

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1250

(09/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

**Baseline capabilities for enhanced global
identity management and interoperability**

Recommendation ITU-T X.1250



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 |

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

Recommendation ITU-T X.1250

Baseline capabilities for enhanced global identity management and interoperability

Summary

Recommendation ITU-T X.1250 describes baseline capabilities for global identity management (IdM) interoperability (i.e., to enhance exchange and trust in the identifiers used by entities in telecommunication/information technology IT networks and services). The definitions and need for IdM are highly context-dependent and often subject to very different policies and practices in different countries. The capabilities include the protection and control of personally identifiable information (PII).

Source

Recommendation ITU-T X.1250 was approved on 25 September 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

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 not 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/>.

© ITU 2010

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

| | Page |
|---|-------------|
| 1 Scope | 1 |
| 2 References..... | 1 |
| 3 Definitions | 1 |
| 3.1 Terms defined elsewhere..... | 1 |
| 3.2 Terms defined in this Recommendation..... | 2 |
| 4 Abbreviations..... | 3 |
| 5 Conventions | 4 |
| 6 General..... | 4 |
| 7 Capabilities for global identity management and interoperability | 5 |
| 7.1 Examples of possible identity management transaction models | 5 |
| 7.2 An interoperable set of identity management (IdM) capabilities..... | 8 |
| 7.3 Four basic identity components..... | 9 |
| 7.4 Discovery of identity capabilities..... | 11 |
| 7.5 Interoperability and bridging..... | 12 |
| 7.6 IdM security..... | 13 |
| 7.7 Protection, control and use of personally identifiable information (PII)..... | 14 |
| 7.8 Auditing and compliance..... | 15 |
| 7.9 Performance, reliability and availability | 16 |
| 7.10 Internationalization..... | 16 |
| Bibliography..... | 17 |

Recommendation ITU-T X.1250¹

Baseline capabilities for enhanced global identity management and interoperability

1 Scope

This Recommendation describes baseline capabilities for enhancing global identity management and interoperability using public telecommunication networks and services. These baseline capabilities are grouped into functional areas:

- Common, structured identity management models.
- Provision of attributes (including identifier), credential and capabilities.
- Discovery of identity service provider resources, capabilities, and federations.
- Interoperability among management platforms, identity service providers and provider federations, including identity service bridge providers.
- Security and other measures to mitigate identity threats and risks, including protection of identity resources, personally identifiable information and privacy.
- Auditing and compliance, including policy enforcement and protection of personally identifiable information.
- Performance, reliability, and availability of identity management capabilities.

Today's telecommunication/IT networks and services are very diverse, highly distributed, highly interconnected, yet substantially autonomous in identity management (IdM). While these networks and capabilities are evolving, their size and complexity may inhibit interoperability among IdM capabilities. For this reason, IdM capabilities in this Recommendation rely substantially on existing network capabilities and general models – including what are effectively best practices. However, to achieve global identity management and interoperability, this Recommendation describes an evolution path and how to build on existing capabilities, where possible. It also defines an identity bridge capability that can be employed in many IdM systems and support architectures to integrate existing IdM capabilities.

The implementation of IdM capabilities in individual countries is subject to requirements specific to the national jurisdiction.

NOTE – The use of the term "identity" in this Recommendation relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 claimant [b-ITU-T Y.2720] and [b-ITU-T X.811]: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

¹ This Recommendation may not be applicable in some countries due to their domestic legislation.

3.1.2 personally identifiable information (PII) [b-ITU-T Y.2720]: The information pertaining to any living person, which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information, even if the information does not clearly identify the person).

3.1.3 relying party [b-ITU-T Y.2720]: An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 agent: An entity that acts on behalf of another entity.

3.2.2 anonymity: The property that an entity cannot be identified within a set of entities.

NOTE – Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on.

3.2.3 attribute: Information bound to an entity that specifies a characteristic of the entity.

3.2.4 authentication: See entity authentication.

3.2.5 authentication assurance: Confidence reached in the authentication process that the communication partner is the entity which it claims to be or is expected to be.

3.2.6 binding: An explicit established association, bonding, or tie.

3.2.7 claim: An assertion made by a claimant of the value or values of one or more identity attributes of a digital subject, typically an assertion which is disputed or in doubt.

3.2.8 entity: Anything that has separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.2.9 entity authentication: A process to achieve sufficient confidence in the binding between the entity and the presented identity.

3.2.10 federation: An association of users, service providers and identity providers.

3.2.11 identifier: One or more attributes used to identify an entity within a context.

3.2.12 identity: The representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within context. For 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, which 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.

3.2.13 identity service bridge provider: An identity service provider that acts as an intermediary among other identity service providers.

3.2.14 identity management: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes);
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and
- supporting business and security applications.

3.2.15 identity service provider: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.2.16 identity pattern: A structured expression of attributes of an entity (e.g., the behaviour of an entity) that could be used in some identification processes.

