International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1258

(09/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Enhanced entity authentication based on aggregated attributes

Recommendation ITU-T X.1258

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1258

Enhanced entity authentication based on aggregated attributes

Summary

Aggregating attributes from multiple attribute authorities may be needed in order to enable a relying party to enhance its trust in the identity of a party. The aggregation can be regarded as having to deal with a collection of globally unique identifiers, which is common across all attribute authorities. Practically, entities do not have a global identifier but have different entity identifiers and attributes assigned by their various identity service providers (IdSPs).

To address the attribute-aggregating problem in this scenario, the concept of identity federation is used. For example, if an e-book store plans to have a sale for seniors, the store has to be given the aggregated set of attributes (credit card and age bracket) from two IdSPs, but without the IdSPs knowing about each other's involvement. In standard federated identity management, an entity can only provide attributes from one identity, but this transaction requires attributes from two. There are several identity federation methods: security assertion markup language (SAML), Shibboleth, open identity (OpenID), and open authentication (OAuth), etc.

Recommendation ITU-T X.1258 introduces the concept of attribute aggregation to allow an entity to aggregate attributes from multiple IdSPs. Attribute aggregation is the mechanism for collecting attributes of an entity retrieved from multiple IdSPs. Attribute aggregation is needed to aggregate the attributes dynamically on demand. IdSP can realize the aggregation request when an entity wants to get a service. Additionally, an entity-centric attribute aggregation mechanism could also be applied to the authentication for mitigating privacy leakage.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1258	2016-09-07	17	11.1002/1000/12850

Keywords

Attribute aggregation, federated identity management.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1258

Enhanced entity authentication based on aggregated attributes

1 Scope

This Recommendation provides enhanced authentication based on aggregation of entity attributes across domains. This Recommendation covers the following topics:

– methods for aggregating multiple identity service provider (IdSP) attributes; and

– enhanced authentication based on aggregated attributes.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attribute [b-ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.2 (entity) authentication [b-ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

3.1.3 circle of trust [b-ITU-T X.1251]: A set of criteria established for joining organizations within a federation for the purposes of trusted access to each other's resources. Note that a circle of trust is also the end result of joining organizations within a federation.

3.1.4 federation [b-ITU-T X.1252]: An association of users, service providers, and identity service providers.

3.1.5 identity [b-ITU-T X.1252]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

3.1.6 identity service provider (IdSP) [b-ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 attribute aggregation: A mechanism for collecting attributes from multiple identity service providers (IdSPs).

NOTE – Once the attributes have been collected, they need to be aggregated and asserted for authentication and authorization.

3.2.2 domain: Management coverage of a single identity service provider (IdSP).

3.2.3 service provider (SP): An entity that provides services to the clients or to the other service providers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CoT	Circle of Trust
DB	Database
ID	Identity
IdM	Identity Management
IdSP	Identity Service Provider
LS	Linking Service
OAuth	Open Authentication
OpenID	Open Identity
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
VC	Virtual Collaboration

5 Conventions

None.

6 General

In general, electronic identity management (IdM) covers the management of any form of digital identity. The development of directories, such as those supported by [b-ITU-T X.500], could be an origin of IdM. [b-ITU-T X.509] defines certificates containing identity attributes. The certificates of [b-ITU-T X.509] and public key infrastructure (PKI) systems operate to prove the online "identity" of a subject. Therefore, IdM could be considered as the management of information.

The identity of an entity may be composed of attributes that characterize this entity in different contexts. Different identities may be needed depending on the context and situation. An IdM system provides tools for the management of these identities in a digital world. IdM is a set of functions and capabilities such as identity creation/deletion, discovery and exchange of information. In the real world, people choose which information can be revealed to others, taking into account the context and sensitivity of the information. In the digital world, in turn, this task is performed by the IdM system.

Based on the technologies and standards with regards to IdM, IdM system methods are classified as conventional, centralized and federated. The characteristics of the conventional method is that a service provider (SP) handles identities and is collocated with the identity service provider (IdSP). An entity creates its digital identity (ID) for each SP from which it wants to get services. Usually, entity IDs are not shared among the different SPs and this approach tends to be more costly for both the entity and the SPs. Each SP may require repeatedly its own set of attributes to form the digital identity of the entity.

The centralized method has been developed as a solution to the inflexibility of the conventional method and shares identities among SPs; it is based on the concept of single authentication, single sign-on (SSO). This method tries to avoid inconsistencies and redundancies in the conventional method, giving entities the capability to interact with various SPs without the need to perform redundant authentication.

Every SP that has trust relationships with an IdSP relies completely on the entity authentications provided by this IdSP. The IdSP is responsible for authenticating an entity and supplying to SPs the attribute information of the entity within a domain, which can represent a company, a university, etc., and is composed of entities, multiple SPs and a single IdSP. SSO provides a great convenience to the entities, since they only need to perform the authentication process once. Thereafter, entities can use the obtained credentials on all SPs they wish to access. However, the weak point of the centralized method is that the IdSP has absolute control over the information of its entities, and may use their information in any way it wants. This is the main reason why the centralized method has not been widely adopted.

