ETSI GS INS 004 V1.1.1 (2010-11)

Group Specification

Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems

Disclaimer

This document has been produced and approved by the ETSI Industry Specification Group Identity and Access Management for Networks and Services (ISG INS) and represents the views of those members who participated in this ISG. It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/INS-004

Keywords
access, ID, management, network, service, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Identity and access management for Networks and Services (INS).

1 Scope

The present document will describe a problem statement to federation establishment based on dynamic SLA negotiations, so called "ad hoc federations". Therefore in the first part the basic technologies, Level of Assurance and Metrics, are described, use cases presented and requirements derived. In the second part are the efforts of current SDO's shown.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] SWIFT Deliverable D302: "Specification of General Identity-centric Security Model that supports user control of privacy".

NOTE: Available at: http://www.ist-swift.org/component/option,com_docman/task,doc_download/gid,17/Itemid,37/

[i.2] SWIFT Deliverable 202 Gap Analysis and Architecture Requirements.

NOTE: Available at: http://www.ist-swift.org/component/option,com_docman/task,doc_download/gid,10/Itemid,37/

[i.3] Open Identity Exchange (OIX)®.

NOTE: http://oix.cloudfour.com/

[i.4] Kantara Initiative™.

NOTE: Available at: http://www.kantarainitiative.org/

[i.5] NIST SP 800-63: "Electronic Authentication Guideline".

NOTE: Available at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AH-F	Ad Hoc Federation
API	Application Programming Interface
AuthN	Authentication
HSP	Hot Spot Provider
IAF	Identity Assurance Framwork
IAWG	Identity Assurance Work Group
ICAM	Identity, Credential and Access Management
ICF	Information Card Foundation
Id-FF	Identity Federation Framework
IdP	Identity Provider
IT	Information Technology
LA	Liberty Alliance
LoA	Level of Assurance
NIST	National Institute of Standards and Technology
OAuth	Open Authentication
OIDF	OpenID Foundation
OITF	Open Identity Trust Framework
OIX	Open Identity Exchange
OMB	Office of Management and Budget
OTP	One Time Password
PAN	Personal Area Network
PIN	Personal Identification Number
PN	Personal Network
PN-F	Personal Network Federation
QoS	Quality of Service
SDO	Standards Developing Organization
SIM	Subscriber Identity Module
SP	Service Provider
TFP	trust framework provider
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
XMPP	Extensible Messaging and Presence Protocol

4 Introduction

Due to increasing usage of Internet services the conventional use of bilateral contracts between Service Providers, Network Providers and the Identity Providers is no longer sufficient. Currently the most used and mature standard for federated service usage is the approach of Liberty Alliance / Kantara (LA). LA specified the Identity Federation Framework (Id-FF) which describes the processes for gaining Level of Assurance (LoA). Today there are a lot of new services which are provided by small companies or even by individuals, which cannot afford the time and money to fulfil the processes described in the Id-FF. To provide services and make them billable, techniques are required which give the possibility of ad hoc federation. Such techniques must provide function to evaluate LoA under consideration of reputation, quality of credentials and risk taking as described in D302 [i.1].

In the present document the terms of LoA and Metric are defined in the context of ad hoc federation, use cases introduced and requirements to a solution defined.

4.1 Level of Assurance (LoA)

Whereas there are several standards for LoA depending on the subject, in the context of add-hoc federation and trust management, we refer to the NIST 800-63 [i.5]. Based on the identified risk of the provided IT-systems with respect to authentication, the US Office of Management and Budget (OMB) defined four different levels of identity assurance.

The level of identity assurance describes the degree of certainty that the credentials presented by the end user have been legally acquired. The following four levels have been defined:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

The higher the risk that a resource is exposed, the higher the level of assurance should be.

In order to identify the risks and select the appropriate level of assurance, the OMB defined a 5 step process. This process can be generalized as follows:

- Step 1: Conduct a risk assessment of system.
- Step 2: Map identified risks to the required assurance level.
- Step 3: Select technology based on the NIST e-authentication technical guidance.
- Step 4: After implementation, validate that the information system has operationally achieved the required assurance level.
- Step 5: Periodically reassess the information system to determine technology refresh requirements.

In the context of the present document we assume that the underlying systems and protocols are secure and concentrate on the authentication context of user registration, how the user authenticated to the current session, the reputation of the user and the Identity Provider as depicted in Figure 1.