3.2.17 manifestation: An observed or discovered (i.e., not self-asserted) representation of an entity. (Compare with assertion.)

3.2.18 pseudonym: An identifier, whose binding to an entity is not known or is known to only a limited extent, within the context in which it is used.

3.2.19 requesting entity: An entity making an identity representation or claim to a relying party within some request context.

3.2.20 terminal object: An object (such as a SIM card) which may have a relationship to a network terminal device (such as a mobile phone).

3.2.21 trust: The firm belief in the reliability and truth of information; or in the competence of an entity to act appropriately, within a specified context.

3.2.22 user: Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

3.2.23 user-centric: An IdM system that can provide the (IdM) user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including PII, between entities.

4 Abbreviations

This Recommendation uses the following abbreviations:

| | |
|------|-------------------------------------|
| DHCP | Dynamic Host Configuration Protocol |
| ID | Identifier |
| IdM | Identity Management |
| IdSP | Identity Service Provider |
| IT | Information Technology |
| NGN | Next Generation Network(s) |
| PII | Personally Identifiable Information |
| RFID | Radio Frequency IDentification |
| SIM | Subscriber Identity Module |
| URL | Uniform Resource Locator |

5 Conventions

None.

6 General

The growth and evolution of communications capabilities has enabled the proliferation of numerous consumer, business, and government e-services. Communications are no longer just a resource to browse for information, the Internet protocol based communications technologies, such as NGN, are becoming an indispensable enabler for conducting daily e-transactions.

The capabilities described in this Recommendation are intended to support the development and deployment of structured and interoperable identity management capabilities under a common framework for all telecommunication/IT network and service systems, subject to regional and national policies concerning personally identifiable information and privacy.

The capabilities described in this Recommendation include:

a) **Examples of common, structured identity management models**

Identity management usually involves an exchange between entities of one or more identities using a telecommunication/IT network or service. In order to meet a desired authentication assurance level, the parties may decide or be required to communicate additional information among themselves or a third party. The initial communications exchange may contain an expression of a preferred authentication process or a delegation. One or both of the parties in the exchange may also choose to remain anonymous or to use pseudonyms. These kinds of interactions can be represented by common models – for which the capabilities are described further in this Recommendation. These models allow for multi-party provisioning of Identity capabilities, if desired or required. The models are also important for implementing interoperable IdM capabilities described and supported across networks, such as NGNs.

b) **Provision and protection of credential, identifier, attribute, and pattern identity capabilities with known assurance levels**

These identity information categories and their provision, maintenance, use, revocation and/or protection to desired assurance levels are common to identity management activities.

c) **Discovery of identity service provider resources, capabilities, and federations**

A critical IdM challenge in the very dynamic and diverse world of network capabilities and applications is discovering current identity sources and the services they provide. Discovery capabilities are often needed to meet the desired assurance levels.

d) **Interoperability among identity platforms, providers and identity federations, including identity service bridge providers**

In a highly distributed public network and capabilities infrastructure with large numbers of nomadic users and providers, identity management may involve large numbers of queries and responses among diverse parties and federations within which they may operate. Global interoperability among parties providing identity management capabilities is essential, and includes common protocols for instituting queries to identity capabilities.

e) **Security and other measures for mitigating identity threats and risks, including protection and control of identity resources and personally identifiable information**

Because identity information and resources are valuable, sensitive, and vital components of networks, especially those considered to be part of a critical national infrastructure, and affect personal privacy, the identity information and resources require security protection that is based on a risk analysis of the IdM environment.

f) **Auditing and compliance, including policy enforcement and protection of personally identifiable information**

Identity management provisioning is usually subject to a variety of legal, regulatory, government, and business requirements that necessitate some level of auditing and compliance capabilities. Such capabilities are wide ranging, including: auditing for compliance to regulations, measures for the protection of personal identifiable information, notices to consumers, and maintaining appropriate time-stamp accuracy and traceability.

g) **Useability and scalability: performance, reliability, availability, internationalization, and disaster recovery**

Identity management capabilities are useable and scalable to accommodate the constant highly distributed evolution of identity systems. Because identity information and resources form the basis by which entities authenticate each other, i.e., accept each other as communication partners, they are often components of the critical infrastructure and may need to adhere to specific levels of performance, reliability, availability and capabilities.

7 Capabilities for global identity management and interoperability

This clause provides examples of possible identity management transaction models; develops interoperable set of identity management (IdM) capabilities and basic identity components. This clause also discusses the discovery of identity capabilities, interoperability and bridging, IdM security, protection, control and use of personally identifiable information (PII), auditing and compliance. The work also considers internationalization, and performance, reliability and availability.

7.1 Examples of possible identity management transaction models

One of the primary transactions in identity management is the basic query-response process common to most structured information exchange shown in Figure 1. The most basic form of message exchange involves two parties using an agreed-upon protocol and information model.

