara initiative, but modified to reflect the new status of the different products and the addition of some other information[9]. The following elements of the software are described:

1. The name of the product
2. The project or organization that developed/maintains the product
3. The link to the main web site or resource

[8] The term "Discovery Service" is used in the context of SAML 2, which refers to the IdP Discovery Service as the implementation of the Common Domain Cookie Writing Service (with additional functions), as defined in the SAML Profile "Identity Provider Discovery Profile". This type of service should not be confused with the INSPIRE Discovery Service for searching and finding spatial data sets and services. .

[9] However, it should be noted that the table is based in readily available online resources, which might have led to incomplete or out-of-date information. This could not be verified in the context of this analysis since this would require carrying out an extensive survey among the producers of the different products.

4. The last year the product was updated
5. The type of license (OSS or commercial)
6. The programming environment / platform of the product
7. The supported roles
8. The support standards and protocols

A total of 65 products are documented, ranging from products from the Open Source community (16) to proprietary products from big (e.g. Oracle) or smaller system vendors (49). Of all those products, 46 provide support for IdP implementations, while 32 (also) support SP implementations. SAML 2.0 is supported by 68% of all the products, while OpenID is supported by 54% of the products and OAuth by 40%. As can be seen from the support of XACML (only 11% of the products support it) we can conclude that the focus of the products is on authentication, rather than on authorization.

Table 4: Tools for the implementation of security standards (adapted and updated from the Kantara Initiative, 2011)

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
adAS	PRiSE	*http://www.adas-sso.com/en/*	2011	OSS	Java jsp, PHP	1	1	1	1		1	1				1	1	1	
ADFS 2.1	Microsoft	*http://msdn.microsoft.com/en-us/library/bb897402.aspx*	2012	Comm.	Java script			1	1			1							
OpenOTP/TiQR SAML IdP	RCDevs	*http://www.rcdevs.com/products/openid/*	2013	Free	Java, JSON, PHP, ASP, .Net	1						1		1			1		1
AssureBridge SAMLConnect	Assure-Bridge	*http://www.assurebridge.com/our-products/samlconnect/*	NK	Comm.	Java, PHP, Python, .Net, Perl, Ruby, Spring	1	1	1			1	1		1					
Authentic2	Entrou-vert	*https://pythonhosted.org/authentic2/*	2012	OSS	PyPI	1	1						1	1					1

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
Bitium	Bitium	*https://www.bitium.com/*	NK	Comm.	NK	1	1					1							
CA Federation Manager	CA	*http://www.ca.com/be/en/securecenter/ca-siteminder-federation.aspx*	2010	Comm.	NK			1											
Centrify DirectControl	Centrify	*http://www.centrify.com/standard-edition/overview.asp*	2014	Comm.	Linux platform					1	1	1		1		1	1		
Citrix Open Cloud	Citrix	*http://www.citrix.com/products/cloudplatform/overview.html*	2014	Comm.	NA														
Cloud Identity Manager	McAfee	*http://www.mcafee.com/us/products/identity-and-access-management/index.aspx*	2014	Comm.	McAfee platform							1	1	1	1		1		
Cloud Federation Service	Radiant Logic	*http://www.radiantlogic.com/products/radiantone-cfs/*	NK	Comm.	NA	1	1	1				1	1	1					

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols												
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
Cloudseal	Cloudseal	*http://www.cloudseal.com/*	NK	SaaS / OSS	REST API, Java SDK, Spring, Tomcat	1	1												
Comfact IDP	Comfact	*http://www.comfact.com/Product/IdP/*	2014	Comm.	Prosale API	1													
Connectis	Connectis	*http://www.connectis.be/en/*	NK	Comm.	NK	1	1												
Corto project home	GÉANT	*https://code.google.com/p/corto/*	2011	OSS	PHP,	1	1					1							
Dot Net Work-flow	The Dot Net Factory	*http://www.dotnetfactory.com/*	NK	Comm.	NK	1	1	1	1	1			1	1				1	
DirX Access	Atos/Sie	*http://atos.net/en-us/home/we-*	2013	Comm	NA												1		

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
	mens	*do/cyber-security.html*		.															
DualShield	Deepnet Security	*http://www.deepnetsecurity.com/products/dualshield/*	2012	Comm.	NA	1						1					1		
Elastic SSO Team	9STAR	*http://www.9starinc.com/solutions/elasticsso-team*	2014	Comm. / SaaS	NA	1					1	1							1
Elastic SSO Enterprise	9STAR	*http://www.9starinc.com/solutions/elasticsso-team*	2014	Comm.	NK	1					1	1							
ESOE	Queens-land University of Tech-nology	*http://esoeproject.qut.edu.au/*	2010	OSS	Java, Apache	1	1					1		1	1		1		

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
Entrust GetAccess	Entrust	*http://www.entrust.com/products/entrust-getaccess/*	2013	Comm.	API's for apps, WebSphere, WebLogic, .NET	1				1	1	1			1		1		
Entrust IdentityGuard	Entrust	*http://www.entrust.com/products/entrust-identityguard/*	2013	Comm.	NK	1													
EIC	Ericsson	*http://excitera.nu/eic05/ericsson.ppt*	NK	Comm.	NK														
EmpowerID	The Dot Net Factory	*http://www.empowerid.com/*	2014	Comm.	Ruby, .NET, Java, HTML 5, PHP	1	1	1	1	1			1	1				1	
Fugen Cloud ID Broker	Fugen Solutions	*http://www.fugensolutions.com/cloud-id-broker.html*	2013	Comm.	NA			1	1		1	1	1	1					

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols												
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
Gluu Server	Gluu	*http://www.gluu.org/gluu-server/overview/*	2014	OSS	Python, Java	1						1		1			1		1
HP IceWall SSO	HP	*http://h50146.www5.hp.com/products/software/security/icewall/eng/sso/*	2012	Comm.	NK		1					1							
ILANTUS Sign On Express	Ilantus	*http://www.ilantus.com/sso_connectors.html*	2012	Comm.	NK	1	1					1	1	1			1		
Intel Cloud SSO	Intel	*https://software.intel.com/en-us/blogs/2012/02/27/introducing-cloud-idaas-intel-cloud-sso*	2012	Comm.	NK	1	1					1	1	1					
iSAML	Avoco	*http://www.avocoidentity.com/avoco-platform/isaml/*	2014	Comm.	NK	1			1			1		1				1	
JOSSO (Community Ed.)	josso.org	*http://www.josso.org*	2013	OSS	Java	1	1		1			1	1			1	1		

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
JOSSO (Enterprise Ed.)	Atricore	*http://www.josso.org*	2013	Comm.	Java	1	1		1			1	1			1	1		
Juniper SSL VPN	Juniper Networks	*http://www.juniper.net/us/en/products-services/security/sa-series/*	2014	Comm.	Hardware	1													
Layer 7	SecureSpan Gateway	*http://www.layer7tech.com/*	2014	Comm.	NK			1	1	1	1	1	1	1		1	1		
Larpe	Entrouvert	*https://dev.entrouvert.org/projects/larpe/wiki/Larpe_Administrator_Guide*	2011	OSS	Python								1	1					1
LemonLDAP	LemonLDAP	*http://lemonldap-ng.org/welcome/*	2014	OSS	Perl	1	1	1				1		1			1	1	1
NetIQ Access Manager	NetIQ (formerly	*https://www.netiq.com/products/access-manager/*	2014	Comm.	JRE	1	1	1		1	1	1	1	1				1	

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols										
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
	Novell)																		
NetWeaver Appserver	SAP	*http://help.sap.com/saphelp_nw70/helpdata/en/84/54953fc405330ee10000000a114084/content.htm*	2014	Comm.	ABAP, Java									1				1	1
OpenAM	ForgeRock (ex. Sun)	*http://openam.forgerock.org/*	2014	OSS	Java 7, C SDK, Jboss, Jetty, Web-sphere, Weblogic, ...	1		1	1				1		1	1		1	
Okta	Okta	*https://www.okta.com/*	2014	Comm.	NK	1	1										1		
OneLogin	OneLogin	*http://www.onelogin.com/*	2014	Comm.	NA	1	1	1			1	1	1	1		1	1	1	1

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
OpenAthens LA	eduserv	*http://www.openathens.net/*	2014	Comm.	JRE v6	1					1	1				1	1		1
OpenAthens SP	eduserv	http://www.openathens.net/	2014	Comm.	Native Java API, Native C API		1				1	1							
Open Select	OpenASe-ASe-lect.org	*http://www.ohloh.net/p/openaselect*	2011	OSS	NK							1	1	1					1
Oracle Identity Federation 11g	Oracle	http://www.oracle.com/technetwork/middleware/id-mgmt/index-084079.html	2013	Comm.	NA	1	1	1			1	1		1				1	
PhoneFactor	Phone-Factor, Inc (ac-quired by	http://www.manageengine.com/products/passwordmanagerpro/help/phone-factor-authentication.html	2013	Comm.	Java, .NET, PHP	1					1	1					1		1

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
	MS)																		
PicketLink	JBoss Commu-nity	http://picketlink.org/	2014	OSS	Java EE and Java SE Platforms						1	1	1	1	1				1
PingFederate	Ping Identity	https://www.pingidentity.com/products/pingfederate/	2013	Comm.	Java, .NET, PHP	1	1	1	1			1	1	1				1	
PortalGuard	PistolStar, Inc.	http://www.portalguard.com/	2012	Comm.	.NET	1	1	1				1					1		
RSA Federated Identity	RSA	http://belgium.emc.com/security/rsa-identity-and-access-management/rsa-federated-identity-manager.htm	2013	Comm.	NK	1	1	1				1		1				1	

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
Safe-where*Identify	Safe-where	http://safewhere.com/product/safewhere-identify/	NK	Comm.	NK	1	1	1	1			1	1	1			1	1	
SecureAuth	Se-cureAuth Corp.	http://www.secureauth.com/	2013	Comm.	J2EE, .NET, ...	1	1				1	1	1	1				1	1
Shibboleth	Internet2	https://shibboleth.net/	2013	OSS	C++, Java	1	1				1	1							
Sim-pleSAMLphp	UNINETT AS	https://simplesamlphp.org/	2013	OSS	PHP			1				1	1	1			1	1	1
SMS Passcode 6	SMSPasscode	http://www.smspasscode.com/company/news-press/version6	2013	Comm.	NA	1													
SSO EasyCon-nect	SSO Easy	http://www.ssoeasy.com/	2014	Comm.	IIS, J2EE, Apache, and other com-mon applica-tion\web	1	1	1			1	1					1		