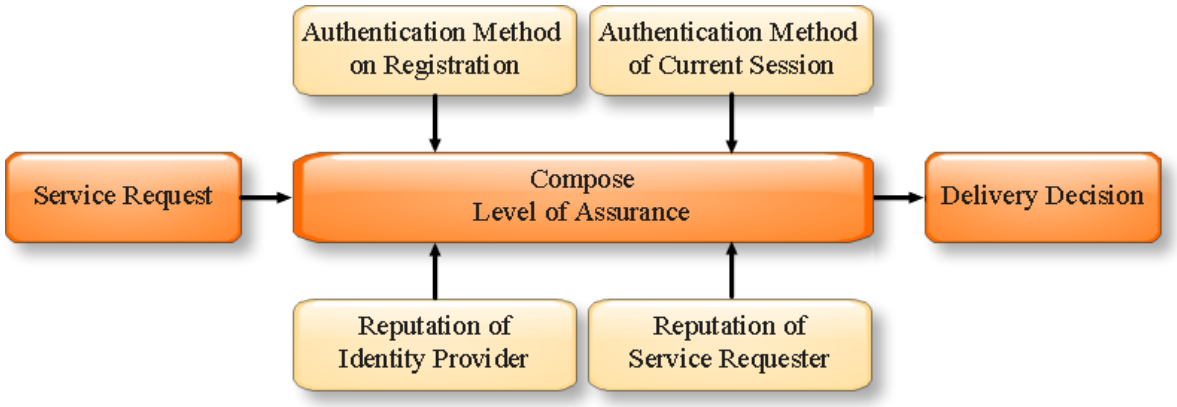

Figure 1: LoA composition

Authentication Method on Registration: this input parameter should indicate which method was used when the user registered to the Identity Provider (IdP), this could be PostIdent, E-Mail verification, etc.

Authentication Method of Current Session: this input parameter should indicate which authentication method was used for the current network / online session, e.g. username/password, username/one time password, SIM-Card, etc.

Reputation of Service Requester: this input parameter should indicate where the user is known by others, e.g. other services, social networks, etc.

Reputation of Identity Provider: at last it is also important which reputation has the IdP of the service requester, who claims to know the user and the aforementioned input parameters are qualified, e.g. a big operator or company the service provider may trust more than an unknown small company.

The service delivery decision depends on the LoA and internal risk taking factors. To qualify these internal factors and to compose the LoA, metrics are necessary so the parameters can be compared and computed.

4.2 Metric

As Tom DeMarco stated, "You can't control what you can't measure" and so it is when a decision for service delivery has to be computed. As shown in Figure 1 there are several influences to the decision making and these influences are in itself multi factored. To measure these factors, adequate metrics has to be developed to quantify and qualify them. This means, through the metric, to define the semantic of the data which are used to compose the LoA. To calculate a factor that indicates a positive delivery decision, the parameters have to be normalised, categorised and compared to the parameters which are needed to describe a particular business model. One solution could be order the parameter through ontology's of each domain, so they can be compared and weighted.

Whatever metric system will be developed it has to be standardised and the definitions shout be available to every buddy involved in the process. Only if there is a common understanding what a factor and the associated value means, e.g. who is the IdP, what age has the user, which cost factors are involved, which authentication method was used, etc. it will be possible to come to a valuable decision.

5 Scenarios and Use Cases

5.1 Scenario 1: Service-bound access

A user is within reach of a hot-spot and wants to access an online flight service. The hot-spot provider (HSP) recognizes that the user is currently not authenticated to the network. Based on the URL the user wants to reach, the HSP tries to contact the flight service and asks if the flight service is willing to pay for the access and if the flight service will pay the HSP grand's access to the user, but only to this requested service. The user checks the flight dates and leaves the hot-spot.

Alternatively the flight service authenticates the user or redirects him to his IdP and provides the service only if the user is properly authenticated and authorized.