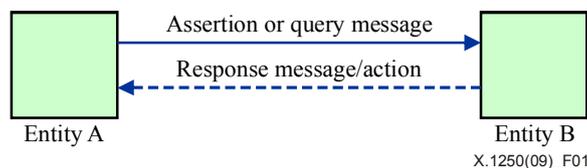


Figure 1 – Basic query/response information exchange process

The parties that participate in this process may be any kind of entity. An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. They can be any physical or virtual object, such as network equipment, software, terminal devices, sensors, actively tagged physical objects (e.g., using RFIDs or optical codes), passively tagged objects. Network devices, for instance, may be treated as entities subject to special IdM capabilities on behalf of end users, providers, and governmental authorities. In the context of digital rights management, the entity may be intellectual property or copyright protected material, such as multimedia or IPTV content. A special type of entity is the group. The group's identity is the intersection of the identities (common attributes) of the group members.

Most identity management use cases involve complex models. For example, where the relying party who originally receives the claim is not the identity service provider, and as illustrated in Figure 2a or 2b, the function of being an identity service provider is separate and distinct from the relying party; the relying party evaluates the responses from the identity service provider(s) and decides whether there is a sufficient level of entity authentication assurance. The primary function of an identity service provider is to manage the creation, update, verification, suspension, and deletion of identity information.

There are many possible identity information exchange models. One model in common use is a three-party query response model shown in Figure 2a. Some of the new open IdM protocols are predicated on this model.

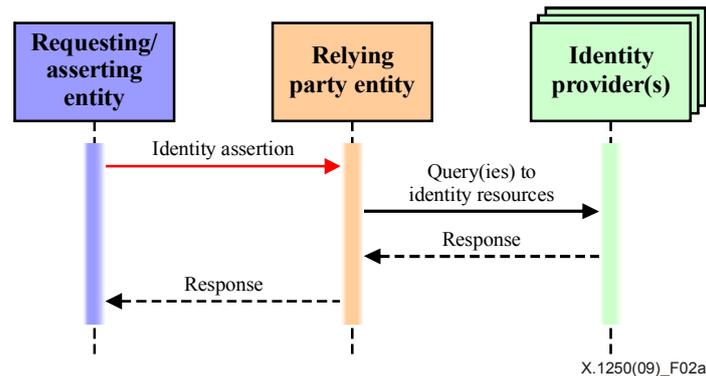


Figure 2a – An example of a three-party identity management model

Another identity management model that provides the requesting party with more control of the identity relationships is depicted in Figure 2b.

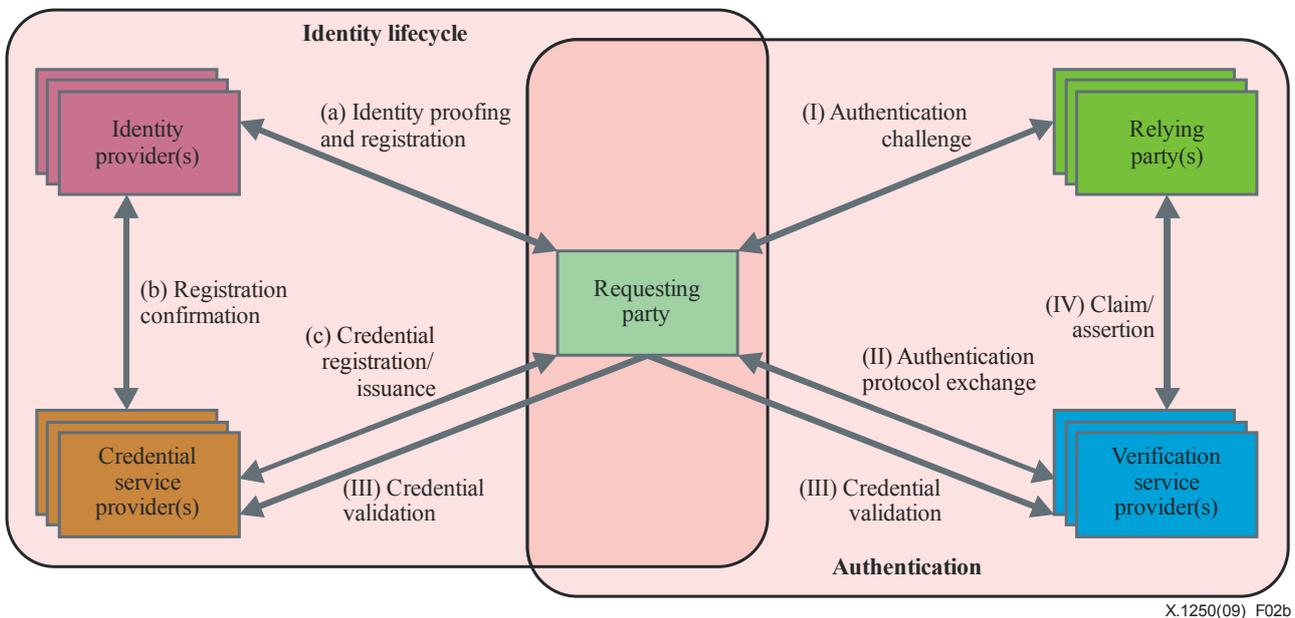


Figure 2b – An example of a user-centric five-party identity management model

"User-centric" models (i.e., that require full requesting party control be enabled over use of their identities) are receiving significant attention and may also be mandated in national and regional jurisdictions. Figure 2b shows an example where specialized roles and capabilities for identity management are provided by different service providers. All queries/responses are directed through the requesting party. For the purposes of these kinds of model, the entities are defined as:

