ETSI GS INS 010 V1.1.1 (2014-03)

Group Specification

Identity and access management for Networks and Services; Requirements of a global distributed discovery mechanism of identifiers, providers and capabilities

Disclaimer

This document has been produced and approved by the Identity and access management for Networks and Services ETSI Industry Specification Group (ISG) 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-0010

Keywords

access, control, ID, management, network,
service

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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://ipr.etsi.org).

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 Group (ISG) Identity and access management for Networks and Services (INS).

Introduction

The analysis presented in GS INS 006 [i.1] concludes that there is a need for the development of a global discovery mechanism of identifiers, providers and capabilities. This work item investigates the requirements of such a mechanism and examines if any existing systems or mechanism meet these requirements and can - fully or partially - support the design of its architecture.

The present document is based on the principle that the global discovery mechanism provides only discovery of information that is somehow related to an identity, and is not by any means involved in any other kind of identity management procedures like information exchange, trust between service providers etc. It should be noted that it is not among the goals of the present document to enforce this principle towards the development of such a mechanism.

1 Scope

The scope of the present document is the identification of the requirements to develop a global distributed discovery of identifiers, providers and capabilities.

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] ETSI GS INS 006: "Identity and access management for Networks and Services; Study to Identify the need for a Global, Distributed Discovery Mechanism".

NOTE: See http://www.etsi.org/deliver/etsi_gs/INS/001_099/006/01.01.01_60/gs_ins006v010101p.pdf.

[i.2] SAML Specifications.

NOTE: See http://saml.xml.org/saml-specifications.

[i.3] International DOI® Foundation, Digital Object Identifier.

NOTE: See http://www.doi.org/.

[i.4] Liberty Alliance Project, Project liberty.

NOTE: See http://www.projectliberty.org.

[i.5] Internet2 Middleware Initiative, Shibboleth®.

NOTE: See http://shibboleth.internet2.edu.

[i.6] Eduserv, OpenAthens.

NOTE: See http://www.openathens.net.

[i.7] InCommon Discovery Service.

NOTE: See https://spaces.internet2.edu/display/InCFederation/Discovery+Service.

[i.8] Handle System®.

NOTE: See http://www.handle.net.

[i.9] IF-MAP.

NOTE: See http://www.if-map.com.

[i.10] Jon Crowcroft, Steven Hand, Richard Mortier, Timothy Roscoe, Andrew Warfield, "Plutarch: An Argument for Network Pluralism", ACM SIGCOMM, 2003.

[i.11] Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, Hari Balakrishnan, Chord: "A Scalable Peer-to-peer Lookup Service for Internet Applications", ACM SIGCOMM, 2001.

[i.12] Petar Maymounkov, David Mazières, Kademlia: "A Peer-to-Peer Information System Based on the XOR Metric", IPTPS, 2002.

[i.13] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, Scott Shenker: "A Scalable Content-Addressable Network", ACM SIGCOMM, 2001.

3 Abbreviations

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

CAN	Content-Addressable Network
DDNS	Dynamic DNS
DDoS	Distributed Denial-of-Service
DHT	Distributed Hash Table
DNS	Domain Name System
DNSSEC	DNS Security Extension
DOI®	Digital Object Identifier
DS	Discovery Service
IdM	Identity Management
ID-WSF	Identity Web Services Framework
IF-MAP	Interface for Metadata Access Points
IP	Internet Protocol
ISG	Industry Specification Group
SAML	Security Assertion Markup Language
STORK	Secure IdenTity AcrOss BoRders LinKed
VID	Virtual Identity
XRDS	EXtensible Resource Descriptor Sequence
XRI	EXtensible Resource Identifier

4 Requirements of a Global Distributed Discovery mechanism of identifiers, providers and capabilities

This clause presents the requirements of a Discovery System (DS) capable of supporting a Global Distributed Discovery mechanism of identifiers, providers and capabilities as identified by the ETSI INS ISG group.