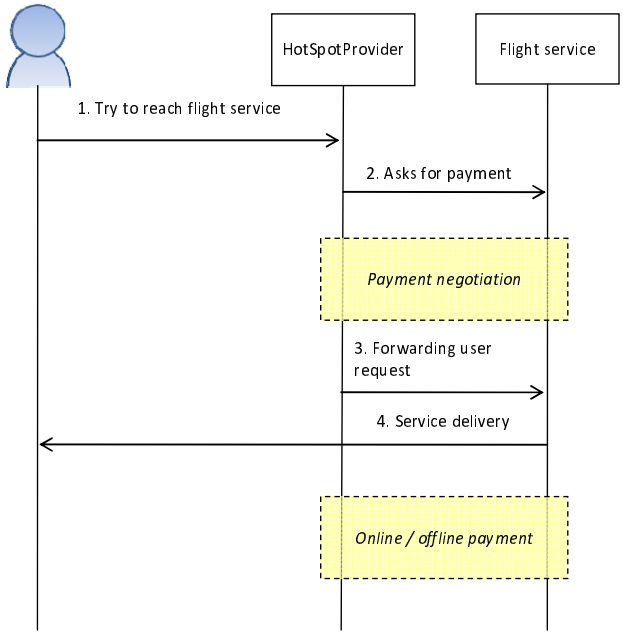

Figure 2: Service-Bound Access simplified

5.2 Scenario 2a: Trust based on reputation

A user wants to download a song from a service provider (SP). The SP asks how the payment will be done. The user decides to use the service anonymous and provides an authentication token from his Identity provider (IdP). The SP checks who issued the token and because it is from a big network operator where the customer is known by PostIdent (confirmation of identity at the post office), he trusts the user. The SP asks the IdP if the token is valid and if the IdP will charge the user for the song. If the IdP agrees, they negotiate a transaction token and the user can download the song. The ISP charges the user and pays the SP.

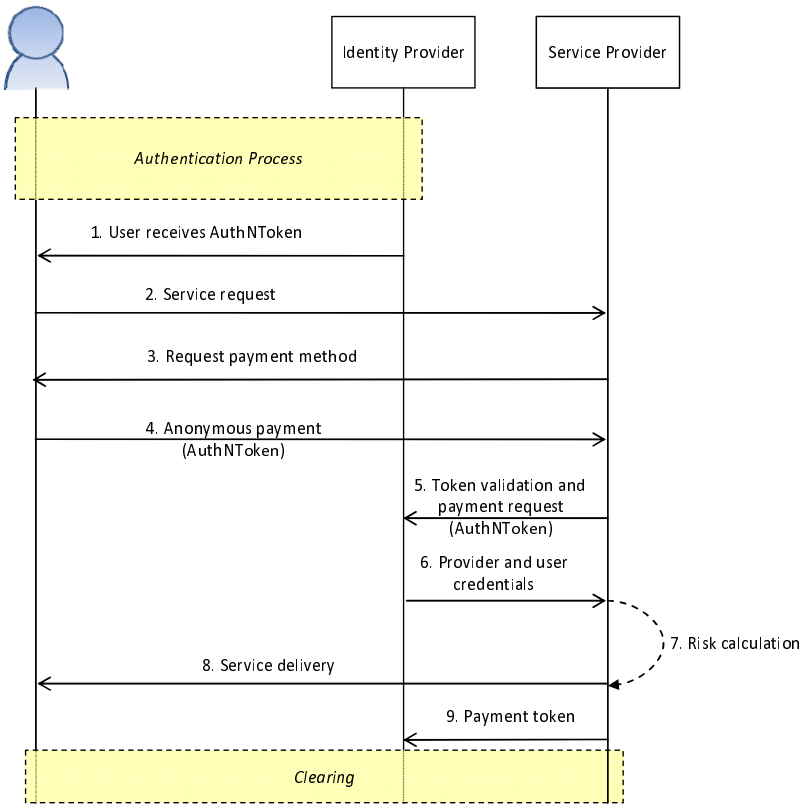

Figure 3: Trust based on reputation

5.3 Scenario 2b: Trust based on reputation

The same scenario like 2a but the IdP is a new provider and is not yet a well known company, so the SP does not know it. In this case we need a transitive trust chain. The SP asks the IdP if the user's token is valid and what IdP can show. The IdP hands out his own received certificate from a trustable party, this can be a Bank or another well known certification institute. The SP verifies the certificate and then delivers the service. The transitive trust chain may influence the risk calculation and therefore the delivery decision.