- **Identity provider:** An entity that maintains and manages, and may create, trusted identity information of other entities (e.g., end user, organizations, and devices) and offers identity-based services. This entity responsible for assigning and issuing attributes (i.e., involving the identity (e.g., for a subscriber to a credential provider) for a specific context) – also described as enrolment – is responsible for the lifecycle management of the identity which includes proofing, registration and maintenance of the identity, including revocation.
- **Credential service provider:** The entity providing capabilities related to the issuance of credentials and tokens (e.g., credentials that bind tokens to verifiable identifiers and attributes).
- **Verification service provider:** The entity providing capabilities of assessing identity information (e.g., claims and credentials) and classifying its validity.
- **Relying party** [b-ITU-T Y.2720]: An entity that relies on an identity representation or claim by a requesting/asserting an entity within some request context.

In general the query-response activities can be grouped into two main categories:

a) Identity lifecycle

- **Identity registration and proofing (i.e., enrolment):** This information flow represents the inauguration of an entity into a specific context, i.e., the registration and proofing processes associated with the assignment of attributes which involve the identity of such entity within such context. For example, this may involve verifying and documenting proofs that a real person is associated with a subscriber name or pseudonym.
- **Registration confirmation:** This information flow represents interactions between an identity service provider and a credential service provider to confirm the registered identities.
- **Credential registration/issuance:** This information flow represents information exchange between the credential service provider and the requesting party to register an identity and obtain credential(s) binding tokens to a name or pseudonym and other attributes associated with the entity.

b) Authentication and assertion

- **Assertion:** This information flow represents information exchange between the relying party and the verification service provider to get a classification of the claim.
- **Authentication challenge:** This information flow represents a relying party challenging or prompting a requesting party for authentication. For example, the relying party may redirect the requesting party to a specific verification service provider, or the requesting party may choose a specific verification service provider.
- **Authentication protocol exchange:** This information flow represents exchange of protocol messages for authentication of the requesting party by the verification service provider.
- **Credential validation:** This information flow represents information exchange between the verification service provider and the credential service provider to validate credentials, if necessary.

The models present in this Recommendation are not exhaustive. They are intended to be flexible, and may include contexts where there are many identity service providers, as well as where the requesting or relying parties are also identity service providers.

c) **Assertion variations**

- **Delegation:** Assertion may also contain an expression of a preferred validation or a "delegation". An expression of a preferred validation informs the relying party about which identity service provider service to query, provided that the relying party can establish a chain of trust to the preferred identity service provider. Delegations provide a means to accommodate situations where an entity acts on behalf of another entity. Such delegations are commonplace, for example, where a parent may act for a child, an adult may act for another incapacitated adult, an employee may act on behalf of a company, or an attorney may act on behalf of a client, or the state on behalf of a citizen or vice versa.
- Delegations may be used to provide a delegated entity with some portion of the capabilities or authorized rights that are assigned to the entity with whom the identity is associated. In such circumstances, the relying party's query to the identity service provider might include additional requests to verify that the delegator has registered the delegate as a permitted agent. This request is in addition to authenticating the agent. Shared or delegated identity relationships may exist among many entities in these models. The extent of delegation chaining (i.e., delegation of a delegation) is subject to available technology as well as laws, regulations or business, federation, and legal policies.
- **Anonymity and pseudonymity:** An entity may also assert an anonymous or pseudonymous identity. In such cases, the level of identity assurance is dependent on extrinsic factors that the relying party would need to take into consideration, as no level of entity assurance may be achievable. Anonymity and pseudonymity may be used where the kind of activity involved does not require actual verification (e.g., where the activity is so trivial that any kind of identity management overhead is not needed). In addition, some laws, regulations or data protection policies may require the use of pseudonymity or anonymity.

7.2 An interoperable set of identity management (IdM) capabilities

Identity management has emerged as a common capability for all layers of basic network models such as found in NGNs [b-ITU-T Y.2012], [b-ITU-T Y.2720]. IdM capabilities are used in the applications portion, for network service control, as part of the underlying transport function, and in the management capabilities that are used to administer these layers.

A lack of coordination frequently exists among these layers for identity management. To the extent appropriate under regional or national policies, interoperable IdM capabilities should be supported in each network stratum.