To resolve the problems resulting from the centralized method, the federated identity method was introduced, based on the distribution of the task of authentication over multiple IdSPs. These IdSPs belong to different domains. The concept of the federated identity relies on trust relationships that are established among multiple IdSPs and the corresponding domains. To connect distributed identity information between an IdSP and an SP, a trust relationship is required between the two parties. This trust relationship is called a circle of trust (CoT), which may include one or more IdSP and SPs. In a CoT, if the user is authenticated in an IdSP, then access to SPs within the CoT without further authentication is permitted. As a result, a user needs to be authenticated only once in a CoT [b-ITU-T X.1251].

Federated IdM is an approach to resolve the risk of a single IdSP and decrease information exchange with the IdSP during authentication. These agreements between IdSPs ensure that identities issued in one domain are recognized by SPs in other domains and the concept of SSO is available even when different domains are involved.

The benefit of federated identities to SPs is that they can handle a smaller number of entities' information. The Kantara Initiative [b-Kantara], Shibboleth [b-Shibboleth] and Higgins [b-Higgins] follow the federated IdM method. In federated identity methods, identities are distributed across different IdSPs, and entities' information can be made available to any other third parties (IdSPs) in the federation.

7 Architectures and flows for attribute aggregation methods

Early work on merging attributes from multiple attribute authorities assumed that the entity had a globally unique identifier that was common across all attribute authorities. In reality, entities do not have global identifiers, but different entity identifiers and attributes assigned by their various IdSPs.

Liberty Alliance [b-Liberty], which was succeeded by the Kantara Initiative [b-Kantara], was the first group to address the attribute-aggregating problem, through their concept of identity federation [b-Chadwick]. However, one unresolved problem is the lack of a standard approach to aggregating entity attributes, asserted by multiple authorities, for an SP to use in its access control decision-making.

A couple of use cases might be helpful to consider why attribute aggregation is needed.

– If an e-book store plans to have a sale for seniors, the store has to be given the aggregated set of attributes (credit card details and proof of senior status) from multiple IdSPs. In this example, it is required for an entity to provide the attributes from two identities.
– Suppose a researcher would like to purchase a computer using a federated bank account from an online store that offers discounts to the educational sector, the researcher must provide proof that he is a member of an educational organization and that he has a specific account

at his bank. Attributes stored in multiple distinct identities need to be collected and the result of this union should be transmitted to an SP, a process known as attribute aggregation [b-Klingenstein].

Sharing and coordinated use of resources within dynamic and multi-institutional communities is fundamental to an increasing range of computer applications, ranging from scientific collaborations to healthcare. Such sharing is necessarily highly controlled. Resource providers and consumers need to define clearly and carefully just what is shared, who is allowed to share, and the conditions under which sharing occurs. A set of individuals or institutions defined by such sharing rules form a so-called virtual collaboration (VC). Providing self-management in order for VCs to be able to easily create and manage memberships and roles for their own groups, and access controls for their own resources, is a challenge, especially when those shared resources are hosted at multiple institutions. In a VC scenario, the federated IdSP cannot usually provide all the attributes that are relevant to participating SPs. Such VC-related attributes, VC name, membership status, member mailing list, etc., need to be aggregated from other sources. Several distinct attribute authorities need to participate in the management of user attributes [b-Hulsebosch].

There are several identity federation methods: the security assertion markup language (SAML), Shibboleth [b-Shibboleth], the Web Services-Federation [b-WS-Federation], the Kantara Initiative [b-Kantara], open identity [b-OpenID], open authentication [b-OAuth], CardSpace [b-CardSpace], Higgins Project [b-Higgins], etc. Based on who mediates the whole process, attribute aggregation methods could be classified into three categories: IdSP-mediated methods, SP-mediated methods and entity-mediated methods.

7.1 Identity service provider-mediated methods

7.1.1 Identity linking

A method, introduced by the Liberty Alliance framework, is one of the first methods to address the problem of attribute aggregation through its concept of identity federation, see Figure 1 [b-Liberty]. In Figure 1, IdSPs allow the entity to create a pair-wise link (CoT3) between two IdSPs. When an entity moves around services, the first IdSP (IdSP1 in Figure 1) asks that entity if it would like to federate this IdSP (IdSP1) with other IdSP (IdSP2). At this point, both IdSPs interact with each other to create a link indicator. While accessing services from an SP, one IdSP provides that link indicator to the SP along with the assertion-containing attributes. The SP can use the indicator to retrieve other assertion-containing attributes from the other IdSP. By combining attributes from both IdSPs, the SP can determine whether the entity can access a service.

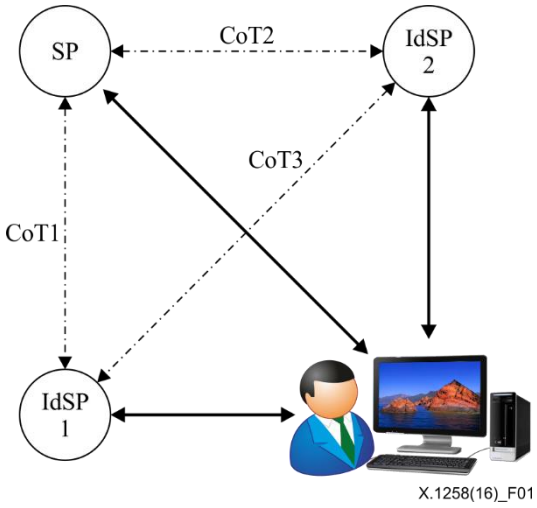

Figure 1 – Architecture of the identity-linking method

Figure 2 shows a conceptual control flow of attribute aggregation using the identity-linking method.