Product name	Project or vendor	Web site	Last release / revision	License	Development Environment	Roles		Protocols										
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
					servers														
Symlabs Federated Identity Suite	Symlabs	http://saml.xml.org/symlabs-symlabs-federated-identity-suite	2008	Comm.	C, C++, Perl, Python, PHP, Java			1					1	1					1
Symplified	Symplified	http://www.symplified.com/	2013	Comm.	NK	1	1	1			1	1	1	1	1			1	
Tivoli Federated Identity Manager	IBM	http://www-03.ibm.com/software/products/en/federated-identity-mgr	2013	Comm.	Jacl, Jython scripting and Java API	1		1	1	1		1	1	1					
TrustBind	NTT Software Corp	http://www.ntt.com/	NK	Comm.	NK									1					

Product name	Project or vendor	Web site	Last re-lease / revi-sion	Li-cense	Develop-ment Envi-ronment	Roles		Protocols											
						IdP	SP	WS-Federation	WS-Trust	WS-Security	SAML 1.x	SAML 2.0	Oauth	OpenID	XACML	Kerberos	LDAP	Social media	Other
TrustBuilder	SecurIT	http://www.trustbuilder.be/	2014	Comm.	Java-EE-based	1	1					1	1	1		1			
Ubisecure Solutions		http://www.ubisecure.com/	2013	Comm.	NA			1				1		1		1	1		1
WSO2	wso2	http://wso2.com/	2013	OSS	NK	1			1				1	1					
ZXID	zxid	http://www.zxid.org/	2013	OSS	Java JNI extension	1	1			1					1				
						46	32	24	14	8	19	44	26	35	7	10	23	16	16

Other toolkits exist to integrate applications and services into SAML federations or to develop SAML IdPs. Most of these are OSS. Examples are:

- LASSO from Entrouvert provides a SAML-Library with C/C++, Python, Java, Perl and PHP components under the GNU General Public License (with an OpenSSL exception)[10];
- Mujina from SURFNet allows configuring and testing of IdP and SP set-ups[11];
- MET from TERENA makes it possible to gather and show information about federations (mostly about SPs and IdPs)[12];
- PyFF from Sunet.se is a SAML Metadata Processor[13];
- Raptor from Jisc is a toolkit to enable Shibboleth IdP statistics analysis[14]

For a more complete list of toolkits see:

http://kantarainitiative.org/confluence/display/certification/2011+Q1+Kantara+Initiative+SAML+2.0+Full-Matrix+Interoperability+Testing

3.3.2 Shibboleth

Shibboleth is one of the most popular open source environments to implement and manage federations. Shibboleth created an architecture and open-source implementation for identity management and federated identity-based authentication and authorization (or access control) infrastructure based on SAML (Shibboleth 2.0 is based on SAML 2.0). The IdP in Shibboleth 2.0 has to do additional processing in order to support passive and forced authentication requests in SAML 2.0. The SP can request a specific method of authentication from the IdP. Shibboleth 2.0 supports additional encryption capacity and sets a default session life of 30 minutes. Attributes can be written in Java or pulled from directories and databases. Standard X.500 attributes are most commonly used, but new attributes can be arbitrarily defined as long as they are understood and interpreted similarly by the IdP and SP in a transaction. Shibboleth is open-source and provided under the Apache 2 license. Several AAA implementations have used Shibboleth, also in the context of SDIs and INSPIRE (e.g. Persistent TestBed (PTB) initiative of AGILE-OGC-EuroSDR).

[10] *http://lasso.entrouvert.org/*

[11] *https://github.com/OpenConext/Mujina/*

[12] *https://github.com/TERENA/met*

[13] *http://leifj.github.io/pyFF/*

[14] *http://iam.cf.ac.uk/trac/RAPTOR/*

4. Access Management Federation Infrastructure: how it works

This chapter describes how the different standards support the AMF infrastructure and organisational set-up. We first describe the process of accessing resources in a secured way, then we describe some of the organisational challenges.

4.1 Secure access to resources

Figure 4 explains in a step-by-step approach how the access management federation infrastructure works based on a hypothetical example indicating the standards used:

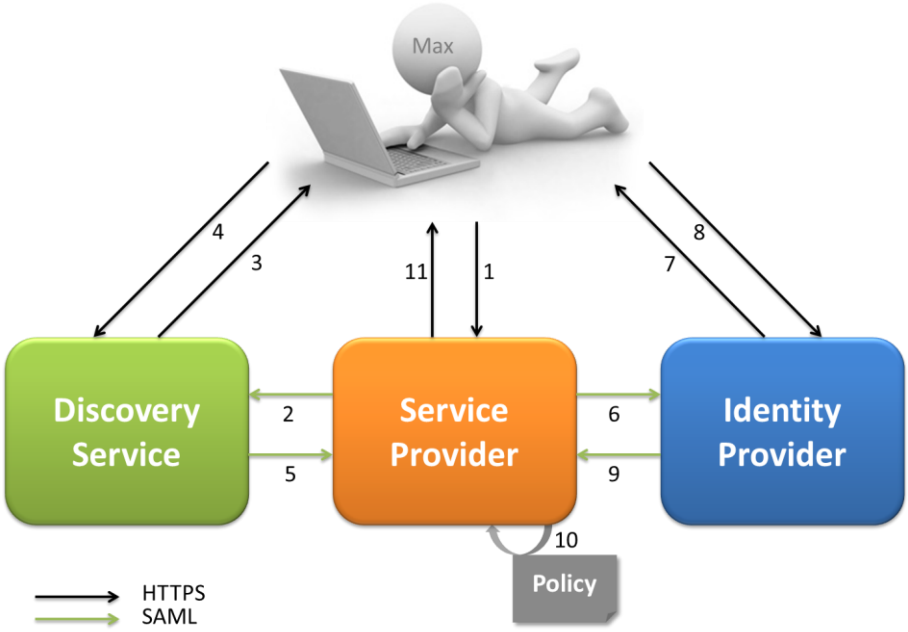

Figure 4: Schematic overview of the access management federation.

- Step 1. The user sends a resource request to a service provider.
- Step 2. Because the service provider does not know the user, it redirects to the discovery service so that the user can select the IdP of his own organization.
- Step 3-4. The discovery service prompts the user with a list of possible identity providers and the user selects his or her home organization.
- Step 5. The discovery service returns this information to the service provider.
- Step 6. The service provider redirects to the selected identity provider.
- Step 7-8. The identity provider prompts the user for the credentials (often username and password, can also be an eID or token). The authentication will always happen at the users' home organization.
- Step 9. The identity provider manages a set of attributes for each registered user. In case of a positive authentication, the appropriate attributes are sent to the service provider. These

attributes will not contain privacy-sensitive information, unless approved by the user.

- Step 10. The service provider uses these attributes to authorize the user. This is done by consulting a policy. This step is always executed locally.
- Step 11. The user is granted or denied access to the data or services accordingly.

Let's clarify this with an example:

Our friend **Max** is an expert working for the JRC. He would like access to resource X, hosted at the servers of the BKG (*Bundesamt für Kartographie und Geodäsie*). The **service provider of the BKG** recognizes some user wants access and informs the discovery service. The **discovery service** prompts Max with a small list of identity providers, amongst others the JRC. Since Max is working for the JRC, he selects this as his home organization. The discovery service passes this information on to the service provider of the BKG, which in turn sends this information to the **JRC's identity provider**. The login screen from the JRC appears and Max has to pass on his credentials (username and password). If he does this correctly, the JRC will send a list of attributes about Max to the service provider of the BKG. These attributes include information that, for example, Max is a member of the JRC and that his role there is 'expert' until 31/12/2016. The service provider of the BKG uses the received attributes about Max and consults a locally stored policy to determine the access rights. One of the rules states that current JRC experts get access to resource X. As a consequence, Max is granted access to this resource.

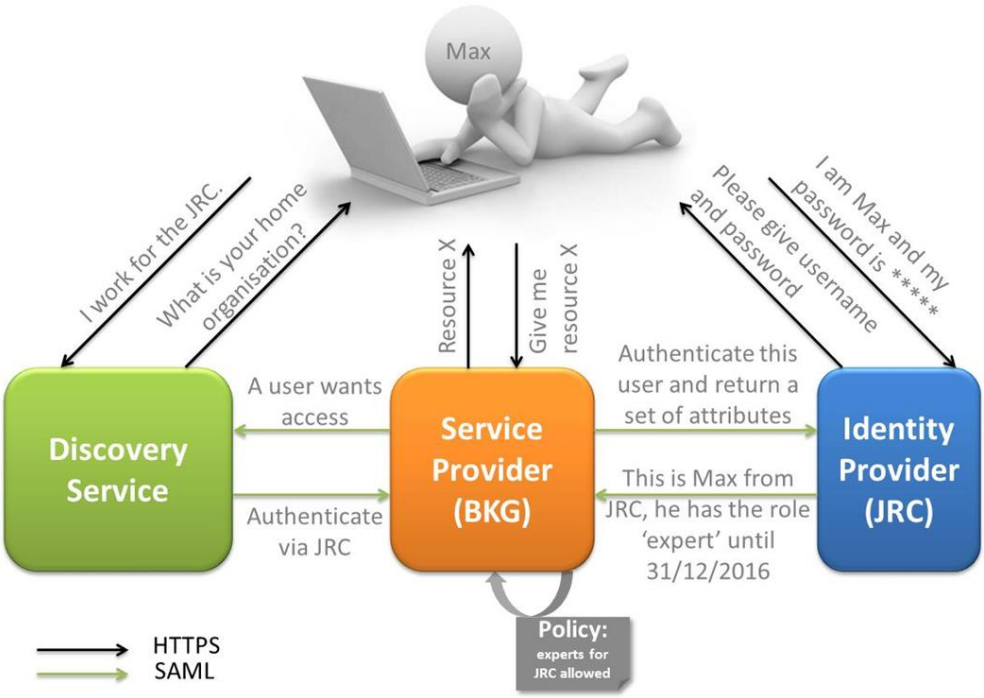

Figure 5: Example of secure access to a resource by a user (Max)

4.2 Organisational issues

The group of entities in the trust relation, managed by the coordinating centre, can be in the order of thousand members. Scaling is no problem for SAML. The white list (metadata) is unrelated to the number of re-

sources (data sets or service endpoints) made available by each service provider. Moreover, a more extensive metadata list, even with thousands of members in the federation, will not jeopardize access performance[15]. A list of the latter should be looked for in the INSPIRE catalogue and/or could be derived from the INSPIRE Monitoring & Reporting sheets. The number of Identity and Service Providers might have an impact on how to organise the federation: e.g. in case of huge numbers (several 10-thousands) a federation of federations might be the solution[16]. In case we speak about a few thousand providers, this would not be necessary. A first estimate of data and service providers (see figure 4) based on number of unique data and service providers per country reveal that hypothetical there would be around 2000[17]. This number can be compared to the academic federation in the US (InCommon) which currently comprises of approximately 1500 SPs and 240 IdPs.