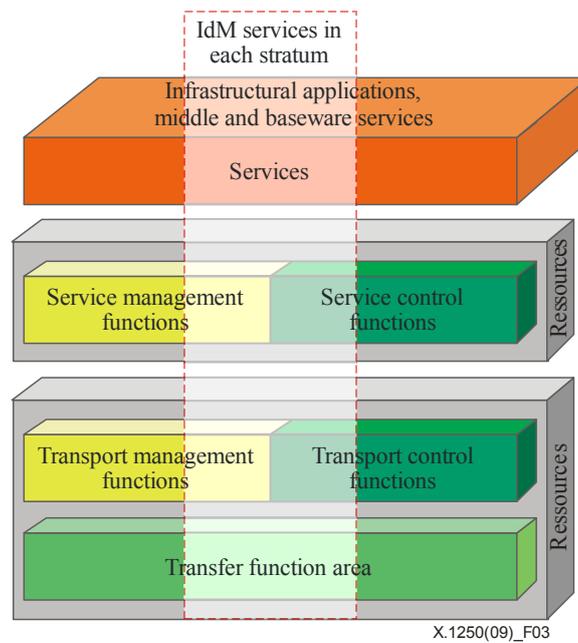


Figure 3 – Scope of identity management network strata interoperability

Figure 3 shows that IdM-related capabilities may exist in all of the vertical layers of the network architecture, and that there is a need for both synchronization and harmonization.

7.3 Four basic identity components

For the purpose of facilitating interoperable IdM capabilities, this Recommendation subdivides identity information into the following four basic categories:

- identifier capabilities,
- credential capabilities,
- attribute capabilities,
- pattern capabilities.

Aggregations of each of the four categories of identity information can be used to support more granular levels of identity assurance, and may be provided as identity capabilities either individually or in some combination by different entities as depicted in Figure 4. The depiction can be regarded as an extension of those found in Figure 2. The query-response model is typically used. It is not necessary that all of these identity capabilities be used in an IdM implementation. Their use – and existence as capabilities – depends on the IdM context – especially the level of entity authentication assurance desired or required.

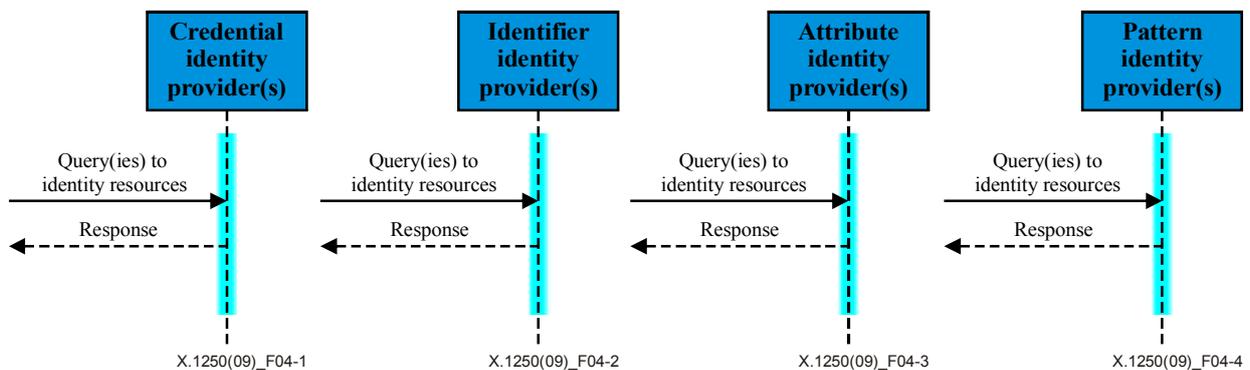


Figure 4 – An example of four basic identity query-response capabilities

The distinctions among these identity capabilities may be functionally blurred. For example, credentials have their own identifiers, and providers maintain some attribute information about the associated identity to which the credential pertains, and the provider may maintain a log-file concerning the credential's use that is used for pattern analysis to minimize identity theft and fraud.

IdM providers in many implementations, such as telecommunication/IT or financial service providers or an institution or organization with a special relationship with an end user or customer, may also provide all these capabilities as a unified bundle. The extent of "IdM openness" and interoperability with IdM providers is a decision based on trust and similar needs, business relationships, and regulatory or legal requirements.

7.3.1 Identifier capabilities

Identifiers are attributes (e.g., names) generally assigned to an entity for information systems management or communications addressing purposes. As such, they usually have a specialized use. For example, telephone numbers, URLs, e-mail addresses are used for both service/device access or routing via communications networks.

7.3.2 Credential capabilities

Credentials are used to support the authentication of entities – either one or both parties to an information exchange or transaction. One of the earliest and still most widespread forms of certificate credential is based on ITU-T X.509 digital certificate standard [b-ITU-T X.509]. Other forms of credentials include government-issued credentials, such as employment related badges, mobile wireless SIM cards and financial institution credit or automatic teller machine (ATM) cards.