(1) An entity sends a service request to an SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1 for authentication.

(4) IdSP 1 authenticates the entity and requests more attributes.

(5) IdSP 1 returns the authentication assertion.

(6) The entity submits an authentication assertion to the SP.

(7) The SP requests more attributes regarding the entity from IdSP 2.

(8) IdSP 2 provides the extra attribute.

(9) The SP verifies the assertions and permits the entity to access the service.

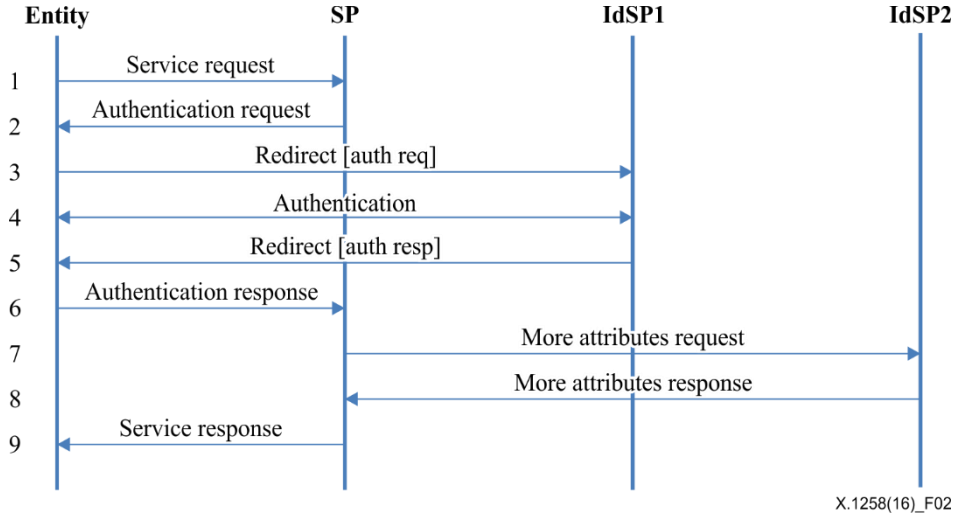

Figure 2 – Attribute aggregation flow using the identity-linking method

7.1.2 Identity proxying

There is a proxy IdSP and an SP has a connection with this IdSP that it trusts completely; other IdSPs are unknown to the SP and they only have trust relationships with the proxy IdSP (IdSP1), see Figure 3 [b-Klingenstein]. If the entity would like to aggregate attributes from multiple IdSPs, the entity is redirected first to the proxy IdSP (IdSP1 in Figure 3), and then the proxy IdSP redirects the entity to other multiple IdSPs. After the entity is authenticated individually at each IdSP, the entity returns an assertion to the proxy IdSP. After this, the proxy IdSP verifies each assertion, retrieves attributes from the IdSPs and aggregates all these attributes. The proxy IdSP could fill up the aggregated set with its own entity attributes and reassert the assertions. Then the proxy IdSP sends all reasserted attribute assertions to the SP. Then, the SP determines whether the entity can access the service based on the aggregated attributes. Because the SP is not aware of the other IdSPs but only has a relationship with the proxy IdSP, it assumes that all attributes have been released by the proxy IdSP.

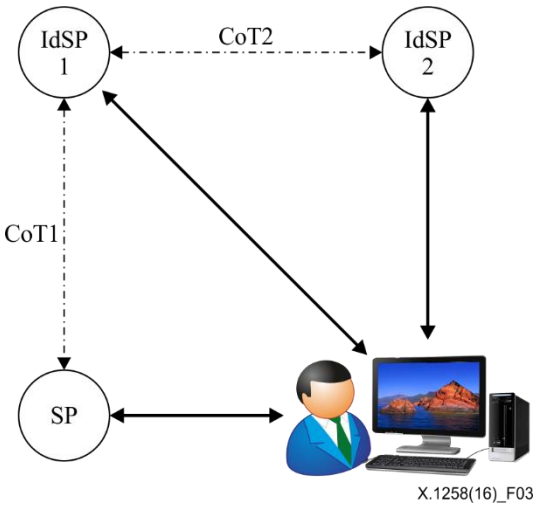

Figure 3 – Architecture of the identity-proxying method

Figure 4 shows a conceptual control flow of attribute aggregation using the identity-proxying method.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1 (as a proxy) for authentication.

(4) IdSP 1 redirects the entity to IdSP 2.

(5) IdSP 2 receives an authentication and attribute request.

(6) IdSP 2 authenticates the entity.

(7) IdSP 2 returns the authentication result and attribute assertions.

(8) The entity forwards the authentication result and attribute assertions to IdSP 1.

(9) IdSP 1 adds additional attributes, signs the assertions and returns them to the entity.

(10) The entity submits the assertions to the SP.

(11) The SP verifies the assertions and permits the entity to access the service.