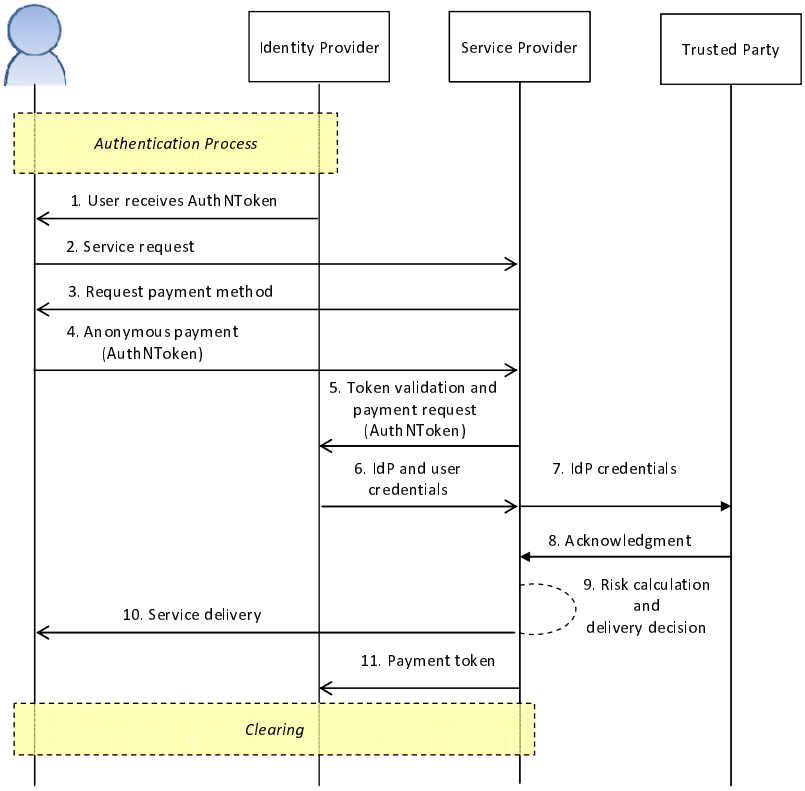

Figure 4

5.4 Scenario 3: Identity Broker - Grid computing

A resource owner offers e.g. data centre resources, contents, or an application to a central Grid-Platform. Before the resources are bound to the platform the resource provider has to identify himself to the identity broker. A resource consumer which wants to use resources from the central Grid-Platform has to identify himself to the identity broker. The identity broker checks the provided credentials and accepts or provides resource by evaluating the credentials, the reputation and the required parameter, e.g. time, pricing, duration, etc.