[15] The only performance issue may appear when the user searches for the IdP using the search field provided by the Discovery Service. When a user is affiliated with one IdP only and saves the selection of the IdP, the search in the IdP list takes place only once. For each established session, only HTTPS and cookies are used on direct communication between the client and the service provider. The entire SAML "machinery" including metadata is not used at that point.

[16] In the context of AAA Infrastructures for research and education, the issue of a federation of federations is discussed and implemented already. For example, the eduroam service in Europe, which operates in the context of the GÉANT project, has evolved into a confederation: a federation of federations. Different concepts and implementations can be seen to exist but it is, to date, unclear if they can be leveraged 'as is' for a federation of geospatial data and services and applications. The setup of a federation for geospatial services and web mapping applications introduces specific technical requirements (although based on common ICT standards). In order to give a clear answer whether the concepts of federation of federations from the academic world can be re-used at all (or with specific modifications) needs a more specific investigation. For further details see: D3.3 - *Technical report on the finalised testbed*).

[17] The figures for Germany and Denmark are not yet included because the name of the provider is not part of the information in the XML file (other member states use the XLS template instead).

Table 5: number of data and service providers in INSPIRE

	Spatial Data Sets				Services							All
	Annex I	Annex II	Annex III	All	Discovery	View	Download	Transfor-mation	Invoke	Other	All	
Austria	16	13	43	**48**	5	16	12	-	-	-	**16**	**48**
Belgium	18	17	35	**46**	9	22	6	-	-	2	**24**	**52**
Bulgaria	19	18	21	**26**	8	8	7	-	-	-	**11**	**27**
Cyprus	15	8	41	**48**	7	5	2	-	-	1	**8**	**49**
Czech Republic	16	3	16	**21**	7	12	2	1	-	5	**13**	**23**
Denmark				**0**							**0**	**0**
Estonia	9	2	7	**14**	1	6	3	1	1	-	**8**	**16**
Finland	48	7	72	**76**	1	35	7	1	-	-	**37**	**78**
France	173	84	369	**481**	3	84	52	-	-	1	**85**	**491**
Germany				**485**							**222**	**492**
Greece	46	27	59	**90**	8	24	1	-	1	3	**27**	**102**
Hungary	10	4	8	**17**	2	8	4	-	-	-	**8**	**18**
Iceland	6	3	18	**21**	7	1	-	1	-	-	**7**	**21**
Italy	26	26	29	**35**	23	32	19	7	1	3	**32**	**40**
Latvia	8	3	13	**17**	1	8	3	-	-	1	**8**	**17**
Liechten-stein	1	1	1	**1**	-	1	1	-	-	-	**1**	**1**
Lithuania	8	5	12	**16**	12	11	4	4	-	-	**12**	**16**
Luxem-bourg	5	3	4	**7**	1	1	1	1	-	-	**1**	**7**
Malta	4	1	0	**4**	1	1	1	-	-	-	**1**	**5**
Nether-lands	9	4	11	**18**	1	10	10	-	-	-	**11**	**22**

Norway	9	6	20	**23**	3	15	14	1	-	3	**19**	**25**
Poland	5	2	10	**13**	5	7	3	-	-	-	**7**	**15**
Romania	17	9	31	**45**	8	12	3	-	-	-	**13**	**48**
Slovakia	13	4	12	**19**	2	8	3	-	-	-	**10**	**19**
Slovenia	7	3	9	**11**	3	5	4	-	-	-	**5**	**11**
Spain	75	49	97	**132**	16	219	37	-	2	6	**226**	**304**
Sweden	9	3	19	**23**	1	11	11	-	-	-	**11**	**23**
UK	43	9	29	**64**	1	6	2	-	-	-	**8**	**68**
Total				**1801**							**831**	**2038**

Another important organizational issue is the complexity of implementation and therefore the need to have the necessary human resources, e.g. ICT experts with good knowledge and skills on secure access mechanisms and the set-up of an AMF. There is a clear need for a coordinating centre for managing the AMF. It is assumed that IdPs are usually existing organizations already doing this type of activities, while it will be a relatively new activity for SPs (these are usually e.g. mapping agencies) who have usually no experience in this field and thus might be obliged to hire expertise from the private market. However it is relatively difficult to make an estimation of the costs related to the set-up of an IdP, an SP or a whole AMF since so many factors are influencing this.

5. ISA PROGRAMME: INTEROPERABILITY SOLUTIONS FOR EUROPEAN PUBLIC ADMINISTRATIONS

The ISA programme consists of more than 40 actions to facilitate cross-border electronic collaboration. Several of them are relevant to this work. The two most important ones are ISA action 1.4 focussing on authentication, while action 1.18 is focussing on authorization. In addition, other activities are taking place that are highly relevant: e.g. Action 1.9 in which Digital Signature Software (DSS) has been developed, and Action 1.19 which included the secured Trans European Services for Telematics between Administrations (sTESTA) initiative and the development of a Platform to support the secure exchange of documents between Public Administrations at national and European level (e-TrustEx). All the ISA actions must facilitate electronic cross-border and cross-sector interaction between European public administrations in an efficient and effective way. Furthermore, European public administrations should improve sharing and the re-use of existing or new Interoperable solutions, common services and generic tools. Finally, it is the aim to obtain flexible and interlinked IT systems allowing smooth implementation of Community policies and activities.

5.1 ISA action 1.4: EU-wide interoperability of electronic identities (ECAS-STORK integration) [12]

STORK [13] (Secure idenTity acrOss boRders linKed) aims to implement EU-wide interoperability of electronic identities (eID). While eID is already used in the area of e-Government in the Member States, it can also be of considerable value for secure access to the European Union's own information systems. The latter have their own authentication system known as ECAS (European Commission Authentication Service).

While STORK was originally developed as a European Large Scale Pilot (LSP), co-funded by the EC under the CIP programme, the results were maintained by Action 1.5 (STORK sustainability). On the other hand, Action 1.4 (ECAS-STORK integration) focused on setting up local proxies or PEPS at the EC side so that the corporate applications of the European Union institutions such as CIRCABC or the e-Justice Portal could benefit and use STORK authentication services in a cross-border dimension. STORK implemented and deployed in various Member States a federated platform based on common specifications and an assurance model. STORK aimed at the provision of electronic identification services for citizen´s accessing e-Government applications in cross-borders set-ups. STORK reference components (PEPS and VIDP modules) are continuously updated to cover the most common operating environments. Moreover, the technical specs (SAML profile and QAA model) are also updated according to new needs. However, the problem with this first phase was that Member State officials and civil servants from all over Europe need to access EC corporate applications, but that the national eIDs are not recognised by the EC applications. Therefore, ECAS credentials are used.

The goal of the current *ECAS-STORK integration action* is to develop a secure and user-friendly solution that will **allow users to access EU information systems, using their national eID** solutions and procedures to authenticate (thus with minimal impact on these information systems). The integration will reduce the number of credentials a user has to rely on. At the same time it will enhance security, since national eID solutions are normally based on credentials that are stronger than just a login name and password. The system will also have to cater for users who are not eligible to use STORK. The ECAS-STORK integration is currently in production mode and it is already used by CIRCABC and the eJustice Portal.

5.2 ISA action 1.18: Federated Authorization Across European Public Administrations [14]

The action aims to extend federated authentication (i.e. verifying if the user is the one he claims to be) by using STORK for federated authorisation (i.e. verifying if the user is entitled to use the requested information or functionality). It **allows users to log in to EC applications and to be granted access based on their role or**

position. For example in case the user is a public official and the application aims at usage by an administration. Access attributes are fully administered in the users' home country. The action removes the overhead to manage users at national level for internal needs and at ECAS level for EC information systems.

The scope of this Action includes reviewing existing approaches in the Member States, choosing a suitable model, defining common, generic specifications and implementing the chosen model. These project's steps cover the needs of a federated authorisation solution. In particular, it addresses the risks and concerns of heterogeneous solutions within the Europe and potential architectural approaches to fulfil the needs of trust and security.

The project that will implement this is STORK 2. It is based on the experience of STORK 1 including experiences in the Member States. It is aiming at setting-up a European Federated Circle of Trust, extending the national circle of trust to the European level, while hiding national details that other countries do not need to deal with. It is fully scalable. The STORK circle of trust is formed by each of the national PEPS, together with each of the corresponding IdPs. These systems trust each other explicitly. This explicit trust means that the relevant data of these circles are stored at each of the other circles' sites: e.g. the certificate which is used for signing, the URL where to send requests to, the country's name and abbreviation, etc. This trust requires that each of these systems is secure; thus each of them has passed a "Security Self-Assessment" with which each of the Member States makes sure to fulfil most usual security criteria[18]. PEPS will verify each request it receives, rejecting requests that are not sent by members of its circle of trust. Its circle of trust includes each Member State PEPS, its own local SPs and, for non-PEPS countries, SPs whose certificate is issued by the national authority or for any other reason trusted by the PEPS. This is in general the mechanism to restrict the access to the PEPS. The STORK platform establishes the interoperability of electronic identities across borders in Europe, allowing nationally recognised credentials to be accepted in a uniform way by service providers in other countries. This involves so many different parties, that often the simplest solutions are chosen. As a service provider normally does not know any ID provider in other countries, the trust cannot be explicit, service providers must trust the ID providers which are trusted by their national authorities, which are in turn trusted by the authority in the SP's country. The other way around, the same rule applies: an ID provider cannot claim to know each service provider in all foreign countries.

STORK supports multiple eIDs and eID types. Also mobile eIDs are supported (e.g. AT, EE, LU, SE…). More countries are involved now (19): in 2012 18 Member States were involved; between 2013 and 2014 5 more Member States and other countries joined or will join (CH, CZ, TR), while two countries are not involved anymore (DE, FI).

STORK 2 addresses issues that were not addressed by STORK 1. This is summarized in table 6.