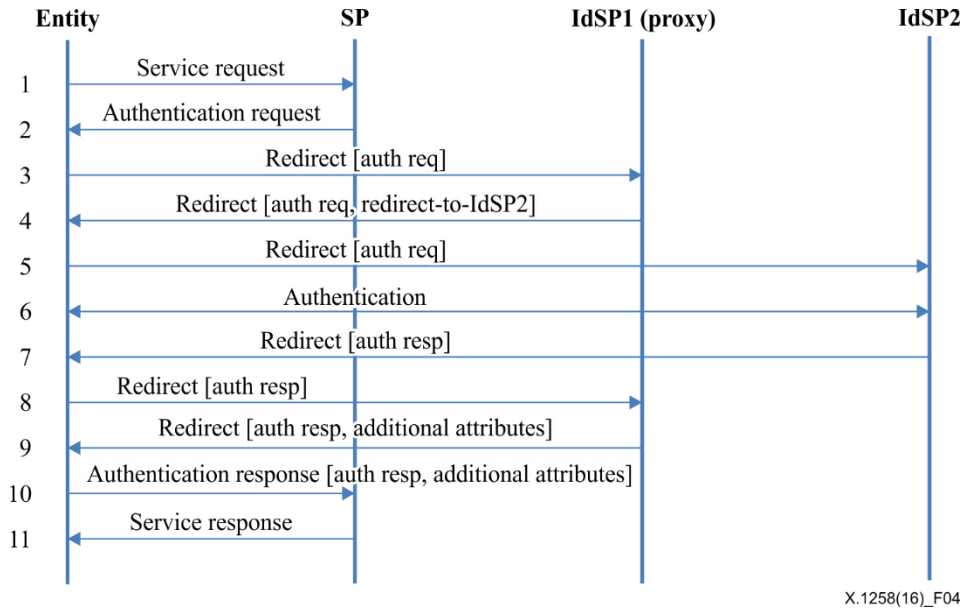

Figure 4 – Attribute aggregation flow using the identity-proxying method

7.1.3 Identity relay

The identity relay method is similar to the proxying method, but does not require strong trust between an SP and a proxy IdSP. Although the proxy method requires the SP to have complete trust in the trusted IdSP, in reality, it might be impossible to provide absolute trust between the proxy IdSP and the SP. In the identity relay method, an intermediary IdSP (or relay IdSP; IdSP1 in Figure 5) can act like a proxy IdSP. Then the flow is similar to that of the proxy method, the entity is first redirected to the relay IdSP and then the relay IdSP redirects the entity to other multiple IdSPs. After the entity is authenticated individually at each IdSP, the entity returns an assertion to the relay IdSP. After that, the relay IdSP combines all assertions into a single assertion and forwards it to the SP. The difference between the proxying and the relay model lies in the signing of the attribute assertions. The relay IdSP does not sign the attribute assertions, but just relays the assertions signed by the origin IdSP. Then, the SP receives encrypted attribute assertions from the IdSPs and relay IdSP, and determines whether the entity can access the service based on the aggregated attributes. This method needs a trust relationship between the IdSPs and SP.

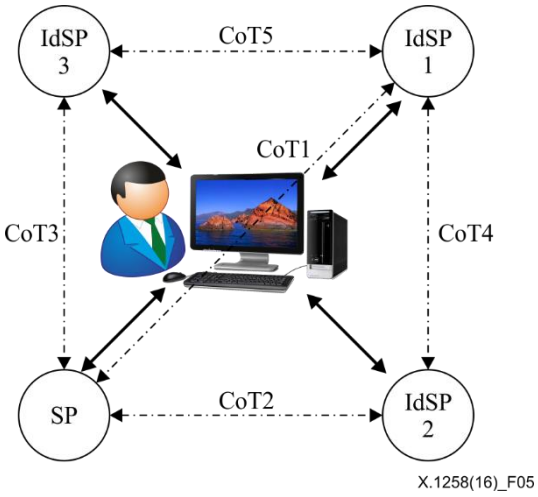

Figure 5 – Architecture of identity relay method

Figure 6 shows a conceptual control flow of attribute aggregation using the identity relay method.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1 (as a relay) for authentication.

(4) IdSP 1 redirects the entity to IdSP 2.

(5) IdSP 2 receives an authentication and attribute request.

(6) IdSP 2 authenticates the entity.

(7) IdSP 2 returns the authentication result and attribute assertions.

(8) The entity forwards the authentication result and attribute assertions to IdSP 1.

(9) IdSP 1 adds additional attributes, signs the assertions and returns them to the entity.

(10) The entity submits the assertions to the SP.

(11) The SP verifies the assertions and permits the entity to access the service.