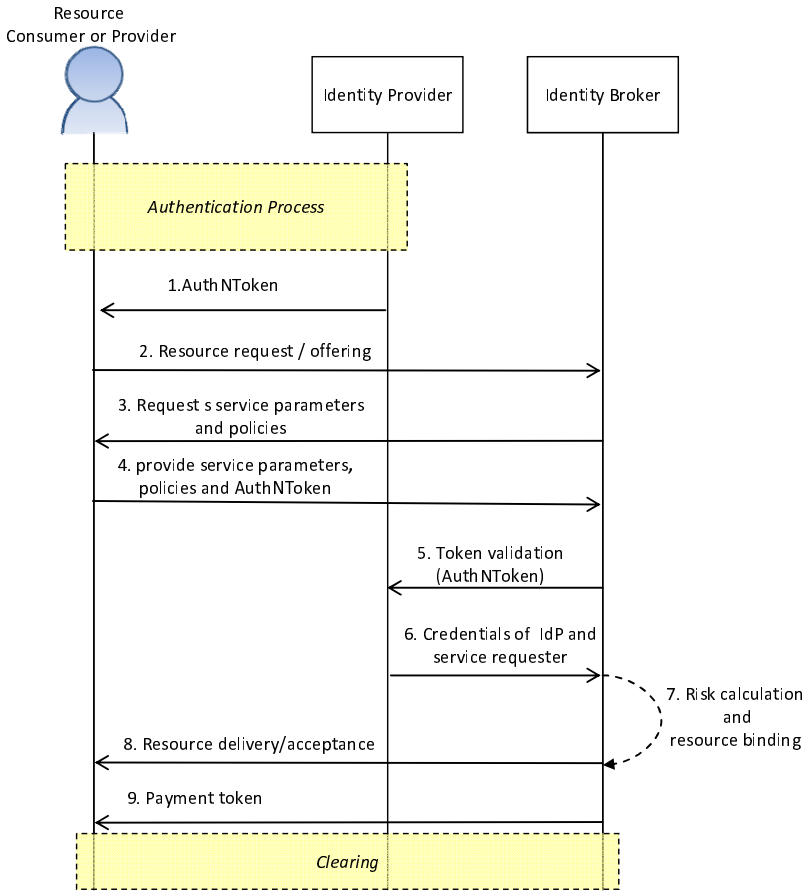

Figure 5

5.5 Scenario 4: Smart Personal Networks

Personal Area Network (PAN) enables local interconnection between various devices of a user (personal devices). A higher challenge is the use of PANs in different geographic locations, such as home, office, car, etc. and to form one secure Personal Network (PN) for the user. Thus the user can freely and safely use all his communicating and computing devices called personal nodes and access personal or public services through them. As such it is a dynamic collection of interconnected heterogeneous personal devices. All these personal nodes may be equipped with one or more communication technologies, such as WPAN, WLAN, UMTS networks, etc. Sooner or later it will be impossible for an individual to manage all the data, networking, functionality and services for so many tools. Smart Personal Networks will be essential.

Basis for Smart Personal Networks is the trust between each involved PAN. The trusted connection between the PANs will be based on different fundaments. On the one hand on well known partner PANs (e.g. infrastructure networks) and otherwise on ad hoc networks which provides services and applications. Especially in the ad hoc case we need clear statements from all the partners to establish a trustful connection and at the end a federation of resources between the PANs. The Personal Network Federation (PN-F) is already described in different sources (e.g. IST MAGNET Beyond).

5.5.1 Scenario Description: Health Monitoring

Monitoring the health condition of a disabled or an elderly person is a potential personal service in a PN, which can collect useful data not only for emergency situations, but also for daily health monitoring and maintenance. Thus a PN incorporates sensing and actuating devices linked to a health-monitoring server at home. Different other PN devices are able to contact the server to use the collected data for specific applications. A medical assistant will establish a wireless connection to the health-monitoring server for analysis processes. The devices of the medical assistant are organised in a PAN based on corporate or public directives.

The medical assistant PAN is authenticated by an IdP and will join the patient PAN in a federation manner to use the health-monitoring server for data access. The patient PAN asks the IdP about the validity of the medical assistant PAN and trusts the decision of the IdP. After the exchange of specific parameters (access rights, rules, time limits, etc.) the ad hoc federation between the two PANs is established.

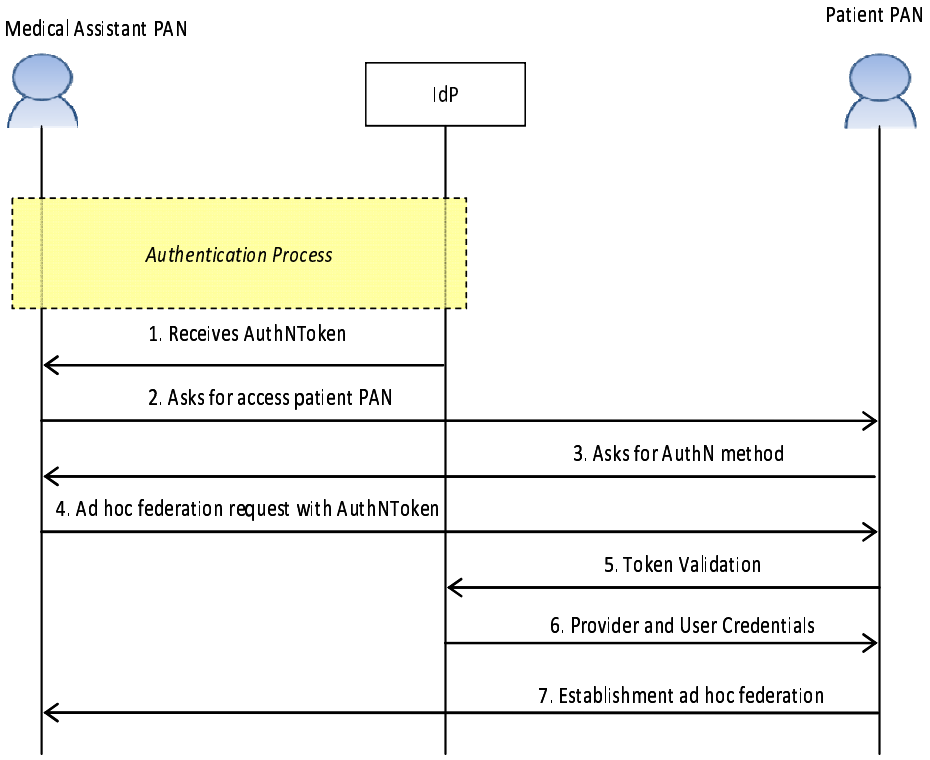

Figure 6: Smart Personal Networks Ad Hoc Federation

6 Requirements

In this clause the previous introduced use cases are analysed and regarding ad hoc federation and trust based on reputation requirements are extracted. Other requirements like "the user has to authenticate himself to his computer" are omitted and can be found in D202 REV [i.2].

