

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1251

(09/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

A framework for user control of digital identity

Recommendation ITU-T X.1251



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.1251

A framework for user control of digital identity

Summary

Recommendation ITU-T X.1251 defines a framework to enhance user control and exchange of their digital identity related information. This Recommendation also defines user and functional capabilities of the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

Source

Recommendation ITU-T X.1251 was approved on 25 September 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

Keywords

Digital contract, digital identity, digital identity client, identity, identity interchange, identity management, identity server.

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/>.

© 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 Terms and definitions	1
3.1 Terms defined elsewhere.....	1
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions.....	3
6 General capabilities	4
6.1 User capabilities	4
6.2 Functional capabilities.....	4
6.3 Security guidelines	5
7 Enhanced user control of digital identity interchange.....	5
7.1 Introduction	5
7.2 Security threats	6
7.3 Conceptual model for digital identity interchange	6
7.4 Digital contract	8
7.5 Three layers for identity interchange.....	9
8 Digital identity interchange framework.....	10
8.1 Design principles	10
8.2 Framework components	11
Appendix I – Reference implementation guideline for a framework for user control of digital identity using WS-trust and Information Card technology	14
I.1 Introduction	14
I.2 Background.....	14
I.3 DIIF capabilities	15
Bibliography.....	18

Recommendation ITU-T X.1251¹

A framework for user control of digital identity

1 Scope

This Recommendation defines a framework to enhance user control and exchange of their digital identity related information.

This Recommendation also defines capabilities for the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

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

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.2 entity [b-ITU-T X.1252]: 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, software application, 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.

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

3.1.4 identifier [b-ITU-T X.1252]: One or more attributes used to identify an entity within a context.

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

3.1.5 identity [b-ITU-T X.1252]: 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.

3.1.6 identity management [b-ITU-T Y.2720]: 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
- enabling business and security applications.

3.1.7 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.

3.1.8 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).

3.1.9 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.

3.1.10 user [b-ITU-T X.1252]: Any entity that makes use of a resource e.g., system, equipment, terminal, process, application, or corporate network.

3.1.11 user-centric [b-ITU-T X.1252]: 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 circle of trust: 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.

3.2.2 digital contract: A contract made in digital form and signed by two entities between whom an agreement is reached.

3.2.3 digital identity: The digital representation of the information known about a specific individual, group or organization.

3.2.4 digital identity client: A client program that provides authentication and credential management, identity interchange and privacy protection service to the user.

3.2.5 identity fraud: A crime in which an impostor obtains key pieces of personally identifiable information (PII) such as social security numbers and driver's license numbers and uses them for his own personal gain.

3.2.6 identity information: The information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses.

3.2.7 identity interchange: A process of disseminating user's identity information between an identity service provider and a relying party through a digital identity client.

3.2.8 identity selector: A software component in a digital identity client available to the user through which the user controls and dispatches his/her digital identities.

3.2.9 identity server: A server that manages the user's credential and identity information and provides it to a digital identity client.

3.2.10 identity synchronization: A process of updating disseminated user's identity information to a relying party when the source of the identity information in an identity service provider is changed.

3.2.11 identity termination: A process of deleting user's identity information from a storage when the validity of it is expired.

3.2.12 identity token: A data model for the digital identity, which can contain a user's PII and credential information.

3.2.13 phishing: The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

3.2.14 privacy policy: The policy statement that defines the rules for protecting access to and dissemination of personal privacy information.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CoT	Circle of Trust
DIC	Digital Identity Client
DIIF	Digital Identity Interchange Framework
IdM	Identity Management
IdS	Identity Server
IdSP	Identity Service Provider
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RP	Relying Party
SP	Service Provider
XML	eXtensible Markup Language

5 Conventions

None.

6 General capabilities

This Recommendation defines the following set of capabilities. The capabilities specified in the user and functional parts below are mandatory unless indicated as optional.