Table 6: Issues addressed by STORK 2 as compared to STORK 1

Issue	STORK 1	STORK 2
Representation and mandates; attribute provision	Limited to natural persons on their own behalf	Core of STORK 2.0 common specifications and all pilots
High attack potentials or	Security addressed, but STORK	Pilot eHealth and Internet

[18] Currently, within the STORK project, there hasn't been enough time to execute a normal security audit by a competent accreditation body.

access to sensitive data	1 pilots had no valuable targets	banking
Private sector services and service providers	Mainly e-Government services	Will pilot company services and Internet banking
Liability and recognition	No provisions if something "goes wrong"	Part of eIDAS, but STORK investigates interim solutions
Standardization and business models	Specifications, but no standards	Dedicated work on eID service offerings

The experience of STORK and related activities of the ISA programme will be taken into consideration in the analysis phase of the project, and in particular in the preparation and development of the testbed. Several aspects could/should be covered:

- The STORK approach for secure access to governmental systems by individual citizens through e-ID will be investigated and might become part of one of the use cases of the testbed. It would be an alternative for the use of OpenID that has already been tested in the context of previous projects.
- STORK, and in particular STORK 2.0 has/is worked/working on the defintion of different type of attributes to be exchanged between IdPs and SPs. This is highly relevant for the AAA-testbed. The proposed attributes in the context of STORK will be analysed and taken into account when preparing the testbed.
- The way the federation of trust is established in STORK 2.0 can provide helpful insights on how the implementation of a CC, IdPs and SP could work in the context of INSPIRE. In particular, it is of interest to take into account how PEPs and PDPs work in STORK.

In the analysis phase several aspects of STORK will be analysed further in more detail.

6. CONCLUSIONS

This report aimed to analyse the state of the art with regard to the existing ICT standards and technologies that could support an AAA implementation for INSPIRE. Secure Authentication and Authorisation providing (public) access to INSPIRE data and services is an important layer of the INSPIRE infrastructure of the Member States. This layer should support Member States' data policies to (eventually) limit public access or to enforce certain conditions for sharing and use: e.g. by providing paying services to access and/or download certain spatial data sets or to limit access to (parts of) spatial data sets for certain user groups.

The most logical choice for implementing an AAA layer is to develop a federated system (AMF) based on existing (generic) ICT standards and technologies and linking to existing AAA solutions already in place in the Member States (e.g. existing IdPs, AAA projects implementing parts of eID solutions in the context of the ISA STORK 2.0 action). The report describes a series of standards and technologies on which such a federated system could be built. The analysis reveals that basic standards for secure communication (e.g. HTTPS), together with standards for central authentication following the principles of Single Sign-On such as SAML, and GeoXACML for decentralised authorisation (eventually based on spatial criteria) at the level of the Service Providers, could work together for the development of an AAA testbed for INSPIRE. Many more standards exist; a full list is provided in annex 1, but most of them are out of scope for the testbed phase. The proposed AMF could easily be combined with existing technical solutions already provided by IdPs and SPs. There exist many software tools to implement federated solutions. The report provides an extensive overview of both open source and proprietary solutions, alongside their characteristics. The consortium proposes to use Shibboleth for the testbed development because a lot of experience was gained in several projects and it allows scaling to take place more easily.

This work has also identified specific topics that still need particular attention in the analysis and testbed phases: 1) the definition of the attributes that will be exchanged between the IdPs and SPs (taking into account legal aspects such as privacy); 2) the attribution of roles / rules as part of the data policy of SPs – who gets access to what / which parts of spatial data sets; 3) performance and scalability aspects, and 4) the connection to and use of the AAA layer from within different types of applications (web mapping, desktop, …). The work will aim to address these issues in more or less detail in the analysis and testbed phase. The most important aspect of the testbed will be to demonstrate how an AMF implementation based on the selected standards and technologies would/could work in practice and in real organisational settings.

Finally, it should be mentioned that there are also many organisational challenges: how would a coordination centre in the context of INSPIRE work (and who will play this role); how many IdPs and SPs will exist in the context of INSPIRE; what different data policies will be developed by SPs (that might influence the complexity of the AAA approach); how can commercial users find an IdP which is setup and known in the AMF or created on-the-fly (e.g. through services/service providers); etc.? These organisational questions will only be tackled through the current project in a limited way, but should certainly be investigated in future work.

7 REFERENCES

[1] "Geospatial Digital Rights Management Reference Model (GeoDRM RM)," 28 02 2006. [Online]. Available: http://www.opengeospatial.org/standards/as/geodrmrm. [Accessed 17 02 2014].

[2] Open Geospatial Consortium, *Architecture of an Access Management Federation for Spatial Data and Services in Germany*, A. Matheus, Ed., 2012.

[3] UK Location, *Access Control and Rights Management Position Statement v1.0*, 2012.

[4] "UK Access Management Federation," UK Federation, [Online]. Available: http://www.ukfederation.org.uk/. [Accessed 02 2014].

[5] "InCommon," InCommon Steering Committee, [Online]. Available: http://www.incommon.org/. [Accessed 02 2014].

[6] "Authentication and Authorization Infrastructure KU Leuven," KU Leuven ICTS, [Online]. Available: http://shib.kuleuven.be/. [Accessed 02 2014].

[7] "DFN-AAI - Authentifikations- und Autorisierungs-Infrastruktur," DFN-Verein, [Online]. Available: https://www.aai.dfn.de. [Accessed 02 2014].

[8] UK Access Management Federation for Education and Research (2011) Rules of Membership, version 2.1.

[9] "eid-idp," Google Code, [Online]. Available: https://code.google.com/p/eid-idp/. [Accessed 02 2014].

[10] "eXtensible Access Control Markup Language (XACML) Version 3.0," OASIS, [Online]. Available: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html. [Accessed 02 2014].

[11] "OASIS Security Services (SAML) TC," OASIS, [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. [Accessed 02 2014].

[12] "Federated Identities: OpenID vs SAML vs OAuth," SoftwareSecured, 06 2013. [Online]. Available: http://www.softwaresecured.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth. [Accessed 02 2014].

[13] JISC (2008). Review of OpenID. JISC Final Report

[14] "eXtensible Access Control Markup Language (XACML) Version 2.0," OASIS, [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf. [Accessed 02 2014].

[15] "Access Control for Geospatial Data," Secure Dimensions GmbH, [Online]. Available: http://geoxacml.secure-dimensions.net//. [Accessed 02 2014].

[16] "EU-wide interoperability of electronic identities," ISA, [Online]. Available: http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-4action_en.htm. [Accessed 02 2014].

[17] "Stork," Stork consortium, [Online]. Available: https://www.eid-stork.eu/. [Accessed 02 2014].

[18] "Federated Authorisation Across European Public Administrations," ISA, [Online]. Available: http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-18action_en.htm. [Accessed 02 2014].

[19] "An interoperable solution for electronic identities (eIDs)," ISA, [Online]. Available: http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-5action_en.htm. [Accessed 02 2014].

[20] Kantara Initiative, 2011.

8 Annex 1: Security Standards Overview

8.1 Standards for securing Communication

This section of the document provides an overview of standards, recommendations and other literature related for establishing secure communication.

8.1.1 Standards associated with the Network Layer

IPSec (see [1])

IPSec defines a protocol that secures Internet Protocol (IP) based communication between network endpoints on ISO/OSI layer 3 (network layer). It thereby creates secure tunnels through untrusted/unsecure networks ensuring confidential and authenticated communication. Sites connected by these tunnels form Virtual Private Networks (VPNs).

The following protocols are used in IPsec:

- ESP (Encapsulating Security Payload) is the encrypted information that is transported,
- AH (Authentication Header) provides authentication for data packets and
- IKE (Internet Key Exchange) negotiates connection parameters.

The strength of IPSec is that applications can use the secure communication established (provided) by IPSec without any knowledge. Even though this is a strength, it needs to be remembered that IPSec does not establish an end-to-end secure communication, as it is provided by message layer security. This is important to understand when building a network topology that consists of multiple segments, each using their own IPSec configuration.

TLS / (SSL) (see [2])

The TLS/SSL protocol enables applications to communicate in a point-to-point fashion by establishing a secure communication channel that supports integrity and confidentiality of the exchanged information. It requires that the server authenticates itself. Also, TLS/SSL provides optional mutual (client) authentication, which is almost never used. Based on a challenge request/response handshake that involves asymmetric encryption, the client and server establish (agree on) a shared secret (symmetric key) to encrypt all further communication that is associated to the current session.

Because TLS/SSL secures the entire information that is exchanged between communication partners, it cannot be used if individual parts of one message are or the entire message is

confidential for receivers different from the client and the server. Also, transparent proxy connections are not possible.

In addition, the use of TLS/SSL is not sufficient if message repudiation is important, as the encryption is based on a shared secret. Here, message layer protection must be established to enable secure and trusted audit.

8.1.2 Standards associated with the Binding Layer

HTTP(S) (see [12])

HTTPS is defined as HTTP over TLS in the IETF RFC 2818. It defines how HTTP leverages TLS to establish a secure communication over the Internet using the *https://* URI scheme. Simply speaking is the result of an HTTPS connection communication of encrypted messages using the standard port 443.

8.1.3 Standards associated to Message Security

WS-Security (see [4])

The prime goal of this OASIS specification is to enable secure exchange of XML messages using the SOAP (see [5]) protocol between communication end-points. It provides support implementing message integrity and confidentiality as well as client (user) authentication. This can be obtained by applying XML Digital Signature (see [6]) and XML Encryption (see [7]) to an XML message in a specific fashion. This standard describes the processing rules in order to create message integrity or confidentiality. It also describes the structure of SOAP messages and the structure or relevant metadata so that they can be processed (by web services) in an interoperable way.

This standard also supports different security tokens to obtain client authentication. It defines processing rules of how to attach security tokens to messages. These security tokens are currently supported:

- “Username” token provides support to share knowledge about the identity of a user. “Password” expresses the password associated with this token. In addition, “Nonce” and “Created” are supported to enable strong digested passwords.
- “X.509” token supports exchange and use of X.509 certificates for the matter of authentication, digital signatures and encryption.
- “SAML” include SAML assertions as a token.
- “Kerberos” token allows to the use of Kerberos tickets.

- "REL" token can be used to attach license information.

8.1.4 Standards associated to Message Content Security

This section of the document provides an overview of standards and recommendations and other literature related for establishing message content security.

XML Digital Signature (see [6])

This W3C Recommendation specifies the processing rules how to apply digital signatures to any type of information; in particular XML structures information and represent the result as well as the relevant metadata in XML. It supports different kinds of digital signatures:

- "Enveloped" signatures are processed over the content that includes the digital signature element itself.
- "Enveloping" signatures are processed over content that is part of the signature element.
- "Detached" signatures are processed over content that is external to the signature element.

XML Encryption (see [7])

This W3C Recommendation specifies the processing rules how to encrypt information and represent the result as well as relevant metadata in XML. It also defines processing rules for the associated decryption. The following types of encryption are supported:

- "Element Encryption" allows encrypting the embracing element and its name.
- "Element Content Encryption" allows encrypting the value of an XML element which leaves the embracing element name in clear text.
- "Any Data Encryption" allows encrypting entire documents.
- "Super-Encryption" supports to encrypt already encrypted data.