1) Independent

1) It is recommended that the DS remains unaffected by the peculiarities of the various IdM operations between an identity producer and an identity consumer.

2) It is recommended that the DS exists as an independent entity which only provides discovery services and not as part of a specific identity management system or infrastructure.

3) The DS' components ought to be independent of each other, so the behavior of a component does not affect the others.

4) It is recommended that the DS remains unaffected by any commercial or other interests that may try to affect its functionality for business or any other non-technical reasons.

5) It is recommended that the ownership of this mechanism is assigned to a global non-profit organization. This organization ought to only supervise the smooth operation of the DS. It is also recommended that the owner organization does not interfere with the DS' functionality nor has access or rights on any of the information registered in it.

2) Distributed

1) It is recommended multiple entities host and run the components required to provide the discovery service. A global entity (non-profit organization) may be present to play a supervisory role.

2) It is required to ensure that there is no single point of failure in the architecture of the DS.

3) It is necessary that the architecture of the DS is scalable and not affected in any way (e.g. functionality, privacy, trust, security, etc.) by its size or the amount of stored information.

4) It is recommended that the DS supports dynamic join and leave of DS components (storage hosts), managed by different domains, holding a portion of the global space and managing the operations related to it (for performance reasons).

3) Global

1) The services of the DS are not to be confined within a specific context. It is necessary to ensure that the DS's services are accessible from everywhere and everyone (domains, federations, countries, networks, etc).

2) It is required for the DS to avoid any conflict with local laws and regulations. Moreover it ought to be able to adjust to diverse regulations that apply across various locations.

3) It is recommended that external entities (users, providers etc) have the ability to freely choose the place (network location within the DS) where they wish to store/register their private data. Also these entities ought to have the ability to easily migrate their private data to other places.

4) The DS ought to provide the means to associate identity related data irrespectively of the location that these data may reside.

5) It is required that the DS architecture ensures that the discovery process is able locate all the information that is relevant to a request. (This does not mean that all this information will be included in the response).

6) The DS ought to behave in a consistent way and always be in position to provide the best available response for a given request.

7) It is recommended that the DS has the ability to provide information about a user (or any other entity) regardless his intervention or accessibility. It is required that this action reflects user's policies and preferences (e.g. the user has previously authorized the DS to act on his behalf).

8) The response time of a request is not critical but it should be reasonable.

4) Privacy Enabled

1) It is required that the DS protects the privacy of the stored information against any kind of internal or external security issues e.g. misconfiguration, attacks from internal or external malicious parties, etc.

2) It is required that the DS always provides the necessary means for an external entity (users, providers, etc) to control its registered information e.g. insert, manage and withdraw information from the infrastructure, apply policies, allow or restrict access to certain information or parties etc.

3) Conflicting policies and rules ought to be acknowledged by the DS and presented to the appropriate entity (owner user, provider etc).

4) It is recommended that the DS supports various options when handling an incoming discovery request e.g. act independently, request the owner's consent, etc.

5) It is recommended that discovery responses provide the minimum of information required to handle a request (minimal disclosure).

6) It is required that discovery operations (requests and responses) are not traceable by unauthorized third parties, so the identity of the entities which perform the operations cannot be guessed.

7) It is recommended that external entities (users, providers etc) have the ability to freely choose the place (network location within the DS) where they wish to store/register their private data. They also ought to have the ability to easily migrate their private data to other places *(This requirement is also relevant with the section "Global")*. It is necessary that the DS keeps track of all the requests and actions performed on specific information and has the ability to present this activity to the owner of the information.

5) Secure

1) An authentication mechanism is required to control the access of authorized entities e.g. users.

2) It is recommended that the information stored in the DS is encrypted, easily invalidated and recoverable with minimum or no cost or harm.

3) A security framework is required to protect the DS from any kind of external attacks, e.g. DDoS.

4) It is required that the DS provides protection against data traffic monitoring that could lead to any kind of malicious or unauthorized actions e.g. construction of user behavior models.