Sometimes, credentials also encompass biometric representations. Some applications require the ability to support the rapid verification that credentials are valid and have not been revoked. However, it must be considered that credential checks may result in a lot of tracing information with the IdSP, which may be a privacy risk. Therefore, strong credentials, which do not require checks, are important.

The complexity of using and managing digital credentials by the general public on a broad scale may be reduced through the adoption of user-centric IdM approaches, combined with credential management capabilities such as digital wallets [b-ITU-T X.1251]. Depending on the context, credential support may include an ability to use a variety of credentials to meet different required entity authentication assurance levels.

7.3.3 Attribute capabilities

As characteristics of entities, attributes are often relatively static – captured as part of the credential or identifier assignment process (e.g., names, physical address, contact information, etc.). In other cases such as a current geospatial location, attributes can be highly dynamic.

Attribute discovery and query capabilities may require specialized interoperable protocols. Such protocols generally support some manner of verification – especially where PII is involved, for the protection and control of personally identifiable information. User-centric interoperable protocols and platforms may also provide a means for the end-user to designate the manner in which attribute information is to be treated.

7.3.4 Pattern capabilities

Identity patterns are a structured expression of attributes of an entity that could be used in some identification processes.

They may consist of observed or discovered (i.e., not claimed or asserted) identity, e.g., reputational or transactional information associated with an entity. It is often especially important to detect identity theft. Specialized pattern identity capabilities are also used to support cybersecurity capabilities, such as the pattern signature of a virus or infrastructure attack.

Like attribute identity capabilities, when the patterns involve real persons, the provision also invokes a potential significant expanding and sometimes conflicting array of federation and potential legal and regulatory requirements – especially for the protection of personally identifiable information. In some jurisdictions, if PII is involved, pattern data retention and analysis capabilities are subject to significant data protection and privacy policies, including prohibition of data collection and mechanisms for deletion of the data.

7.3.5 General IdM data management capabilities

A number of IdM capabilities apply to IdM system management and the management of IdM data for all the identity capabilities. Capabilities include support for:

- the ability of a requesting party to access/delete/modify/monitor/control its own identity information, subject to laws, regulations and/or applicable policies;
- the ability of authorized entities (e.g., system administrators, parents, public safety, law enforcement, and other authorized third parties) to access/modify/monitor its identity information, subject to laws, regulations and/or applicable policies;
- the import/export of identity information, subject to laws, regulations and/or applicable policies;
- a mechanism to indicate some kind of information about the quality level of the information that they provide to relying parties. This requires an agreement between those parties, about the informative value;
- the ability for a requesting party to delegate the management of its identity information to another entity;
- lifecycle management for all identities, including a means for rapidly verifying the current status of information, subject to laws, regulations and/or applicable policies;
- a common mechanism to identify and control the dissemination of all identities, subject to laws, regulations and/or applicable policies.

7.3.6 Entity assurance levels

Resources and provisioning have associated assurance levels that vary significantly depending on a large number of technical and administrative factors, which conform to policies and standards appropriate for the context.

Capabilities include support for:

- indicating the assurance levels of public identifier information, especially for registration authorities for public communications, including assignees sub-allocating identifiers in hierarchical name and numbering systems;
- a mutual protocol indicating levels of assurance associated with the information provided. Common global, open, mechanisms are recommended;
- a mechanism for a requesting party, relying party, or e.g., identity service provider to specify the assurance and validity conditions for an identity service, and specify what action is to take place if the conditions are not met.

7.4 Discovery of identity capabilities

A critical IdM challenge in the very dynamic and diverse world of network capabilities and applications is discovering sources for each of the four core IdM capabilities. There are enormous distributed, autonomous, sources available. It is not sufficient for IdM capabilities to simply exist. Relying parties need standard means to learn of their existence and how to reach them as illustrated in Figure 5, below. The discovery process may require the support of a new discovery protocol, similar in nature to the dynamic host control protocol where a client can discover a DHCP server

and acquire an IP address and gateway information. Thus, the discovery process may be as simple as the identity holder providing a valid URI or OID to the relying party.

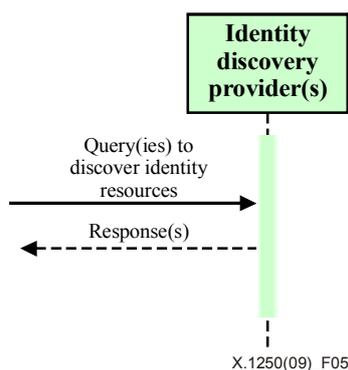


Figure 5 – Example of identity discovery query-response capabilities from any entity

In addition, the discovery of identity capabilities should include the discovery of capabilities available through federations. Some federations and communities using specified protocols have developed partial solutions to meet discovery needs within the boundaries of their user communities. However, there is currently no means for global or inter-federation discovery. A system that supports discovery is desirable. Desirable discovery capabilities include support for:

- identity service provider business agreement policies across federation or domains;
- single sign on/single log out, and publish this capability in a standard way, so that it becomes discoverable.