XKMS (see [8])

The XML Key Management Specification is a W3C Note comprises of two sections specifying a XML Key Information Service (X-KISS) and a XML Key Registration Service (X-KRSS) as well as the associated protocols for the distribution and registration of public keys that can be used in conjunction with the W3C Recommendations XML Digital Signature and XML Encryption.

- The Key Information Service Specification describes the protocols that allow an application delegating the processing of XML Digital Signatures (or parts of it) to a trusted service. The application hereby gains simplicity and performance issues concentrate on the trusted service.
- The Key Registration Service Specification describes the protocol to register (and revoke) public keys with a trusted service. The associated private key can be generated

by the service or the client. This requires in the first case assertions by the client toward the proof of possession and in the latter case protocol mechanisms for securely sending the private key to the client. In order to allow a meaningful use of public keys and support for cryptographic verification, the client can request that the service registers particular information with a public key.

8.2 Standards for Authentication

This section of the document provides an overview of standards, recommendations and other literature related to authentication and identity management.

X.509 (see [13])

A X.509 certificate is an information bundle where an identity is bound to a public key. The format of the identity can be a X.500 name, an email address or a DNS entry. The information bundle is digitally signed by the CA which guarantees tamper resistance and authenticity. Today, version 3 of X.509 (x.509v3) is been used that allows the use of extension attributes that can be defined as necessary.

X.509 certificates are used to establish HTTPS communications, typically between a web browser and a web server. They are also been used for signing emails, electronic documents such as PDF files or XML formatted messages that are sent by web services.

Because X.509 certificates are based on asymmetric encryption, a private key is associated to the public key. In order to create confidential documents and emails, a X.509 certificate can also been used.

PKI (see [13])

Public Key Infrastructure (PKI) as described in ITU-T standard provides the means by which public keys can be bind to identities in such a way that identification is possible without prior authentication. It also describes management procedures that guarantee that identities are unique throughout the Internet. This can be ensured creating a unique root certificate for each CA and each CA ensures that all maintained identities are unique throughout the CA.

So in a PKI, proof of identity is realized by use of X.509 certificates that are released by CAs. It is therefore essential that a trust relationship with the CA (from which the X.509 certificate is released) is established. This can be set up by accepting (or installing) the X.509 (root) cer-

tificate of the CA. With all standard a web browsers, root certificates of all common CAs are pre-installed so that the user does not have to do that.

Beside the management of identities through a certain number of trusted CAs, PKI describes also the means of revocation for X.509 certificates. Each CA maintains a so called Certificate Revocation List (CRL) that contains the (permanently) revoked certificates. Even each certificate has a pre-defined lifecycle that is set by creation, it can perhaps be necessary that the certificate – so the assurance of the CA that a certain identity is bound to the certificate – expires prior to the pre-defined lifecycle. Reasons for revocation are given in the IETF RFC 3280 (see [14]). One reason is that the private key that is associated to the identity has been tampered. Another reason is that a certificate was released for a fraud identity. One well known example was the certificate that was issued to the fraud identity "Microsoft Incorporation".

Kerberos (see [15])

Kerberos is a Computer Network Authentication Protocol that was developed by the Massachusetts Institute of Technology (MIT) that allows proving of identities between communication partners to each other using a non-secure network. Therefore, Kerberos provides mutual authentication so that the user and the server can verify each other's identity. The protocol protects against eavesdropping (wiretapping) and replay attacks. Today, Kerberos is mainly used for authentication in Microsoft Windows Systems.

Technically, authentication is based on so called Kerberos Tickets. After a successful login at the Authentication Server (AS) using a long term shared secret such as a username / password, the client receives a ticket from the AS. This AS-ticket can then be used to obtain shorter lifecycle tickets to be used with other servers.

LDAP (see [16])

The Lightweight Directory Access Protocol (LDAP) is a protocol for querying and modifying entries of a Directory Service (DS). A DS is a computer program that stores information (typically structured using X.500) about users and computers in a network. Each entry has a unique identifier, called the distinguished name (dn). Each entry can have additional attributes that have a name and a value that – as a whole – define the characteristics of the entry. The stored information is used by administrators to assign roles or access permissions to resources. In an Attribute Based Access Control (ABAC) System, the attributes and their values can be used to derive the authorization decision. In such systems, it is vital to keep the X.500 structure backward compatible.

The LDAP can be used by other authentication protocols to query/exchange identity information.

XCBF (see [17])

The XML Common Biometric Format (XCBF) is an OASIS standard that defines cryptographic messages, based on a common set of XML encodings for the Common Biometric Exchange File Format (CBEFF) that allow the secure collection, distribution and processing of biometric information for the purpose of authentication. In particular, it allows the verification of identity based on human characteristics such as DNA, fingerprints, iris scans and hand geometry.

SAML (see [9])

The Security Assertion Markup Language is an OASIS standard that specifies the structure, the exchange and the processing of assertions about the identity of a subject. An assertion is a structured package of information using the XML notation that is prepared and issued by a so called asserting party and consumed by a so called relying party. Constraints are specified by this standard that allows expressing the restrictions by the asserting party to guarantee appropriate consumption of assertions by the relying party. Also, assertions can be digitally signed to ensure integrity and authenticity. Also, encryption can be applied to make assertions or parts of it confidential. In addition, extension points are defined that allows the extension of assertion to meet project specific needs. Three types of assertions are specified by the standard supporting different use cases at the relying party:

- "Authentication Assertion" provides information about the asserted subject toward the means by which a subject was authenticated, by whom and at what time.
- "Attribute Assertion" provides information about the characteristics of the asserted subject.
- "Authorization Assertion" states that access to a particular resource is to be permitted/denied for the asserted subject.

In regard to exchange (request and response) assertions between the asserting and relying party, this standard specifies the following protocols (relevant excerpt) and the appropriate sequence of messages:

- "Assertion Query and Request Protocol" defines the processing rules of how existing assertions can be queried and the structure of the messages.
- "Authentication Request Protocol" enables the relying party to request assertion statements about the means by which a subject was authenticated.
- "Artifact Resolution Protocol" defines how SAML artefact references can be exchanged instead of the assertions itself.
- "Name Identifier Management Protocol" defines how an asserting party can change the name of an identifier that was previously established and is been used by relying parties.

- "Single Logout Protocol" defines a sequence of message exchange with the goal to terminate all existing sessions of the subject with other relying parties close to real time. However, there is no confirmation message because the logout with all relying parties cannot be guaranteed.
- "Name Identifier Mapping Protocol" defines an exchange of identifier names that can be used to establish identity federations.

An extension to the SAML standard (see [10]) defines the following bindings (relevant excerpt) that define an association of SAML protocol messages to the underlying communication/message protocols for a particular architecture:

- "SAML SOAP Binding" defines how SAML assertions are to be exchanged using SOAP messages and how SOAP header elements are to be used to do so.
- "Reverse SOAP (PAOS) Binding" describes a mechanism where the client is able to act as a SOAP responder or intermediary relevant for implementing the "Enhanced Client or Proxy (ECP) Profile".
- "HTTP Redirect Binding" enables the exchange of SAML messages as URL parameters. In order to ensure the length limit of a URL is not exceeded, message encryption is used. This binding is relevant, where HTTP user agents of restricted capabilities are involved in the message exchange.
- "HTTP POST Binding" defines how SAML messages can be send inside a HTML form using base64 encoding.
- "HTTP Artifact Binding" defines how SAML request and response messages are exchanged using a reference – an artefact. This binding is essential for implementing the "Artifact Resolution Profile".

An extension to the SAML standard (see [11]) defines the following profiles (relevant excerpt):

- "Web Browser SSO Profile" defines how a Single-Sign-On can be established using a (regular) web browser as the client.
- "Single Logout Profile" defines the sequence of messages relevant to ensure that a user is logged out at all participating services.
- "Enhanced Client or Proxy (ECP) Profile" defines the exchange of request/response messages for a client that knows which asserting party to contact and knowing that it supports PAOS Binding.
- "Identity Provider Discovery Profile" defines mechanisms by which a relying party can discover, which asserting parties a principal uses for the "Web Browser SSO profile".
- "Name Identifier Management Profile" defines mechanisms that can be used by the asserting/relying party to associate a different name to a principal.
- "Artefact Resolution Profile" defines a mechanism where client or client interface restrictions exist that prevents the direct exchange of SAML assertions. A SAML artefact a unique (one-time) reference in the Internet, issued by the asserting party that points to a particular assertion stored at the asserting party that can be requested by the relying party.
- "Assertion Query/Request Profile" defines the basic mechanisms to query/request assertions using synchronous communication.

- "SAML Attribute Profiles" defines a unique naming for SAML attributes of "build-in" types such as X.500/LDAP, UUID, DCE PAC and XACML.

8.3 Standards for Authorization (Attribute Based Access Control)

This section of the document provides an overview of standards, recommendations and other literature related to ABAC.

XACML (see [18], [19], [20], [21])

The eXtensible Access Control Markup Language (XACML) as specified in the OASIS standard describes a multi-purpose Policy Language that allows the declaration of access rights in XML. It further defines the process of interpreting Policies in order to derive an authorization decision. In addition, it describes structures of request/response messages in XML that allows requesting an authorization decision from a Policy Decision Point (PDP) as it is useful in a Service Oriented Architecture.

Different profiles to XACML exist that define specific use of XACML. The following is an excerpt of important profiles:

- "RBAC Profile" (see [19]) defines how to declare XACML based access rights based on the Role Based Access Control (RBAC) Model. This profile supports RBAC0 (core RBAC) and RBAC1 (hierarchical RBAC). There is no support for RBAC2 (constraint RBAC).
- "SAML Profile" (see [20]) defines extensions to SAML so that XACML specific information can be securely exchanged. The following different extensions are defined:
    - "AttributeQuery" can be used for requesting one or more attributes from an Attribute Authority.
    - "AttributeStatement" defines a standard SAML statement that contains one or more attributes. This statement may be used in a SAML Response from an Attribute Authority, or it may be used in a SAML Assertion as a format for storing attributes in an Attribute Repository.
    - "XACMLPolicyQuery" can be used for requesting one or more policies from a Policy Administration Point (PAP).
    - "XACMLPolicyStatement" defines a SAML statement extension that can be used in a SAML response from a PAP.
    - "XACMLAuthzDecisionQuery" defines a SAML request extension that can be used by a PEP to request an authorization decision from an XACML PDP. This is an alternative to the XACMLAuthorizationDecisionRequest defined in XACML.
    - "XACMLAuthzDecisionStatement" defines a SAML statement extension that can be used in a SAML response from an XACML PDP. This is an alternative to the XACMLAuthorizationDecisionResponse defined in XACML.
- "DSIG Profile" (see [21]) defines a recommendation to exchange authorization decision request and responses based on the SAML Profile for XACML that supports applying digital signatures for the purpose of authentication and establishing message

integrity. This is a relevant profile as XACML itself does not support to apply digital signatures to the XACML native authorization decision request and response messages.