6.1 User capabilities

The following are required to satisfy user's capabilities:

- 1) Support for mutual authentication mechanisms.
- 2) Provision of a consistent authentication interface to support various authentication mechanisms with a digital identity client (DIC).
- 3) Provision of an identity selector that allows the user to choose which credential is going to be used for authentication. The choice of the credential to be used for authentication might also be constrained by some website's requirements. For the user's convenience, the choice of the authentication method and associated credential might also be delegated to the identity service provider (possibility for the user to only choose an identity service provider and not specifically a particular credential to be used to authenticate at that identity service provider).
- 4) Provision of an intuitive and consistent interface to manage his/her credential information with maximum security.
- 5) Support for auto fill-in registration or subscription of a website to minimize the user's interaction with the site including the user's full control to activate and deactivate such mechanisms. This is optional.
- 6) Provision of identity information at any time a user wishes and allows the user to fully control the identity interchange with an appropriate privacy protection mechanism.
- 7) Provision of automatic updates for shared identity information when the original source is changed under his/her full control.
- 8) Provision of full user control over how the security and privacy policies are established and how they are enforced to control identity interchange before sharing identity information so that the user can have a direct influence on establishing a policy and enforcing it.
- 9) Provision for users to view the details of identity information they share with each entity.
- 10) Support for authentication session management capabilities to avoid the user having to systematically re-authenticate at an identity service provider in order to access websites.

6.2 Functional capabilities

The functional capabilities for the digital identity interchange framework are defined as follows. These functional capabilities are required to provide the minimum functions needed for the digital identity interchange framework.

- 1) Support integrated credential management that can manage the user's credential information for authentication.
- 2) Support identity interchange link management to provide a user with a full-scale view of the entities with which the user has connections for identity interchange.
- 3) Support multiple authentication mechanisms, which can include password-based, PKI-based, and biometric-based authentications.
- 4) Support identity interchange mechanisms that can provide a bidirectional link to share the user's identity information between entities using DIC.
- 5) Support the digital contract mechanism to establish a contract for identity interchange and to be used to enforce the security and privacy policies for the release of PII.

- 6) Support identity information synchronization to update the distributed and shared identity information consistently when the source of disseminated identity information is changed. Identity information that needs to be synchronized is restricted to PII that is changed by a user directly.
- 7) Support universal token transformation to make the framework interoperable with existing identity management systems.
- 8) Make the framework as agnostic as possible to the authentication process in order to avoid dependencies between DIC and supported authentication mechanisms at identity service providers (or at least make the framework so that it easily supports all authentication mechanisms, especially telecom operator's specific ones).
- 9) Support mechanisms to enable the identity service provider to interact with the user during the authentication process and provide its own authentication interface (GUI).
- 10) Support storage of identity tokens on various media (USB dongle, SIM card, network-based storage service, etc.) with a well-defined storage layer to be used by DIC.

6.3 Security guidelines

In order to develop secure DIIF, the following security guidelines are recommended:

- The security of DIIF communication will depend on the underlying trust model, which is typically based on key management infrastructure (e.g., PKI or secret key).
- Some form of transport layer security protocol should be used to provide data integrity and confidentiality (e.g., by encryption) when the message is transported by a network.
- The digital contract should be digitally signed by the parties reaching an agreement; it could be encrypted as an option if necessary.
- Data including identity information stored in DIC should be digitally signed and encrypted while in storage.
- Since a user is allowed to move its identity token from one device to another, there must be a policy to maintain data security while the data is in transit.

7 Enhanced user control of digital identity interchange

7.1 Introduction

Identity federation [b-LA-FF] has been introduced to connect distributed identity information between an identity service provider (IdSP) and a service provider (SP). If the SP wants to assure authentication information from the IdSP, a trust relationship is required to exist between the two parties. This trust domain 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.

However, the number of authentications a user must undertake increases as the number of CoTs grows. In this situation, a user has to authenticate to the CoT every time the user visits. This means that the user has to manage credential information from an IdSP in a CoT. This often causes the user to forget the password or to write it down, which increases the risk of unauthorized disclosure. Federation within a CoT provides a convenient way to exchange a user's identity information. However, sharing identity information among CoTs requires a prior business agreement, which usually takes a long time to complete because of the legal procedures involved. If the domain for identity management is limited to the enterprise environment, then federation technology provides a feasible solution in an efficient and effective way. But if the domain of the identity management (IdM) system extends to the Internet, it is difficult to reach business agreements between enterprises for all federations.

In large scale application-focused IdM systems, it may be that identity services and policies are designed to satisfy requirements for IdSPs and SPs and optimized for the requirements of applications (e.g., provisioning user account information). When an identity service is provided for the user, the identity exchange usually takes place between an IdSP and a SP directly. In this case, a user has a limited control over the dissemination of their identity information.