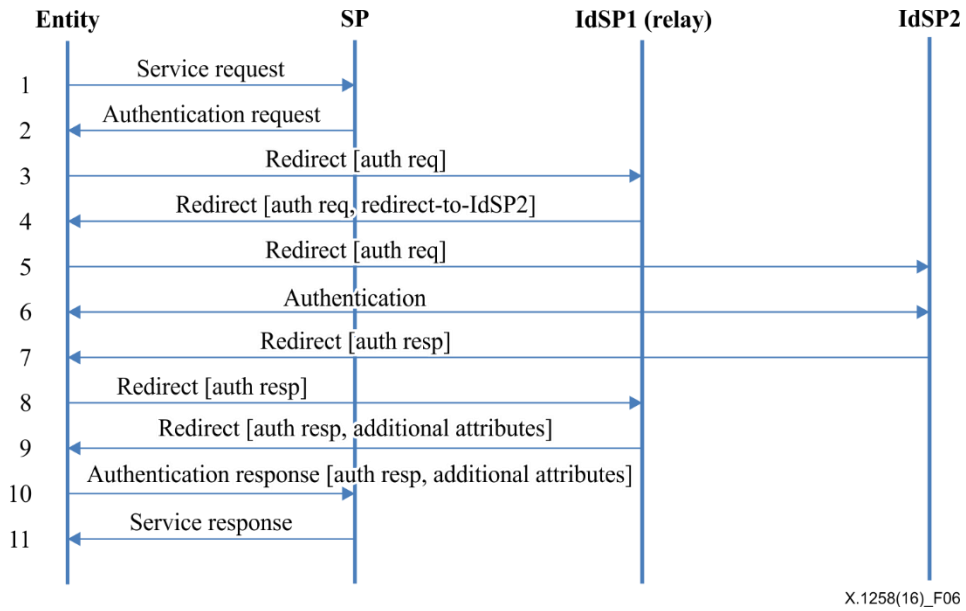

Figure 6 – Attribute aggregation flow using the identity relay method

7.2 Service provider-mediated methods

7.2.1 Application database

The application database (DB) method is the simplest of the attribute aggregation methods, see Figure 7 [b-Hulsebosch]. The SP retains extra entity attributes, a nickname, entity-preferences for that particular service, group membership, etc., in addition to the attributes supplied by the IdSP. The SP manages the added attributes for applications. Furthermore, such attributes of its DB can be retrieved later for the SP to determine whether the entity can access a particular service.

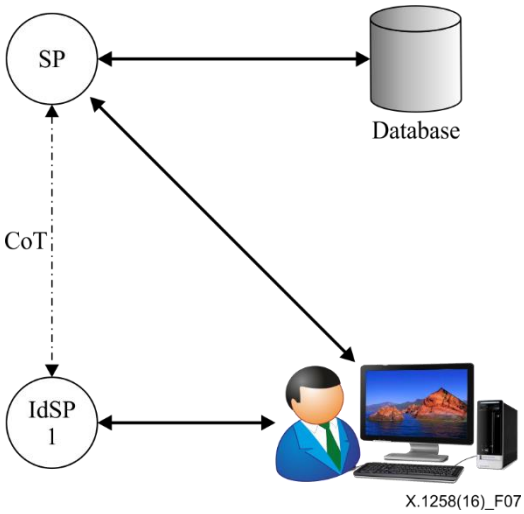

Figure 7 – Architecture of application database method

Figure 8 shows a conceptual control flow of attribute aggregation using the application DB.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1 for authentication.

(4) IdSP 1 authenticates the entity.

(5) After authentication success, IdSP 1 returns the authentication result and the assertion.

(6) The entity submits the authentication assertion to the SP.

(7) The SP retrieves additional entity attributes from its DB, if necessary.

(8) The SP verifies the assertion(s) and permits the entity to access the service.

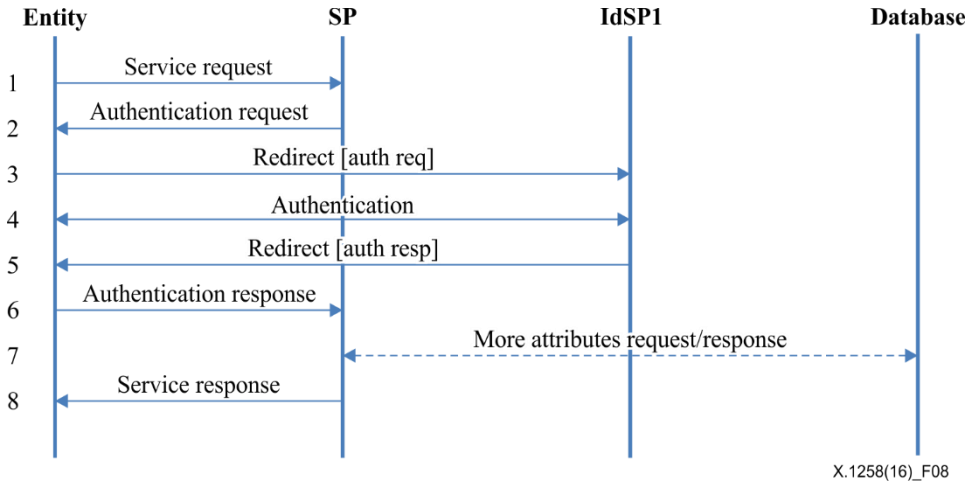

Figure 8 – Attribute aggregation flow using application database method

7.2.2 Service provider

The SP method allows the entity to aggregate attributes from multiple IdSPs in a single session, see Figure 9 [b-Hulsebosch]. The entity is redirected to different IdSPs one after the other where the entity is authenticated separately and returns an attribute assertion to the SP. The SP aggregates the attribute assertions from IdSPs and determines whether the entity can access a particular service.

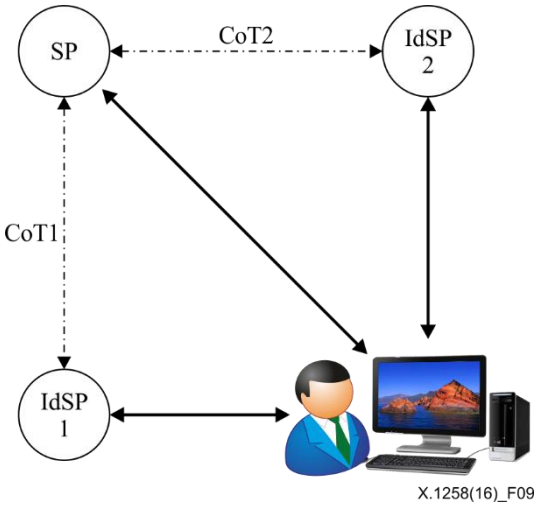

Figure 9 – Architecture of the service provider method

Figure 10 shows a conceptual control flow of attribute aggregation using the SP method.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1 for authentication.