GeoXACML (see [22], [23], [24])

The Geospatial eXtensible Access Control Markup Language (GeoXACML) is a standard by the Open Geospatial Consortium Inc. (OGC) that defines a geo-specific extension to XACML v2.0. It extends the XACML Policy Language by the new data type "Geometry" and several geo-specific functions that allow the declaration and enforcement of access rights that can be associated to geometric characteristics of the resource. The two extensions (see [23] and [24]) define particular XML encodings of a XACML AttributeValue element of type Geometry, based on the Geography Markup Language (GML). In particular, GeoXACML extension A provides support for GML2 and extension B provides support for GML3 formatted geometries.

8.4 Standards for Licensing

This section of the document provides an overview of standards, recommendations and other literature related to Licensing/Digital Rights Management.

XrML (see [25])

The eXtensible Rights Markup Language (XrML) is a proprietary XML dialect to express rights over digital content which is been used by Microsoft. It is not a standard and owned by ContentGuard (founded by Microsoft and Xerox) which holds related US patens. XrML version 1.0 is the successor of DPRL (Digital Property Rights Language) developed at Xerox PARC that defines computer work specific rights such as "copy", "backup", etc. Version 2.0 developed by ContentGuard was developed to be medium independent. Version 2.1 of XrML was standardized by ISO as Part 5 of the MPEG-21 standards suite (see next topic).

REL (Mpeg REL) (see [26])

The Rights Expressions Language as specified in ISO/IEC 21000-5 (see [26]) defines an XML dialect to express usage rights through tamper resistant enforceable licenses for moving pictures (MPEG) files. In order to protect the owners' assets, a Digital Rights Management System is required of which REL is one key component.

The kernel part of a license is the Rights Expression that grants defined usage rights to a particular consumer (user). Because the rights of a license are typically enforced on the user's

computer the content owner relies on the tamper resistance of the license and of the component that interprets the licensed rights. Assuming a tamper resistant license, the meaning of the granted rights must be shared by the creator of the license (typically the content owner) and the software developer of the (MPEG) player. To ensure this, it is vital to standardize a certain set of rights and their semantics (e.g. play, print) as it is done by this standard.

ODRL (see [27])

The Open Digital Rights Language (ODRL) Version 1.1 is a W3C Note that specifies an Expression Language and the representation in XML. It further defines the semantics of core expressions.

The core entities of the ODRL Language are Assets, Rights and Parties. An Asset represents the content that is to be protected either in physical or digital form. Rights include Permissions that are the actual usage that are allowed on the asset. The Parties represent the end user (consumer) and the Rights holders that typically have been involved in the creation of the content or own it.

The standard defines in the ODRL Data Dictionary Semantics section a set of core rights and their semantics for Permissions, Constraints, Requirements, Rights Holders and Context. This standard also provides extension points for the definition of project specific of data dictionary elements. One example given in the standard is associated to the mobile community, where rights such as “ring” or “send” are relevant.

8.5 Standards for Web Services

This section of the document provides an overview of standards, recommendations and other literature related to securing Web Services.

SOAP (see [28])

The Simple Object Access Protocol (SOAP) provides the foundation of communication for web services. SOAP defines a particular XML structure that separates the information of a message into a “Header” and a “Body” part. The “Body” part of the message contains the actual information that is to be transported and the “Header” element can keep optional (security related) metadata as it relevant to protect the “Body” information as a whole or partially.

SOAP supports multiple bindings, where the HTTP (and HTTPS) binding is the must common one. It enables the communication between sites using the "standard" WWW port to pass through a firewall.

Based on SOAP, WS-Security defines mechanisms and XML structures how to protect SOAP messages in an interoperable way (so that it can be understand by the receiver) toward integrity and confidentiality using XML Digital Signatures and XML Encryption.

For some use cases, the input and/or output of a web service might be in binary format instead of XML. For these cases, a base64 encoding of the binary data can be transported in the SOAP Body. However this is possible, the base64 encoding increases the size of the information and XML parsing or digital signatures and encryption face a decrease in performance. In order to exchange binary data via SOAP, SOAP with attachments can be used.

WSDL (see [29])

In order to bind to a web services, its network end points (operations and binding) and the (SOAP) structure of input and output message can be described using the Web Services Description Language (WSDL). More precise, WSDL is a W3C note that defines a model and the XML notation to describe web services to support ease of use by the following elements:

- The "types" element describes the messages that can be received and send by the web service
- The "interface" element contains information about the functionality of the web service
- The "binding" element has the information of how to access the web service
- The "service" element provides the actual network endpoint where the web service can be accessed

WSDL 2.0 supports a full HTTP binding including GET / POST (/ DELETE / PUT / etc.) and SOAP.

WS-Addressing (see [30])

Web Services Addressing is a W3C Recommendation that supersedes the WS-Referral & WS-Routing initiatives by Microsoft. It specifies a transport neutral mechanism to communicate addressing information for messages and service endpoint references. Using SOAP and HTTP(/HTTPS) the sender relies on TCP/IP to route the message to the right receiver. Once

delivered, the receiver uses information from the SOAP message itself to figure out what to do with the message. WS-Addressing allows to disconnect this relationship by inserting WS-Addressing metadata information (structured in XML) into the SOAP Header. Looking at it from a security point of view, this enables communication partners to securely exchange synchronous but more important asynchronous (unsolicited) messages. In order to ensure a trusted processing, XML Digital Signature can be applied to make WS-Addressing metadata tamper resistant and authentic.

In "Web Services Policy Attachment for Endpoint Reference (WS-PAEPR)" (see [31]) is described, how to use WS-Policy (see [32]) Information into the Endpoint Reference provided by WS-Addressing. This enables to express service security requirements that ought to be met in order to access (execute) the referenced service.

WS-Policy: (see [32])

Web Services Policy is W3C Recommendation that allows to describe and advertise policies of a web service in XML. A policy can express requirements toward Quality of Service characteristics, privacy considerations, security constraints, etc.

From the standpoint of security, WS-Policy describes the capabilities and constraints of the security policies on intermediary services and end point services such as required security tokens, supported encryption algorithms, etc. WS-Policy also defines how to associate policies with web services. In addition, WS-Policy defines operators to combine and intersect policies.

WS-Policy Attachment (see [33])

Web-Services Policy Attachment is a W3C Recommendation that is based on WS-Policy. It specifies how to derive the effective policy for subjects from "scattered" policies by merging all relevant parts. This is important as constraints can be expressed at different levels (web service, operation, message, communication channel, environment, authorization, cryptographic algorithms, tokens, etc.) that must be taken under consideration at the moment when authorization is enforced.

In addition, this recommendation specifies two general-purpose mechanisms for associating policies to different versions of WSDL and UDDI. Universal Description, Discovery and Inte-

gration (UDDU) defines a registry service for publishing, searching and obtaining WSDL documents.

The specified model for attaching WS-Policies to WSDL includes how to partition a WSDL construct into “service”, “endpoint”, “operation” and “message” policy subjects and the semantics for attaching a policy to each policy subject. It further defines how to combine policies for a single policy subject that is attached to multiple WSDL components.

The defined mechanisms for associating policies to policy subjects through the use of UDDI involve two possibilities: Policies can be made available via direct (remote) reference or as tModels registered within UDDI. Independent from the approach, this recommendation defines how to calculate the effective policy.

WS-SecurityPolicy (see [34])

Web Services SecurityPolicy is an OASIS standard that defines a framework that allows to express web services security related constraints and requirements to be used in conjunction with WS-Policy.

In order to support that, WS-SecurityPolicy defines initial sets of assertions that are used by the service to express to the client how messages can be secured. The intent is to be flexible on the one hand side in terms of tokens and cryptographic algorithms but still been expressive to ensure interoperability toward assertion matching between communication partners. Deriving the applicable policy out of a set of possible alternatives is based on the WS-Policy intersection mechanism and first-level, QName matching.

WS-SecurityPolicy supports the following types of assertions:

- “Protection assertions” define the parts of a message that are to be protected.
- “Conditional assertions” define preconditions of security such as which tokens can be used for integrity or confidentiality or which cryptographic algorithms can be used.
- “Security binding assertions” define how Conditional assertions are to be used to protect messages parts as declared using Protection assertions.
- “Supporting token assertions” define the types of tokens that can be used to secure individual operations of the service or messages.
- “Web Services Security and Trust assertions” define token referencing and additional trust options.

WS-Trust (see [35])

Web Services Trust is an OASIS standard that defines extensions to WS-Security for managing (issuing, renewing, cancelling, validating) security tokens for the purpose of establishing brokered trust relations between web services of communication partners through the exchange of secured messages. For supporting Brokered Trust this standard introduces the concept of a Security Token Service (STS). In order to use the STS in an interoperable way, XML message formats are defined for the messages to request and respond security tokens as well as negotiation and challenging mechanisms.

It is important to note that this specification does not define any security token types. It just specifies how to deal with them to establish trust between web services of not directly trusted communication partners.

WS-SecureConversation (see [36])

Web Services Secure Conversation is an OASIS standard that defines the concept of a Security Context (Security Context Token), how to establish and/or reference it in order to exchange a sequence of messages within a session instead of single messages, as supported by WS-Security. This standard defines three ways of how to establish a security context:

- Security Context Token (SCT) created by a security token service,
- SCT created by one of the communication parties and propagated with a message and
- SCT created by negotiation.

In addition the standard defines mechanisms for amending, renewing and cancelling an established security context. Because the encryption of the messages exchanged within an established security context is based on shared secrets, this standard also defines how to derive keys as well as the refreshing of keys in order to prevent providing too much encrypted data for analysis.

This standard is designed to be used in conjunction with other WS-* standards, in particular WS-Security and WS-Trust.

8.6 Draft Standards for Web Services

This section gives a short overview of current initiatives and draft standards in the area of security for web services and secure communication.

WS-Reliable Messaging (see [37])

WS-Reliable Messaging is an OASIS Draft that aims at providing modular mechanisms for reliable exchange of messages regardless to network failures. The defined SOAP based messaging protocol provides support to identify, track and manage reliable transfer of messages between a sender and a receiver.

This draft defines an extensible mechanism which use is anticipated with WS-Security standards such as WS-Policy to integrate other security requirements in an interoperable way.

WS-RM Policy (see [38])

Web Service Reliable Messaging Policy defines policy assertions applicable for reliable messaging to be used with WS-Policy and WS-Reliable Messaging.

The Sequence Security Policy assertion (extending WS-SecurityPolicy assertion) of this draft standard enables the destination and the source of a reliable communication to express the security requirements, particularly relevant for a sequence of messages.