5) It is recommended that the DS is able to support the establishment of secure connections/channels for any kind of communication with internal or external entities (users, providers etc). Such communication may involve actions like discovery requests, data registration, user account management etc.

6) Trusted

1) It is recommended that the DS is able to prove its trustworthiness to all external entities that interact with it.

2) It is recommended that the DS has the necessary means to monitor its components behaviour and take actions to prevent or stop inappropriate actions.

3) It is recommended that the DS does not interfere with trust relations between external entities that use its functionality.

4) An access control framework is required to provide the means to validate external parties which wish to register information in the DS. It is recommended that the DS is able to accept and evaluate any kind of input from any available trust frameworks or other sources in order to validate external entities that want to register information in its infrastructure.

5) It is recommended that the DS does **not** validate external entities which issue discovery requests to the DS. Exceptions may apply for external parties that have been reported to act maliciously.

6) It is recommended that the DS is able to notify the owners of the information requested in a discovery request and ask permission to include their data in the response.

7) Open and Extensible

1) It is recommended that the DS has the ability to support, adopt and provide additional functionality in the form of external frameworks.

2) It is recommended that external entities (users, providers etc) have the ability to create and manage multiple accounts in the DS.

8) Interoperable

1) It is required that the DS' services are not restricted to only specific technologies, protocols and formats etc. It is necessary that the DS has the ability to handle any kind of identity information, and all types of existing formats.

2) It is recommended that the DS does not introduce new types of identifiers and formats that need to be enforced in existing networks and services procedures. The creation of new formats that do not affect the operation of existing networks (e.g. for DS' internal purposes) is acceptable.

3) It is recommended that globally accepted semantics are adopted to describe hosted data, requests and responses in a unified manner (e.g. SAML [i.2], DOI® [i.3], etc).

4) It is recommended that among the DS's capabilities is the ability to transform external entities' actions and choices to globally accepted semantics - information.

5) It is required that the DS defines and follows a clear process for the insertion of new globally accepted elements (e.g. description of a new identity attribute).

9) User friendly

1) It is recommended that the use of the DS should be intuitive to the user.

2) It is recommended that the DS search mechanism supports finding elements from their semantic description, using various and different ontologies (and vocabularies) to regulate them.

5 Existing discovery systems & mechanisms vs the Requirements of a global DS

This clause will present the most relevant discovery systems and mechanisms and evaluate whether they can support the development a global discovery mechanism of identifiers, providers and capabilities.

5.1 Federated Identity Management Frameworks

The notion "federation" can be interpreted in many ways. Any kind of collaboration between two or more parties can be characterized as a federation. In the present document the word federation describes a group of domains, which agree on a specific set of rules and share/exchange information within a closed Circle of Trust. Based on this interpretation we will analyse the federated IdM systems and their ability to support the development of a Global Distributed Discovery mechanism of identifiers, providers and capabilities.

The majority of the federated IdM systems design their own proprietary Discovery Systems (DS) based on the procedures and services of the federation. Such DS are the ID-WSF Discovery Service proposed in Liberty Alliance [i.4] project, the "Where Are You From (WAYF)" service from the early versions of Shibboleth [i.5] and Athens [i.6], the InCommon Discovery Service [i.7] from Shibboleth etc. (More information about these systems are available on [i.1]). Despite the fact that these DS have large diversities, there are foundational architectural similarities and principles based on which all of them are designed. This clause will examine these DSs as one category and evaluate their capability to support a Global Distributed Discovery mechanism of identifiers, providers and capabilities.

Advantages

1) Use of well established protocols

Federated IdM systems and their DSs generally use widely accepted protocols and formats to support communication between its participants. This offers easy adaptation of new components, features and entities, etc.

2) User friendly

The majority of the procedures needed to operate a DS in a federation are not presented to the end users and are handled by the providers that form the federation. Such procedures are for example the association of identities and identity related data issued by different providers, registration of information in the DS, policy enforcement etc. Hiding these complex operations from the users, allow federated IdM to construct more user-friendly interfaces, which require the minimum of users' intervention to fully operate.