(4) IdSP 1 authenticates the entity.

(5) IdSP 1 returns an authentication result and assertion.

(6) The entity submits an authentication assertion to the SP.

(7) The SP asks the entity for more attributes regarding the entity.

(8) The entity sends more attribute requests to IdSP 2.

(9) IdSP 2 authenticates the entity.

(10) IdSP 2 provides the additional attributes.

(11) The entity submits the authentication assertions to the SP.

(12) The SP verifies the assertion(s) and permits the entity to access the service.

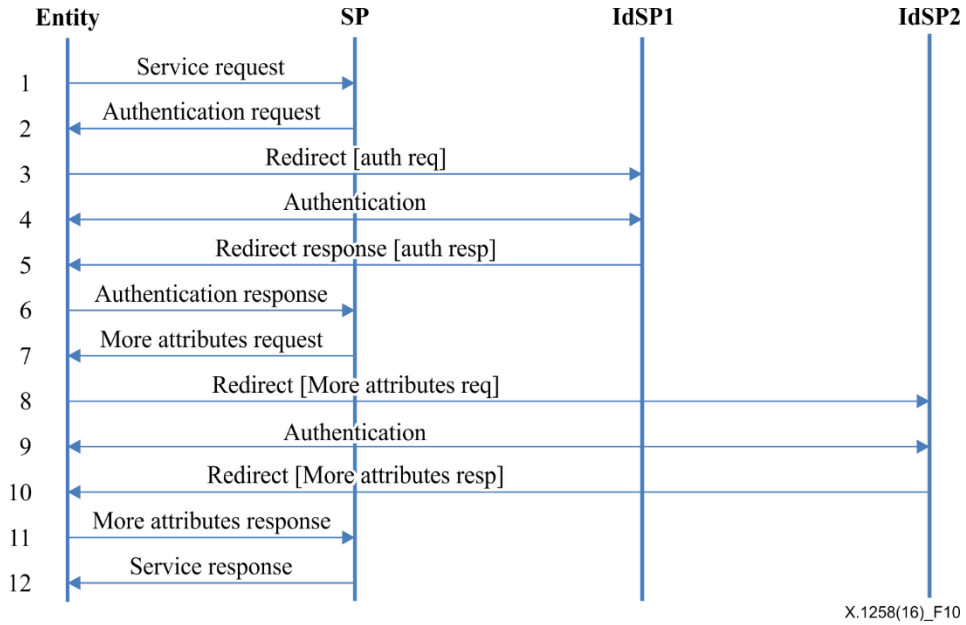

Figure 10 – Attribute aggregation flow using the service provider method

7.2.3 Linking service

The linking service (LS) method is a combination of the linking and identity relay method. The LS is a special type of SP, see Figure 11, which is used by the entity using a LS-supplied identifier [b-Chadwick], [b-Hulsebosch]. The LS-supplied identifier is used to link different IdSPs using the IdSP-supplied LS-specific persistent identifiers in a table called the linking table. If an entity wants to access a service, the entity visits the SP and is redirected to the first IdSP (IdSP 1 in Figure 11). The entity is authenticated at IdSP 1, and then an assertion containing entity attributes and the identifier for the LS are returned to the SP through the entity. The SP forwards the identifier to the LS to get more attributes. At this point, two options are available: either the LS can retrieve the list of linked IdSPs for this persistent identifier using the linking table and retrieve attributes from each of them, which are then combined at the LS and are returned to the SP or the LS can send back the list of linked IdSPs to the SP. Then the SP retrieves the attributes from each IdSP. Finally, the SP determines whether the entity can access the service based on the aggregated attributes.

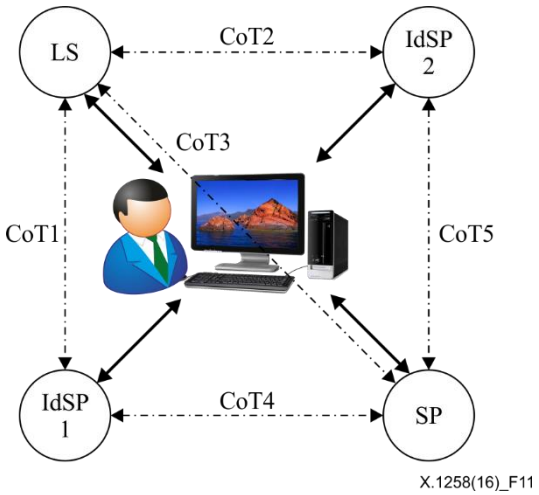

Figure 11 – Architecture of the linking service method

Figure 12 shows a conceptual control flow of attribute aggregation using the LS method.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) The entity is redirected to IdSP 1.

(4) IdSP 1 authenticates the entity.

(5) IdSP 1 returns an authentication assertion and the identifier for the LS.

(6) The entity submits the assertion and the identifier for the LS to the SP.

(7) The SP sends more attribute requests to the entity.

(8) The entity is redirected to the LS.

(9) The LS asks IdSP 2 for attributes.

(10) IdSP 2 provides the attributes.

(11) The attributes are returned to the entity.

(12) The entity submits the authentication assertion(s) to the SP.