WS-MakeConnection (see [39])

Web Services Make Connection is an OASIS Committee Draft that describes a mechanism to deliver a message between two endpoints if the sending end-point cannot establish a connection to the receiving end-point. In order to achieve this, WS-MakeConnection defines a mechanism to uniquely identify non-addressable endpoints. It does this for the SOAP binding.

This committee draft (specification) integrates with WS-Security, WS-Policy and WS-ReliableMessaging that supports the realization of security related aspects. Because the use of WS-Security secures messages by applying asymmetric keys, the performance might become an issue for large messages or high message throughput. WS-MakeConnection allows the use of WS-Trust and WS-SecureConversation to negotiate a shared secret (symmetric key) to encode messages.

WS-Federation / WS-Authorization / WS-Privacy (see [40])

Web Services Federation Language as of version 1.2 is an OASIS Editors Draft that defines mechanisms to protect resources from one security realm to subjects of another security realm. This requires a federation between the two security realms (identity and resource) such that the origin of authentication assertions from the authentication realm can be trusted by the access control realm. WS-Federation builds on WS-Trust to ensure this.

In addition, it is essential to ensure secure exchange of messages between the trusted realms. WS-Federation builds WS-Security to ensure this.

It is important to note that the federation mechanisms defined in this document are not limited to SOAP enabled Web Services; the Web Browser Environment is also supported. This is achieved by providing an HTTP encoding of the WS-Trust messages Request Security Token (RST) and Request Security Token Response (RSTR).

WS-Federation builds on Security Token Services (STSs) to exchange relevant security information. In order to ensure interoperability to an Authentication Service, this document defines a common profile of the STS as defined in WS-Trust. In addition, this document defines additional XML elements to become part of the RST that allows further specification of the authorization context in which a security token is requested.

Upon requesting a security token it might often be the case that some related information is private to a person or an organization. In order to obtain a security token that contains private information, the requestor can ask the provider to encrypt the private information. In order to express these constraints, this document defines an additional XML element for the RST message.

8.7 Standards for eBusiness

This section of the document provides an overview of standards related to electronic business.

ISO/TS 15000 (see [44], [45], [46], [47], [48])

This multi-part international ISO standard defines the electronic business eXtensible Markup Language (ebXML) that provides support for an interoperable exchange of messages to facilitate global trade. In order to achieve the linking of business processes, each part of the standard defines certain (technical and non-technical) aspects such as Information Transfer, Meaning and Process. The main concern with Information Transfer is the safe and reliable

exchange of information (messages) over the (un-secure) Internet. The Meaning aspect establishes a common (identical) understanding of the exchanged information about the order and/or deliverable. The Process aspect is related to the standardization of sequence of actions concerning messages to be sent and orders to be fulfilled. In addition, ebXML defines the structure of an ebXML registry, where process, messages and data definitions can be stored. In addition the standard defines mechanisms that guarantee inter-registry communication for the purpose of synchronisation.

Part 1 defines the collaboration-protocol profile (ebCPP) that can be used for business transactions between business communication partners. Part 1 also defines the agreement specification (CPA) that can be used as a message exchange agreement between the business partners. The CPA defines the minimum agreement toward message, communication security constraints, that are created by the intersection of the business partners' CPPs. The CPA also contains a binding to a Process Specification document that defines the interactions between the business partners, specific to the actual business collaboration.

Part 2 defines a communications-protocol (ebMS) neutral method for exchanging electronic business messages that ensures the reliable and secure delivery of business messages. In particular the ebXML message structure is defined and the behaviour of the message handling services that are used to send and receive ebXML messages. In order to achieve that, the ebXML SOAP Envelope extension is defined and the Reliable Messaging protocol is leveraged to ensure the once-and-only-once message delivery semantics.

Part 3 defines the registry information model (ebRIM) in which the term "repository item" is used to identify the actual information object that is stored in the registry (e.g. XML document) and the "RegistryEntry" which is used to refer to metadata about a repository item. The information, stored in an ebXML registry can be used to facilitate ebXML-based B2B partnerships or transactions. The Registry Information Model defines what types of objects are stored in the registry and how the stored objects are organized in the registry. It acts as a blue print for implementers to decide which types to include into the registry and which attributes and methods the actual objects might need. The actual Registry Information Model is provided as UML diagrams, in which different classes and their association are introduced: RegistryObject, Slot, Association, ExternalIdentifer, ExternalLink, ClassificationScheme, ClassificationNode, Classification, RegistryPackage, AuditableEvent, User, PostAddress, EmailAddress, Organization, Service, ServiceBinding and SpecificationLink.

Part 4 defines how to build ebXML registry services (ebRS) to provide access to the information stored in an ebXML registry. It therefore defines interfaces for the registry service, the interaction protocol and message structures.

8.8 ISO Standard for Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC)

This section of the document provides an overview of standards related to the security evaluation, abbreviated Common Criteria.

ISO/IEC 15408 (see [49], [50], [51])

This multi-part international ISO Standard defines what is well known as Common Criteria for Information Technology Security Evaluation (CC).

Based on this standard it is possible to compare the results of independent security evaluations for products such as operating systems, computer networks, distributed systems and applications. It supports that by providing a common set of requirements for security functions for a product to be certified and for applied assurance measures. The result of the security evaluation undertaken by competent and independent licensed laboratories that document how much the security requirements of a product meet the requirements might provide a help to the customer for evaluating if a product is suitable. CC knows seven assurance levels:

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

In other words, ISO/IEC 15408 provides the capabilities for customers to specify certain security requirements, product (soft- and hardware) vendors can claim certain to have implemented those requirements and independent certification bodies can conduct tests on the product to actually proof the claim(s). A list of certified products according to the Common Criteria is available at *http://www.commoncriteriaportal.org*. For example, the “Interactive Link Data Diode Device” from Tenix Pty Limited, Sydney, Australia is the only product with the assurance level EAL7. It is used to separate high and low classified networks ensuring a secure unidirectional data flow to the high classified network only.

In particular, ISO/IEC 15408 can be applied to certify that products are not vulnerable to human or system initiated actions that cause the unwanted disclosure, (unnoticed) modification or loss of information processed or stored by a certified product. Therefore, this standard allows to certify that information confidentiality, integrity and availability is ensured.

This ISO International Standard is presented as three parts:

Part 1 (Introduction and general model) provides the introduction to ISO/IEC 15408, defines general concepts and principals for IT security evaluation and a general model for evaluation.

Part 2 (Security functional requirements) "defines the required structure and content of security functional components for the purpose of security evaluation" [50]. It also includes "a catalogue of functional components that will meet the common security functionality requirements of many IT products and systems" [50].

Part 3 (Security assurance requirements) defines the evaluation assurance levels and defines a scale for measuring assurance. It also contains the criteria for evaluation of assurance of Protection Profiles and Security Targets as specified in Part 2. For example, it defines assurance through evaluation by different techniques such as "verification of proofs" or "penetration testing". In addition, it defines assurance scales to state the minimal effort required to reach a particular assurance scale.

8.9 Standards for Security Techniques

This section of the document provides an overview of standards related to the security assurance.

ISO/IEC 15443 (see [52], [53], [54])

This international multi-part ISO Standard categorizes security assurance methods to a generic lifecycle model in order to gain high level of confidence when certifying security functionality of a deliverable. A deliverable in the context of this standard can be related but is broader than the definition of a TOE as defined in ISO/IEC 15408. Part 1 of this standard provides general definitions, an overview and a framework for assurance methods. Part 2 defines different assurance methods. Part 3 analyses different assurance methods and their applicability to the lifecycle: Concept/Specification, Design/Development, Integration, Deployment and Operation.

Part 1 defines three categories of assurance methods for the assessment of the deliverable, the process used to develop the deliverable and the environment such as personnel and facilities. It is stated that the selection of the right assurance method can be different for the same deliverable if the environment changes and that specific assurance methods can only be applied to certain time periods of the lifecycle.

Part 2 defines different security evaluation criteria for different markets and a visualization how it is to be used and to which timeframe of the lifecycle it applies to. For example, chapter 6.12 defines the "ITSEC/ITSEM Evaluation Criteria and Methodology for the European market". Its visualization is =>D=>, =>I=> and =>O=> meaning that it is applicable to Product/System/Service Design/Implementation, Integration/Verification and Operation.

Part 3 defines (as one most important aspect) which assurance approach will provide the most reliable results fitting the needs of the Assurance Authority. It therefore illustrates the difference between Product vs. Product, Process vs. Environment and Product vs. Environment assurance. It also gives the (relative) value for each Assurance Approach indicating how applicable it is to the context of the Assurance Authority and how to deal with assurance of complex deliverables such as a combination of hard- or software components, security services, environmental aspects or any combination of them.

8.10 Standards for Open Systems Interconnection

This section of the document provides an overview of standards related to the definition of security requirements and concepts.

ISO/IEC 10181 (see [55], [56], [57], [58], [59], [60], [60])

This international multi-part ISO Standard defines security frameworks for Open System environments. It defines that "Open Systems" include Database, Distributed Applications, Open Distributed Processing (ODP) and Open Systems Interconnection (OSI). Security Frameworks are defined in order to provide protection for systems and objects within the systems as well as interactions between systems. The concept of Security Frameworks of this standard is meant as the base for further detailed specification in the other parts.

Part 1 describes the organization of Security Frameworks, defines relevant security concepts and describes relationships of the services of the frameworks. It hereby uses security architecture definitions from ISO/IEC 7498-2 such as access control, availability, denial of service, digital signature and encipherment. It also provides other relevant definitions such as security information, security domain, security policy, trust entities, trust and trusted third parties. For the security information it defines security labels, cryptographic checkvalues, security certificates and security tokens. In addition, it defines denial of service and availability in such a sense that a denial of service cannot always be prevented. In these cases, other security services can be used to detect the lack of availability and allows to apply corrective measures. Annex A of Part 1 provides an example of protection measures for security certificates.

Part 2 of this standard defines all aspects of Authentication in Open Systems and the relationship with other security functions such as access control.

Part 3 of this standard defines all aspects of Access Control in Open Systems as it applies to the interactions of user to processes, user to data, process to process and process to data. It also defines the relationships to other security functionality such as authentication and audit.

Part 4 of this standard refines all aspects of non-repudiation and extends the concepts defined in ISO/IEC 7498-2.

Part 5 of this standard defines confidentiality as a service "to protect information from unauthorized disclosure" in retrieval, transfer or managed.

Part 6 of this standard defines integrity as a property that "data has not been altered or destroyed in an unauthorized manner". This applies to data in retrieval, transfer or management.

Part 7 of this standard defines the basic concepts of, a general model for and identifies relationships between services for security audit and alarms.