Nr.	Use case	Requirement description	LoA / Metric
01	All	Self-organization and maintenance AH-F needs to be self-organized and self-maintained. This required first of all the definition of policies and rules to determine how and when the formation of the federation will take place. Next, the overlay (in term of services or in terms of members) should be formed and maintained without user intervention, making use of naming, routing and mobility management solutions.	
02	All	Application Support Federation members need to specify which resources, applications, services are made accessible to the federation. As such communication is confined in terms of the available resources and data. Profiles will play an important role here.	
03	All	Scalability and QoS AH-F enables a lot of potential application scenarios and addresses a large user base. As a result, the number of federations can become huge and in addition, entities can partake in multiple federations. Therefore solutions are needed that are scalable and that can provide high-quality user experience.	Metric / LoA
04	5.1	The Access Provider must distinguish authenticated and not authenticated users.	LoA
05	5.1	The Access Provider may ask on each non authenticated request the targeted URL if it will pay or may maintain a white /black list.	LoA
06	All	Participating parties must support a set of standard API.	
07	All	A value or token must be used to indicate the required service.	Metric
08	5.1	Access Provider and SP should authenticate each other.	LoA
09	5.1	All participating parties should hold accounting records.	Metric / LoA
10	5.1	The renderer of service must provide accounting and charging information.	LoA
11	5.1	For payment negotiation at least the following parameters are required Currency, amount, time unit, start date time, estimated end date time, online / offline charging, accounting interval.	Metric
12	5.1	The Access Provider must provide service parameters, at least access medium, bandwidth, location.	Metric
13	5.2	The service provider should maintain a blacklist.	LoA
14	5.2	The service provider should maintain a white list.	LoA
15	5.2	The service provider must indicate to the IdP which parameters are required.	Metric / LoA
16	All	The user must control which data are transferred by consent or policy.	Metric / LoA
17	5.3	The trust chain should be transitive.	LoA
18	5.4	An Identity broker has to calculate the risk of accept and to provide resources and map the risks according to the required service parameters.	Metric
19	5.5	Membership management: Ad hoc federation (AH-F) can be seen as a cooperation of different domains, which are members of an AH-F domain, whereby entities of each of the members make resources available. The composition of the members and their resources can change over the time. Therefore, mechanisms to define and initialize new federations and to define, configure, manage and store the membership information of devices are required.	General
20	5.5	Security Security is a major aspect in AH-F as multiple domains are involved and takes place at different levels: access to the AH-F based on membership, secure transport of data within the federation and the access rights to resources and services of the federation.	General

7 Current Status

7.1 Involved SDO

Currently there are different activities to define how identity exchange over diverse domains should work. But on the one hand they are more coordinating and contracting initiatives and on the other hand they are not defining exactly the procedures for scenarios on an ad hoc manner.

7.1.1 Open Identity Solutions for Open Government

The US government has setup the Open Identity Initiative which seeks to leverage existing industry credentials for Federal use. The Initiative approves credentials for government use through the Trust Framework Providers who assess industry Identity Providers. The Trust Framework Provider Adoption Process outlines the process that the Identity, Credential and Access Management (ICAM) community uses to accrediting organizations that assess commercial identity providers.

This approach enables a scalable model for extending identity assurance across a broad range of citizen and business needs. These Trust Frameworks include requirements for trust framework provider (TFP) auditing qualifications and processes, TFP organizational maturity, TFP member identity provider organizational maturity, TFP member identity provider credentials and their issuance, and TFP member identity provider privacy policies.

The Adoption Process defines a process whereby the government can assess the efficacy of the Trust Frameworks for federal purposes so that an Agency online application or service can trust an electronic identity credential provided to it at a known level of assurance comparable to one of the four OMB Levels of Assurance. Trust Frameworks that are comparable to federal standards are adopted through this process, allowing federal relying parties to trust credential services that have been assessed under the framework. The adoption process is as follows:

1) Assessment package submission
2) Value determination
3) Comparability
4) Adoption decision

The sets of Trust Criteria for LOA 1 through 4 are taken verbatim from NIST SP 800-63 [i.5].

The current state is as following (15.05.2010).