7.5 Interoperability and bridging

Global interoperability among parties providing identity management resources is an essential provisioning requirement. This clause describes capabilities for instituting queries within a federation or through a bridge provider.

Federations are based on a principle of mutual acceptance of authentication results between the participating domains, not on a sharing of identity information between those domains.

7.5.1 Federation-related capabilities

Federation-related capabilities include:

- a relying party's ability to establish an authentication (i.e., security) domain through alliances and participation in federations;
- obtaining authorization from the requesting party to federate the requesting party's identities, subject to laws, regulations and applicable policy;
- the ability for a requesting party to delegate authority to federate its identity, subject to laws, regulations and applicable policy.

7.5.2 Identity bridge related capabilities

Identity bridge related capabilities include:

- the ability for a requesting party to be able to set permissions and prohibitions regarding identity bridging capabilities;
- a mechanism to discover the identity service provider of the related requesting party;

- a mechanism for identity bridging to:
 - a) allow federation of requesting party accounts at an identity service provider and a relying party in different authentication domains provided each has appropriate permissions from the requesting party and identity service bridge provider; and
 - b) convey the address of an identity service provider in a response message to a relying party;
- a mechanism to accomplish interoperability of the requesting party information obtained from one identity service provider and allowing it to be recognized and used by the related identity service provider and relying parties in different domains (e.g., two networks);
- where a federation is created through an identity service bridge provider, a means to notify the relying party or an identity service provider when a change occurs in the identity service bridge provider's policies. This mechanism allows the relying party or an identity service provider the option of terminating its participation in the federation;
- where a federation is created through an identity service bridge provider, a means to notify the requesting party when a change occurs in the identity service bridge provider's policies. This mechanism allows the requesting party of terminating the acceptance and participation in the federation.

7.6 IdM security

Because identity information and the network resources that provide identity capabilities are valuable, sensitive, and vital components of networks, especially those considered to be part of a critical national infrastructure, they will require security protection. Securing an IdM infrastructure encompasses administrative policies, operating practices, technologies, and techniques to prevent the compromise of IdM systems and data, whether it be stationary or in transit.

This clause supplements security best practices found in [b-ITU-T X.1205] with several capabilities to help secure IdM infrastructures that include:

- secure transactions (e.g., with confidentiality, integrity, anti-replay protection) between all parties (requesting party, relying party, identity service provider);
- mechanisms for non-repudiation of IdM transactions;
- secure discovery of identity capabilities, for example, to protect against identity service provider impersonation;
- security information for auditing IdM transactions;
- implementation of capabilities to detect and respond to intruder activity based on IdM transaction analysis and possibly to alert identity owners about suspected attacks on their identity information;
- implementation of means to allow relying parties to rapidly inform identity service providers about identity compromise and secure this reporting capability from exploitation.

Usage policies and directives – also sometimes referred to as "identity governance" – are also important measures in a multi-identity service provider environment to mitigate threats and risks, as well as to protect personally identifiable information. Where federations, alliances, or bridge providers are involved, these measures may be promulgated by all participating relying parties and identity service providers. The increasing use of user-centric IdM applications may also enable requesting end users to specify policies that have a binding to their identity attributes, as described and recommended in clause 7.7. The implementation of common security capabilities among those participating in a federation has significant benefits, and federations should have well-developed security specifications.

Desirable IdM security and policy capabilities include:

- entity authentication assurance capabilities in accordance with applicable guidelines;
- a non-repudiation mechanism for IdM transactions;
- the dynamic establishment of time-limited mechanisms for transient and changing relationships. This may require a mutually trusted bridge provider belonging to one or more federations;
- security between federations, including negotiation mechanisms for secure inter-federation communications and the exchange of information between federations in response to cybersecurity threats;
- enabling applications on terminal objects to have a means to authorize access to end user identity information of the terminal object, subject to laws, regulations and applicable policy;
- a mechanism for notification to be sent from the relevant identity service provider to all affected parties in the event that an identity is reported compromised or revoked;
- a secure method to learn of identity capabilities;
- logging of security information for IdM transactions with sufficient detail to establish accountability and enable forensic analysis;
- intrusion detection and response capabilities for IdM transactions;
- mechanisms to allow relying parties to report identity compromise.

7.7 Protection, control and use of personally identifiable information (PII)

There are several facets to safeguarding personally identifiable information. Two of them include the use of security capabilities in the IdM infrastructure, and the use of capabilities that provide transparency and notice to entities concerning the use of their identity information coupled with the ability to bind their preferences to that information. In this context, "binding" consists of some persistent mechanism that enables a third party possessing the identity information to discover the associated entity's PII policy capabilities. Increasingly, both user-centric product platforms as well as identity service bridge provider capabilities allow for these kinds of preferences to be implemented.