In addition, Part 1 defines the key management framework as its functions are applicable to any information technology environment where digital signatures and encipherment is used.

8.11 Other Literature

WS-MDE (see [41])

Web Services Metadata Exchange (WS-MetadataExchange) is a draft specification document that fits into the WS-* standards from OASIS but is not published by OASIS. It defines how service specific metadata that describes the conditions for establishing communication can be requested as a WS-Transfer resource. Therefore, the document defines the structure of a GetMetadata and Metadata element that can be inserted in a regular SOAP message. In addition, this document provides several mechanisms to aid service endpoints and requestors in bootstrapping communication, issuing a HTTP/GET request. The document strongly rec-

ommends the use of WS-Security to secure messages so that the exchanged metadata can be relied on.

WS-Transfer (see [42])

Web Services Transfer (WS-Transfer) is a W3C member submission that defines a SOAP based mechanism for acquiring, creating and deleting XML-based representations of entities using a web services infrastructure. More specific, it defines operations to Get, Put, Create and Delete representations of resources. Therefore, the document defines “Resources” that are addressable entities providing an XML representation and “Resource Factories” are web services that can create a new resource from an XML-based description.

WS-RT (see [43])

Web Services Resource Transfer (WS-RT) is a draft specification document that fits into the WS-* standards from OASIS but is not published by OASIS. It specifically defines extensions to WS-Transfer that allows to operate on fragments of resource representations using the WS-Transfer operations Get, Put, Create and Delete. In order to achieve that, it defines the QName and XPath Expression Dialect.

Literature for the annex

[1] **IPSec:** IP Security – IETF RFC 4301 (2005) (soboletes RFC 2401 from1998): *http://tools.ietf.org/html/rfc4301*

[2] **TLS:** Transport Layer Security – IETF RFC 2246 (1999): *http://tools.ietf.org/html/rfc2246*

[3] HTTP/HTTPS

[4] **Web Services Security**: SOAP Message Security 1.1 (WS-Security 2004) – OASIS Standard Specification, 1 February 2006: *http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf*

[5] SOAP

[6] **XML Digital Signature:** XML-Signature Syntax and Processing – W3C Recommendation 12 February 2002: *http://www.w3.org/TR/xmldsig-core/*

[7] **XML Encryption**: XML Encryption Syntax and Processing – W3C Recommendation 10 December 2002: *http://www.w3.org/TR/xmlenc-core/*

[8] **XKMS**: XML Key Management Specification (XKMS) – W3C Note 30 March 2001: *http://www.w3.org/TR/xkms/*

[9] **SAML**: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005: *http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf*

[10] **SAML-**Bindings: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005: *http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf*

[11] **SAML-**Profiles: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005: *http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf*

[12] **HTTPS:** HTTP Over TLS – IETF RFC 2818 (2000): *http://tools.ietf.org/html/rfc2818*

[13] **X.509 / PKI**: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T Standard, 08/2005: *http://www.ietf.org/html.charters/pkix-charter.html*

[14] **CRL:** Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – IETF RFC 3280: *http://tools.ietf.org/html/rfc3280*

[15] **Kerberos:** The Kerberos Network Authentication Service (V5) – IETF RFC 4120 (2005) obsoletes 1510 (1993): *http://tools.ietf.org/html/rfc4120*

[16] **LDAP:** Lightweight Directory Access Protocol (LDAP): The Protocol – IETF RFC 4511 (2006): *http://tools.ietf.org/html/rfc4511*

[17] **XCBF**: XML Common Biometric Format, OASIS Standard, August 2003: *http://www.oasis-open.org/committees/download.php/3353/oasis-200305-xcbf-specification-1.1.doc*

[18] **XACML:** eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS Standard, 1 Feb 2005: *http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf*

[19] **XACML RBAC Profile:** Core and hierarchical role based access control (RBAC) profile of XACML v2.0, OASIS Standard, 1 February 2005: *http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf*

[20] **XACML SAML Profile**: SAML 2.0 profile of XACML v2.0, OASIS Standard, 1 February 2005: *http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-saml-profile-spec-os.pdf*

[21] **XACML DSIG Profile**: XML Digital Signature profile of XACML v2.0, OASIS Standard, 1 February 2005: *http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-dsig-profile-spec-os.pdf*

[22] **GeoXACML:** Geospatial eXtensible Access Control Markup Language (GeoXACML) v1.0, Open Geospatial Consortium, Inc., 2008/02/20: *http://portal.opengeospatial.org/files/?artifact_id=25218*

[23] **GeoXACML Extension A:** Geospatial eXtensible Access Control Markup Language (GeoXACML) Extension A – GML2 Encoding Version 1.0: *http://portal.opengeospatial.org/files/?artifact_id=25219*

[24] **GeoXACML Extension B**: Geospatial eXtensible Access Control Markup Language (GeoXACML) Extension B – GML3 Encoding Version 1.0: *http://portal.opengeospatial.org/files/?artifact_id=25220*

[25] **XrML:** XrML - eXtensible rights Markup Language, ContentGuard: *http://www.xrml.org/*

[26] **REL**: Information technology -- Multimedia framework (MPEG-21) -- Part 5: Rights Expression Language, ISO/IEC 21000-5:2004: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36095*

[27] **ODRL**: Open Digital Rights Language (ODRL) Version 1.1, W3C Note, 19 September 2002: *http://www.w3.org/TR/odrl/*

[28] **SOAP**: Simple Object Access Protocol (SOAP), W3C Recommendation (Second Edition) 27 April 2007: *http://www.w3.org/TR/soap/*

[29] **WSDL**: Web Services Description Language (WSDL) 1.1, W3C Note 15 March 2001: *http://www.w3.org/TR/wsdl*

[30] **WS-Addressing:** Web Services Addressing 1.0 – Core W3C Recommendation 9 May 2006: *http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/*
(This Recommendation supersedes WS-Routing and WS-Referral as proposed by Microsoft in 2001)

[31] **WS-PAEPR**: Web Services Policy Attachment for Endpoint Reference (WS-PAEPR), W3C Member Submission 20 July 2007: *http://www.w3.org/Submission/WS-PAEPR/*

[32] **WS-Policy**: Web Services Policy 1.5 – Framework, W3C Recommendation 04 September 2007: *http://www.w3.org/TR/2007/REC-ws-policy-20070904/*

[33] **WS-Policy Attachment**: Web Services Policy 1.5 – Attachment, W3C Recommendation, 04 September 2007: *http://www.w3.org/TR/ws-policy-attach/*

[34] **WS-SecurityPolicy:** WS-SecurityPolicy 1.2, OASIS Standard, 1 July 2007: *http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf*

[35] **WS-Trust:** WS-Trust 1.3, OASIS Standard, 19 March 2007: *http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf*

[36] **WS-SecureConversation:** WS-SecureConversation 1.3, OASIS Standard, 1 March 2007: *http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.pdf*

[37] **WS-Reliable Messaging:** Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2, Committee Draft, 28 February 2008: *http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.2-spec-cd-01.pdf*

[38] **WS-RM Policy**: Web Services Reliable Messaging Policy Assertion (WS-RM Policy) Version 1.2, Committee Draft, 28 February 2008: *http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-cd-01.pdf*

[39] **WS-MakeConnection:** Web Services Make Connection (WS-MakeConnection) Version 1.1, Committee Draft, 28 February 2008: *http://docs.oasis-open.org/ws-rx/wsmc/200702/wsmc-1.1-spec-cd-01.pdf*

[40] **WS-Federation / WS-Authorization / WS-Privacy:** Web Services Federation Language (WS-Federation) Version 1.2, Editors Draft – 06, May 21, 2008: *http://www.oasis-open.org/committees/download.php/28360/ws-federation-1.2-spec-ed-06.doc*

[41] **WS-MetadataExchange:** Web Services Metadata Exchange (WS-MetadataExchange), Version 1.1, August 2006, Microsoft, IBM, Sun and SAP: *http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf*

[42] **WS-Transfer:** Web Services Transfer (WS-Transfer), W3C Member Submission, 27 September 2006: *http://www.w3.org/Submission/WS-Transfer/*

[43] **WS-RT:** Web Services Resource Transfer (WS-RT), Version 1.0, August 2006: *http://schemas.xmlsoap.org/ws/2006/08/resourceTransfer/WS-ResourceTransfer.pdf*

[44] **ISO/TS 15000-1:** Electronic business eXtensible Markup Language (ebXML) -- Part 1: Collaboration-protocol profile and agreement specification (ebCPP), ISO 2004: *http://www.iso.org/iso/catalogue_detail?csnumber=39972*

[45] **ISO/TS 15000-2**: Electronic business eXtensible Markup Language (ebXML) -- Part 2: Message service specification (ebMS), ISO 2004: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39973*

[46] **ISO/TS 15000-3**: Electronic business eXtensible Markup Language (ebXML) – Part 3: Registry information model specification (ebRIM), ISO 2004: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39974*

[47] **ISO/TS 15000-4**: Electronic business eXtensible Markup Language (ebXML) – Part 4: Registry services specification (ebRS), ISO 2004: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39975*

[48] **ISO/TS 15000-5**: Electronic business eXtensible Markup Language (ebXML) – Part 5: ebXML Core Components Technical Specification, Version 2.01(ebCCTS), ISO 2005: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41022*

[49] **ISO/IEC 15408-1:** Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, ISO 2005: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c040612_ISO_IEC_15408-1_2005(E).zip*

[50] **ISO/IEC 15408-2:** Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements, ISO 2005:
http://standards.iso.org/ittf/PubliclyAvailableStandards/c040613_ISO_IEC_15408-2_2005(E).zip

[51] **ISO/IEC 15408-3:** Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements, ISO 2005:
http://standards.iso.org/ittf/PubliclyAvailableStandards/c040614_ISO_IEC_15408-3_2005(E).zip

[52] **ISO/IEC 15443-1**: Information technology - Security techniques - A framework for IT security assurance - Part 1: Overview and framework, ISO 2005:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39733

[53] **ISO/IEC 15443-2**: Information technology - Security techniques - A framework for IT security assurance - Part 2: Assurance methods, ISO 2005:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39271

[54] **ISO/IEC 15443-3**: Information technology - Security techniques - A framework for IT security assurance - Part 3: Analysis of assurance methods, ISO 2007:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41693

[55] **ISO/IEC 10181-1:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24404

[56] **ISO/IEC 10181-2:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18198

[57] **ISO/IEC 10181-3:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199

[58] **ISO/IEC 10181-4:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=23615

[59] **ISO/IEC 10181-5:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24329

[60] **ISO/IEC 10181-6:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=24330

[61] **ISO/IEC 10181-7:** Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework, ISO 1996:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18200