Trust Framework Providers:

- Open Identity Exchange - Provisional Approval
- Kantara Initiative - Provisional Approval
- InCommon Federation - Draft submission under review

The Scheme Adoption Process outlines the process that the ICAM community uses to develop and/or approve specification profiles for achieving portable identity over the Internet.

Adopted Schemes:

- ICAM OpenID 2.0 Profile - Fully adopted
- Kantara SAML 2.0 eGovernment Profile - Fully adopted
- ICAM IMI 1.0 Profile - Fully adopted
- ICAM WS-Federation - In development

Identity Providers:

- Google - OpenID Foundation, Pilot assessment with NIH in progress
- Yahoo - OpenID Foundation, Pilot assessment in progress
- PayPal - OpenID Foundation, InfoCard Foundation, Pilot assessment in progress
- Equifax - InfoCard Foundation
- VeriSign - OpenID Foundation
- Wave

7.1.2 Open Identity Exchange

The Open Identity Exchange (OIX) [i.3] is a non-profit organization dedicated to building trust in the exchange of online identity credentials across public and private sectors. OIX also received initial grants from the OpenID Foundation (OIDF) and Information Card Foundation (ICF) to advance assurance for open identity technologies. The initial members are Google, PayPal, Equifax, VeriSign, Verizon, CA and Booz Hamilton. OIX works as an Open Identity Trust Framework (OITF) provider, which follows an open market model to provide the certification services needed to deliver the levels of identity assurance and protection needed by communities. The OITF is a set of technical, operational and legal requirements and enforcement mechanisms for parties exchanging identity information.

7.1.3 Roles and Relationships

Beside the already established roles to exchange identity information (Identity Service Provider, Relying Party and User) the OITF introduces additional actors to look after the defined requirements and mechanisms to support the flow of information among the other roles. The roles and relationships of these additional actors are as follows:

Policymakers decide the technical, operational and legal requirements for exchanges involving identity information among a group they govern.

OITF Providers translate the requirements of policymakers into their own blueprint for a trust framework that they then proceed to build. The OITF Provider typically operates a certification listing service that indicates which identity service providers and relying parties have been certified by which assessors, for which criteria, and for which trust frameworks.

Assessors evaluate identity service providers and relying parties and certify that they are capable of following the OITF Provider's blueprint.

Auditors may be called on to check that parties practices have been in line with what was agreed for the OITF.

Dispute resolvers may provide dispute resolution services for disagreements of a legal nature.

Figure 7 shows these roles and relationships in terms of agreements that link the participants [i.1].

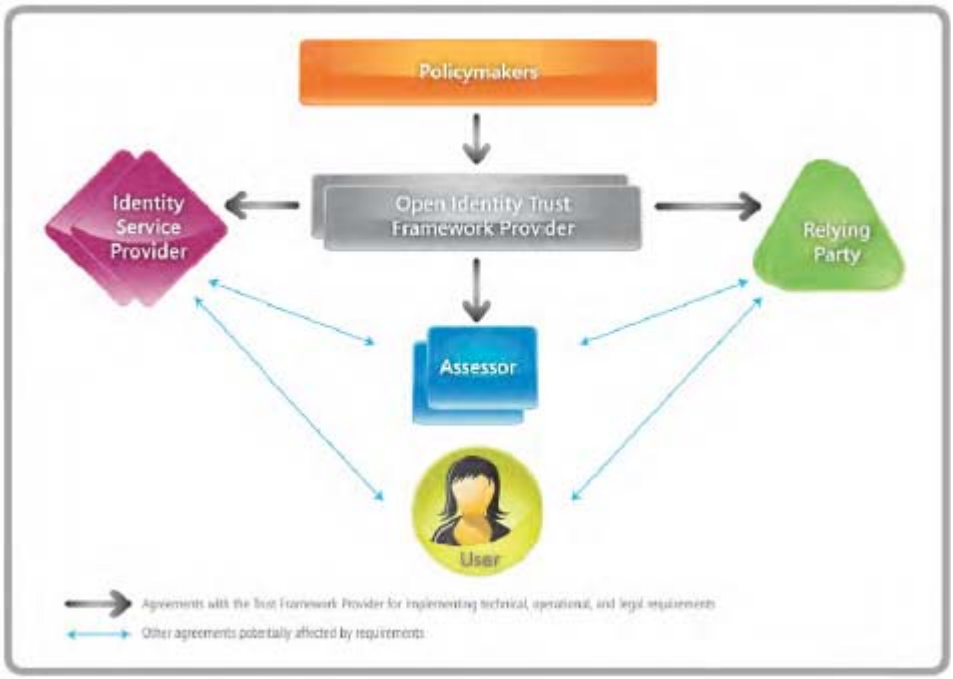

Figure 7: The participants in an OITF for identity information

7.1.4 Kantara Initiative

Kantara Initiative [i.4] was announced on April 20, 2009, by leaders of several foundations and associations working on various aspects of digital identity. It is intended to be a robust and well-funded focal point for collaboration to address the issues we each share across the identity community.