In some national and regional jurisdictions, PII must be collected fairly, and according to an explicit and legitimate end purpose. The related information exchanged between communicating parties should be limited to the data that is needed to allow the relying party to provide a service or a resource to a requesting party.

From a privacy point of view, in some national jurisdictions, there are a number of principles which have to be taken into account:

- binding PII must be collected for specific, explicit and legitimate purposes, and not further processed in a way that is compatible with those purposes;
- PII must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- PII must be accurate and kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- PII must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed;
- PII should not be shared between applications for different purposes;

- PII must be limited to the minimum needed for a specific purpose;
- PII must be secured. Appropriate technical and organizational measures must be taken to protect PII against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;
- persons have the right to access, rectify or erase PII related to them;
- PII must not be kept for longer than necessary for its defined purposes.

Other jurisdictions require protection mechanisms including the use of notifications whenever an account is accessed or information is changed. Use of PII in telecommunication/ICT networks and services should be done according to an explicit end purpose. It is with regard to this end purpose that one can appreciate the relevant, adequate and non-excessive nature of the data recorded, the categories of persons or organizations who may receive these data, and the duration for which the collected data may be stored.

Capabilities include:

- collection, processing and protection of PII in accordance with data protection and privacy principles and legislation. At a minimum, the protections should include those specified by the OECD as global privacy guidelines. Regional/national applicable regulations may impose additional mandatory requirements for compliance (e.g., European Data Protection Directive 95/46/EC);
- securing and protecting recognized limits to minimize the collection of personally identifiable information. The PII should be obtained for specified, explicit and legitimate purposes, only with the consent of the data subject;
- features such that, when an identity service provider has separately federated a requesting party's identity with two or more relying parties, it should not be possible for the relying parties to use information given to them by the identity service provider to determine that the identities refer to the same requesting party;
- a notification service when requesting party's attributes change;
- a notification service when requesting party's consent declarations change;
- provision to alert identity owners to IdM transaction activity interpreted by the identity service provider as an attempt to compromise their identities;
- provision to notify identity owners of the compromise of the identity service provider's systems and capabilities;
- the ability to enforce duration limits on the storage of PII, so that it is not kept for longer than its defined purposes;
- the ability of related entities to check, correct and delete the related PII according to laws, regulations and policies.

7.8 Auditing and compliance

IdM is subject to a variety of legal, regulatory and industry business requirements that may necessitate some level of auditing and compliance. Examples of auditing and compliance measures include maintaining security logs, protecting and appropriately using personal information, and providing notice to entities to which the information applies. Auditing should comply with PII protection capabilities described in clause 7.7, above, especially due to the fact that another new party may be involved and can result in a conflict to privacy laws, regulations and policies.

Capabilities include:

- mechanisms, to enable forensic analysis;
- mutual and secure mechanisms to exchange identity management auditing information;

- time-stamping;
- context-dependent timestamping of records, according to the importance of the audited information and the time value;
- care must be taken to ensure that identity management auditing implementations meet applicable privacy requirements.

7.8.1 Timestamp accuracy capabilities

Accurate timestamps are very important for managing identity lifecycles and for maintaining security within IdM systems, as all identity information exists within bounded time-frames. Auditing describes the occurrence of events within those time-frames. For auditing purposes, timestamps are essential, and the quality, if not the usability of audit data, is determined by timestamp accuracy at the appropriate event locations to sufficiently audit highly asynchronous and distributed network and application capabilities. Desirable capabilities include timestamp accuracy capabilities sufficient for auditing at agreed common reference locations, appropriate to a mutually agreed level of assurance.

7.9 Performance, reliability and availability

IdM is an important network capability that needs to be designed and implemented to achieve performance, reliability, and availability objectives. It is recommended that IdM reliability and availability objectives be comparable to other critical network functions because IdM forms the core of authenticating and authorizing access and all transactions in the network. This means, for instance, ensuring that IdM power, environmental support, and connectivity objectives are sufficient. IdM performance (e.g., query response time) should meet the expected IdM query loads.

Availability of an IdM system is not homogeneous across all components (issuing elements, look-up elements, revocation elements) and must be ultimately linked to the assurance level in the credential. The following availability requirements are desirable, but will differ among the building block components (repository, enrolment system, revocation capability):

- reliability and availability at levels comparable to other critical network elements, systems and capabilities;
- incorporation of IdM capabilities in provider disaster recovery plans;
- IdM implementations that provide reasonable response times for IdM transactions.

7.10 Internationalization

For global interoperability, support for the use of diverse character sets and languages is necessary. Internationalization objectives are recognized as an important design and support requisite for all public network-based applications, including IdM capabilities.

Bibliography

- [b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- [b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications.*
- [b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*
- [b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*
- [b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity.*
- [b-ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture.*
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*
- [b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*
- [b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*
- [b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.*

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 | 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 |
| Series Z | Languages and general software aspects for telecommunication systems |