Since the identity information is exchanged between enterprise entities without user intervention, security and privacy protection may be neglected. The problem occurs because two entities try to share the user's identity information, which belongs to the user. Since the two entities deal with the user's identity, they need to have a prior business and privacy policy agreement. If an entity only needs to share the user's identity with the original owner, then each entity only needs to make an agreement and establish a security and privacy policy with the owner for the use of his/her identity information (or with the entity that manages his/her identity).

In order to solve the problem, this Recommendation defines a framework to enhance user control when digital identity related information for the user is exchanged.

7.2 Security threats

Unless properly addressed, many of the threats appearing in cyber space are highly likely to exist in IdM systems. The general security threats in cyber space are described in [ITU-T X.1205].

In IdM systems, there are various security threats that make the system vulnerable or lead to a security compromise that puts an organization at risk. Identity fraud is one of the most common types of security threat to the IdM environment.

Identity fraud is a high-profile security issue, particularly for organizations that store and manage large amounts of personally identifiable information. Not only can compromises resulting in the loss of personal data undermine customer and institutional confidence and result in costly damage to an organization's reputation, but data breaches can also be financially costly to organizations. These days identity fraud can be triggered by phishing.

Phishing is an attempt by a third party to solicit confidential information from an individual, a group, or an organization by mimicking, or spoofing, a specific, usually well-known brand, usually for financial gain. A phishing website is a site designed to mimic the legitimate website of the organization whose brand is being spoofed. An attacker attempts to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, that he/she may then use to commit fraudulent acts. In IdM systems, phishing is a serious threat because the victim's authentication information or other personally identifiable information – when captured by an attacker – can be used in identity theft or other fraudulent activity.

7.3 Conceptual model for digital identity interchange

In this conceptual model, the digital identity interchange framework (DIIF) employs the concept of a digital identity client (DIC) that can control the interchange of digital identity information. The control that is given to the user to control the release of identity information can substantially mitigate security threats that are described in the security threats clause (see clause 7.2).

Figure 1 illustrates the conceptual model for digital identity interchange.