(13) The SP verifies the assertion(s) and permits the entity to access the service.

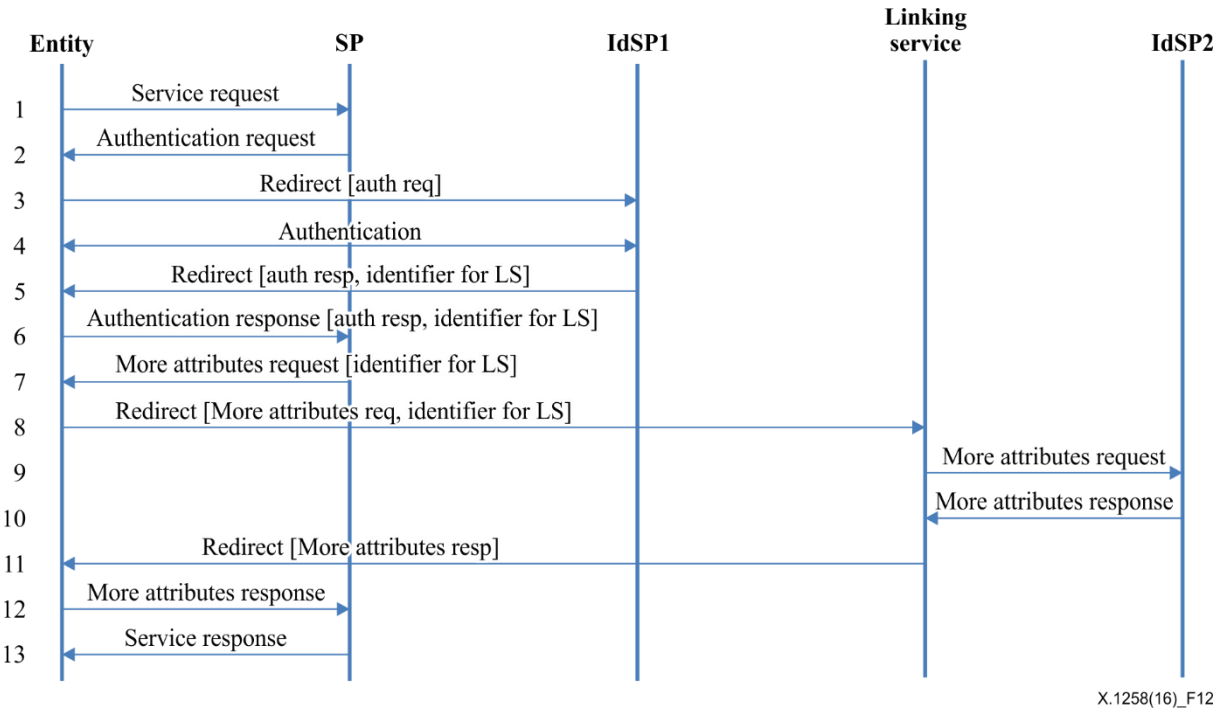

Figure 12 – Attribute aggregation flow using the linking service method

7.3 Entity-mediated method

The entity-mediated method uses a client (the entity-agent or application) that has the capability to aggregate attributes from different IdSPs, see Figure 13 [b-Klingenstein], and [b-Hulsebosch]. The SP informs the client about the list of trusted IdSPs. The client redirects the entity to each of these IdSPs. After respective authentication at each IdSP, the client receives assertions from all IdSPs and presents the combined set of assertions to the SP. The SP verifies each assertion, retrieves all attributes and then determines whether the entity can access the service.

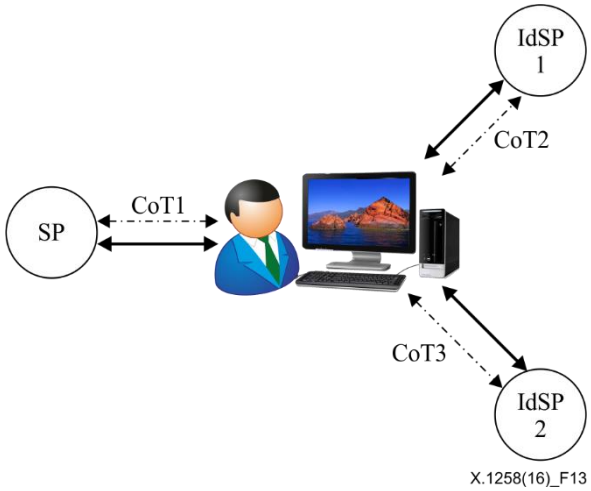

Figure 13 – Architecture of the client method

Figure 14 shows a conceptual control flow of attribute aggregation using the client method.

(1) The entity sends a service request to the SP.

(2) When the SP needs the service permission of the entity, the SP sends an authentication and an authentication assertion request.

(3) IdSP 1 authenticates the entity.

(4) IdSP 1 returns the authentication assertion.

(5) The entity is redirected to IdSP 2 for more attribute assertion(s).

(6) IdSP 2 authenticates the entity.

(7) IdSP 2 returns the attribute assertion(s).

(8) The entity submits the authentication assertion(s) to the SP.

(9) The SP verifies the assertion(s) and permits the entity to access the service.