Kantara Initiative has setup different certification programs to ensure the interoperability of identity solutions. The certification program assesses applicants against strict criteria according to the Level of Assurance desired to be attained, and grants to candidates of the program the right to use the Kantara Initiative Mark.

7.1.5 Identity Assurance Certification Program

One of the key areas of focus is identity assurance where the Identity Assurance Work Group (IAWG) is driving the work of fostering adoption of identity credential services based on four distinct levels of assurance measured and validated in an open trust framework.

7.1.6 IAF Identity Assurance Levels: Snapshot View

Assurance Level	Example	Assessment Criteria-Organization	Assessment Criteria-Identity Proofing	Assessment Criteria-Credential Mgmt
AL1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL2	Change of address of record by a beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt ID	Single factor; prove control of token through authentication protocol
AL3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria - stronger attestation and verification of records	Multi-factor auth: cryptographic protocol; "soft", "hard", or "OTP" tokens
AL4	Dispensation of a controlled drug or $1M bank wire	Stringent organizational criteria	More stringent criteria - stronger attestation and verification	Multi-factor auth w/ hard tokens only; crypto protocol w/ keys bound to auth process

The end goal of this activity is to provide public and private sector organizations with a uniform means of relying on digital credentials issued by a variety of identity assurance providers (credential service providers) in order to advance trusted identity and facilitate public access to online services and information. Interoperability of e-authentication systems, mutual acceptance of rules, policies and supporting business processes is critical to the cost-effective operation of safe and secure systems that perform essential electronic transactions and tasks across industry lines.

In terms of services that will be certified, this program is technology agnostic - no specific requirements for technology protocol use are made of applicants. It is anticipate certifying services created utilizing a wide variety of open/standard identity technology, including but not limited to XMPP extensions, ID-WSF, iNames, Information Cards, OAuth, OpenID, SAML, XDI, PKI , IGF, XRD, XACML, OPML, APML, RDF, RSS, MicroFormats, OATH, WS, XRI, activity streams, OpenSocial, Portable Contacts, CX, etc.

7.1.7 Interoperability Certification Program

The Interoperability Certification Programs helps vendors to solve harmonization and interoperability challenges among identity-enabled enterprise, Web 2.0 and Web-based applications and services. The testing and certification program will help effectively accelerate adoption of new technologies and standards, helping deployers to deploy with confidence, success and minimal time and cost, and vendors to incorporate standards effectively and interoperability into their offerings.

7.2 Conclusion

The different initiatives show the necessity of inter domain federation very clearly. Only the approaches are mostly, as mentioned in the introduction, based on organisational aspects like assessment of a company or institution and do not meet really the requirements of "ad hoc federation" in the sense of the described use cases. The main point in the present document is that we search for a mechanism to cooperate or operate in an inter domain environment without a central instance for assessment. Approaches which rely on global central solutions never worked well because to find an agreement who is the master on control is very difficult. As it was over years with certificates where never was found an agreement who provides the global root certificate. Additionally centralised international trust relations are over the time not static, so we need a more dynamic solution which is based on the risk taking of each participating individual user and organisation. The solutions or mechanisms which will allow to instantiate an ad hoc federation are still open and should be discussed in ETSI or et al. in the identity community. The only thing what has to be "central" is a common understanding what parameters are used and what their values means. Therefore a central register, e.g. at Internet Corporation for Assigned Names and Numbers (ICANN), should be established and maintained.

If "Dynamic federation negotiation and trust management in IdM systems" could be achieved it would revolutionise the internet marketplace.

8 Authors & contributors

The following people have contributed to the present document:

Rapporteur:
Wolfgang, Steigerwald, Deutsche Telekom AG

Other contributors:
Peter, Scholta, Deutsche Telekom AG

Dr. Jörg, Abendroth, Nokia Siemens Networks GmbH & Co. KG

History

Document history		
V1.1.1	November 2010	Publication