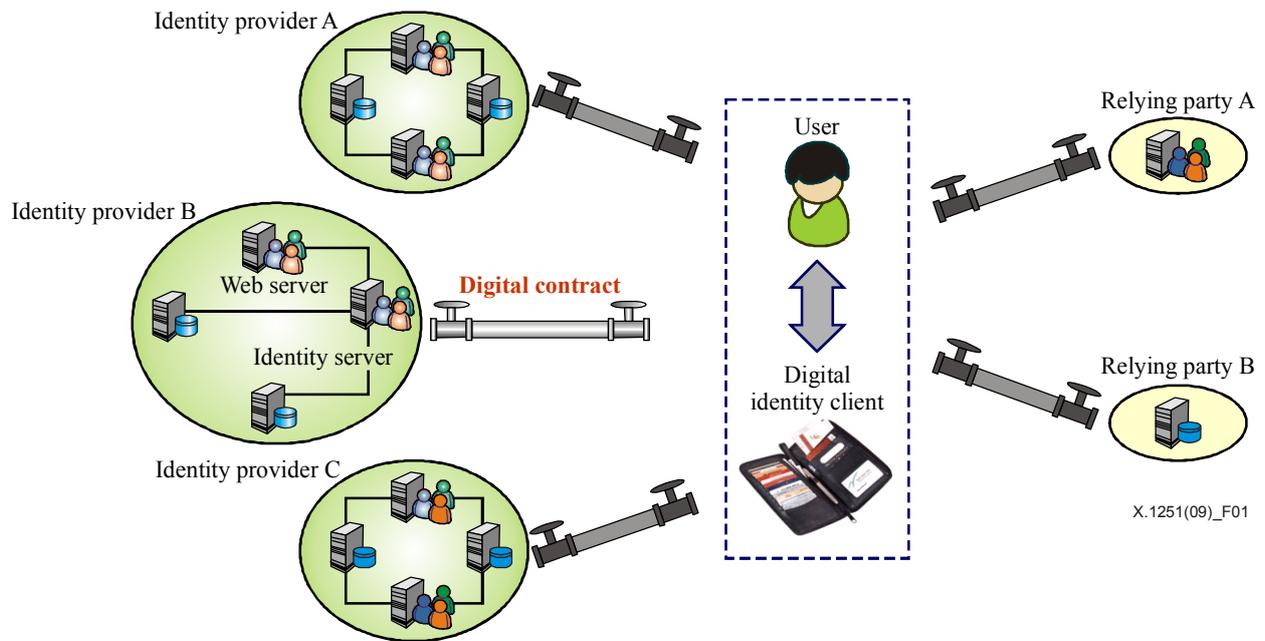


Figure 1 – The conceptual model for digital identity interchange

7.3.1 Identity server

An identity server (IdS) is the main server that provides the user's identity information to a requesting entity or requests identity information to a DIC for web services. The IdS can be an identity service provider if it provides identity information; otherwise, it can be a relying party (RP) if it consumes identity information that a user provides. It is possible that the role of an IdS can be both an identity service provider and a relying party. In this case, the IdS disseminates its own identity information for some web services while it requires user's identity information for some other web services. A web server can request an IdS to provide it with the user's identity information in order for it to provide a web service.

7.3.2 Digital identity client

The digital identity client is a program that provides authentication, credential and session management, identity interchange and privacy protection services to the user. If it needs to share identity information with an IdSP or RP, then the DIC establishes a link with the IdS in a domain. The DIC may contract with the IdS to describe the terms and conditions for the identity interchange service so that privacy and security aspects of identity information exchanged can be enhanced. Each user's identity information flows through the DIC so that the user in question can control the sharing of his/her identity information. In particular, depending on the policy agreed between a user and an entity, the user has full control over which identity data is exchanged for what purposes, for whom it is intended, and for how long it will be used. Discovery of the user's identity information is not necessary since the client has all the link information required to push and pull identity information.

7.3.3 Identity service provider

An identity service provider (IdSP) is the entity that manages user's identity information, provides authentication and authorization services and provides identity interchange services for web servers. An IdSP is the conceptual role model that can be assigned to the entity that manages the user's identity and provides such information when DIC requests it. The IdSP manages the identity information, which is submitted by a user or generated by itself.

7.3.4 Relying party

A relying party (RP) is another conceptual role model that is assigned to the entity that requests the user's identity from a DIC and provides a service using the received identity information. The RP does not rely on an IdSP for authentication. A user will use the DIC to be authenticated to the RP.

7.3.5 User

A user is defined in clause 3. In the conceptual model a user usually refers to a person or a subscriber in the user-centric IdM context. The user is the end user that owns and operates a DIC.

7.4 Digital contract

Personally identifiable information (PII) flowing between an identity service provider and a relying party must go through a digital identity client in a user-centric identity management environment. This provides a user with an opportunity to control the use of his/her PII. A digital contract is made only between a user and an IdSP or between a user and a relying party. Multi-party contracts are not allowed since they can complicate the management issues that a user needs to cope with. A digital contract is the core component that can provide fine-grained control for the user to control his PII flows. Figure 2 illustrates the structure of a digital contract.

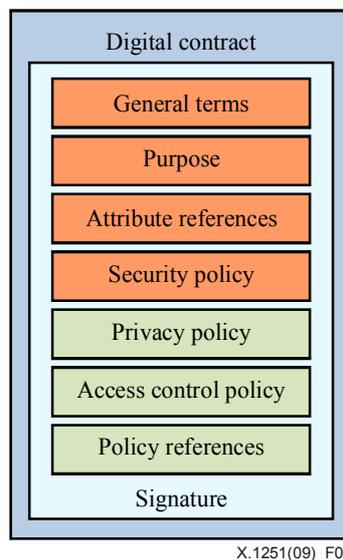


Figure 2 – The structure for a digital contract

The types of controls that digital contracts can define include any policies required to mediate an identity interchange relationship. Based on the regulations or other policy requirements, the digital contract may not be required at every identity interchange. It is only needed when the flow or caching of a shared PII needs to be controlled. This component is as flexible and extensible as real world contracts (e.g., non-disclosure agreements). Furthermore, since digital contracts can be XML documents themselves, they can govern their own revision, amendment, and deletion (i.e., real-world contracts). The elements of such a contract include:

- 1) General terms: Describing the version, agreement date, and validation date as well as any notice for a user. This is a mandatory element.
- 2) Purpose: The intended use for a user's PII. This is a mandatory element.
- 3) Attribute references: Indicating which attributes of an entity the contract refers to. This is a mandatory element.