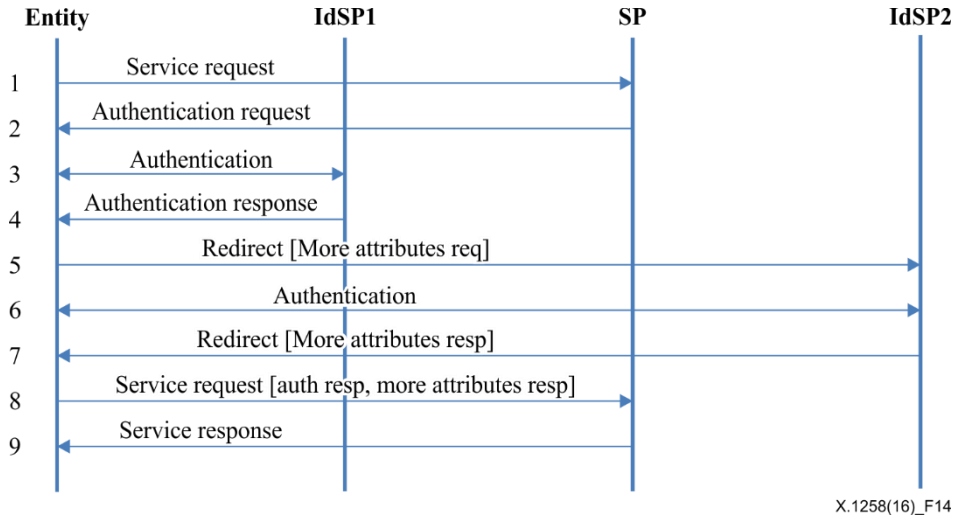

Figure 14 – Attribute aggregation flow using the client method

8 Comparison of the aggregated authentication methods

The seven methods of clause 7 are new approaches from the traditional federated IdM system. Each of these methods has additional entities or interactions. Based on these modifications, the seven methods can be analysed and compared by factors in order to select a suitable aggregation method. The designer and developer should consider issues such as: who mediates/aggregates/verifies the attributes, implementation difficulty or the addition of new elements.

Clause 7 presents several methods based on SAML for attribute aggregation. These methods could be interoperable based on how they are expressed in SAML.

Aggregation methods are analysed with respect to aggregation mediation, aggregation enforcement and additional element. A comparison of aggregated methods is shown in Table 1.

In Table 1,a tick "✓" in a cell indicates that the aggregation method of the row has the capability of the column. More precisely, the marked capability should be supported by the implementation of the marked method.

Table 1 – Comparison of aggregation methods

Aggregation method	Capability						
	IdSP mediation	**SP mediation**	**Client mediation**	**IdSP aggregation**	**SP aggregation**	**Client aggregation**	**Additional element**
Identity linking	✓				✓		
Identity proxying	✓			✓			
Identity relay	✓			✓			
Application database		✓			✓		DB
Service provider		✓			✓		
Linking service		✓			✓		LS
Client			✓			✓	client

Regarding the identity-linking method, the aggregation is mediated by the IdSP and enforced at the SP. It means that the attribute aggregation protocol should be implemented in the IdSP and SP. However, in other cases, the aggregation mediation and enforcement can be implemented in the same provider. It might be easier for the provider to operate the attribute aggregation rather than the identity-linking method. Regarding additional elements for attribute aggregation, the application DB method needs its own DB; the linking service method needs an LS (linking service) as a special type of SP; the entity-mediated method needs a client as an agent. Based on these criteria, the identity-proxying method and identity relay method are recommended in IdSP-mediated methods and the SP method is recommended in SP-mediated methods.

Bibliography

[b-ITU-T X.500] Recommendation ITU-T X.500 (2016) | ISO/IEC 9594-1:2017, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-CardSpace] *Introducing windows cardspace*. MSDN technical articles, Microsoft Corporation.
Available (viewed 2016-12-19) at: http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[b-Chadwick] Chadwick, D.W., Inman, G. (2009). Attribute aggregation in federated identity management. *IEEE Computer*, **42**(5), pp. 33–40.
<http://doi.ieeecomputersociety.org/10.1109/MC.2009.143>

[b-Higgins] Higgins, *Project.*
Available (viewed 2016-12-05) at: <http://www.eclipse.org/higgins/>

[b-Hulsebosch] Hulsebosch, B., Wegdam, M., Zoetekouw, B., van Dijk, N,, Poortinga-van Wijnen, R. (2012), Virtual collaboration attribute management. 41 pp. Available (viewed 2016-12-05) at:
<https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/EDS+11-06+Attribute+Management+v1.0.pdf >

[b-Kantara] Kantara, *Initiative*
Available (viewed 2016-12-19) at: https://kantarainitiative.org/reports-recommendations/

[b-Klingenstein] Klingenstein, N. (2007). Attribute aggregation and federated identity. In: *Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07)*, p. 26–29.

[b-Liberty] Liberty Alliance, *ID-FF 1.2 Specifications*, Available (viewed 2016-12-05) at:
<http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications

[b-OAuth] OAuth.
Available (viewed 2016-12-19) at: http://oauth.net/documentation/getting-started/

[b-OpenID] OpenID authentication 2.0.
Available (viewed 2016-12-19) at: http://openid.net/specs/openid-authentication-2_0.html

[b-Shibboleth] Shibboleth Consortium, *Open Source Project*.
Available (viewed 2016-12-05) at: <https://shibboleth.net/>

[b-WS-Federation] Web Services Federation Language (WS-Federation) Version 1.2.
Available (viewed 2016-12-19) at: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017