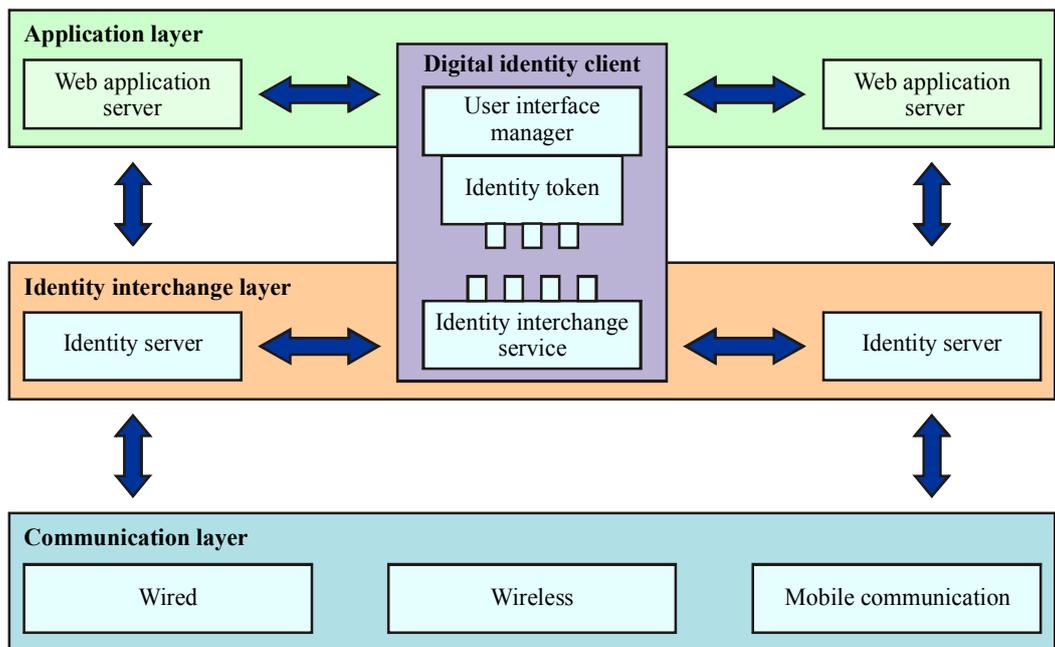
- 4) Security policy: This element is required to contain an authentication and information security policy that indicates how two entities can be authenticated and how information is secured. This is a mandatory element.
- 5) Privacy policy: The element can contain any kind of privacy policy statement. Synchronization and termination of user's disseminated PII's can be specified here. Privacy protection in accordance with applicable regional/national privacy legislation must be provided. Therefore, this is an optional element.
- 6) Access control policy: Any access control policy or authorization policy can be described in this element. This is an optional element.
- 7) Policy references: References to externally defined policies can be specified here. This is an optional element.
- 8) Signature: A contract can be made by two entities reaching an agreement on the content of the digital contract. However, the contract can have a maximum of two digital signatures, representing the two entities agreeing to the contract. However, for the reasons given in the first paragraph of this clause, there can be no more than two signatures. It must be signed by two entities for its validity and integrity. By signing the contract, a user gives consent. The effect of a signature covers from general terms to policy references as shown in Figure 2. This is a mandatory element.

7.5 Three layers for identity interchange

This clause defines three layers: the application, identity interchange and communication layers.

7.5.1 Application layer

The application layer may be a typical web application running in the Internet or in a mobile communication environment. For instance, a user uses a web browser to request web service from a web server. When an entity in the application needs to request an identity service or authentication, it calls the service provided in the identity interchange layer. Logically, the DIC is located in both the application and identity interchange layer connecting both layers to provide seamless identity-related services to a user. Every time a user tries to login to a website, the user calls the identity selector, which is a component of the user interface manager in the client, to select a token representing an identity to authenticate to the website. When a web application needs to share the user's identity information to deal with the user's service request, it can call one of the identity interchange services provided in the identity interchange layer. The location of a service description in the identity interchange layer is provided for administration of the web application.



X.1251(09)_F03

Figure 3 – Identity interchange layer

7.5.2 Identity interchange layer

The identity interchange layer provides a transparent identity interchange link layer to facilitate identity interchange between entities and to give a user full control in enforcing his/her security and privacy policies.

By introducing this layer, the sharing of identity information between various entities can be developed and deployed independently of any application since an application does not need to know the detailed operation of identity interchange. Furthermore, the identity interchange layer can provide various identity interchange-related functions to existing IdM solutions that do not themselves have identity interchange capabilities. The detailed description of how the identity interchange layer facilitates security and privacy policy compliance is given in the digital contract clause (see clause 7.4).

7.5.3 Communication layer

The communication layer is an independent layer that is responsible for transporting data from one device to another.

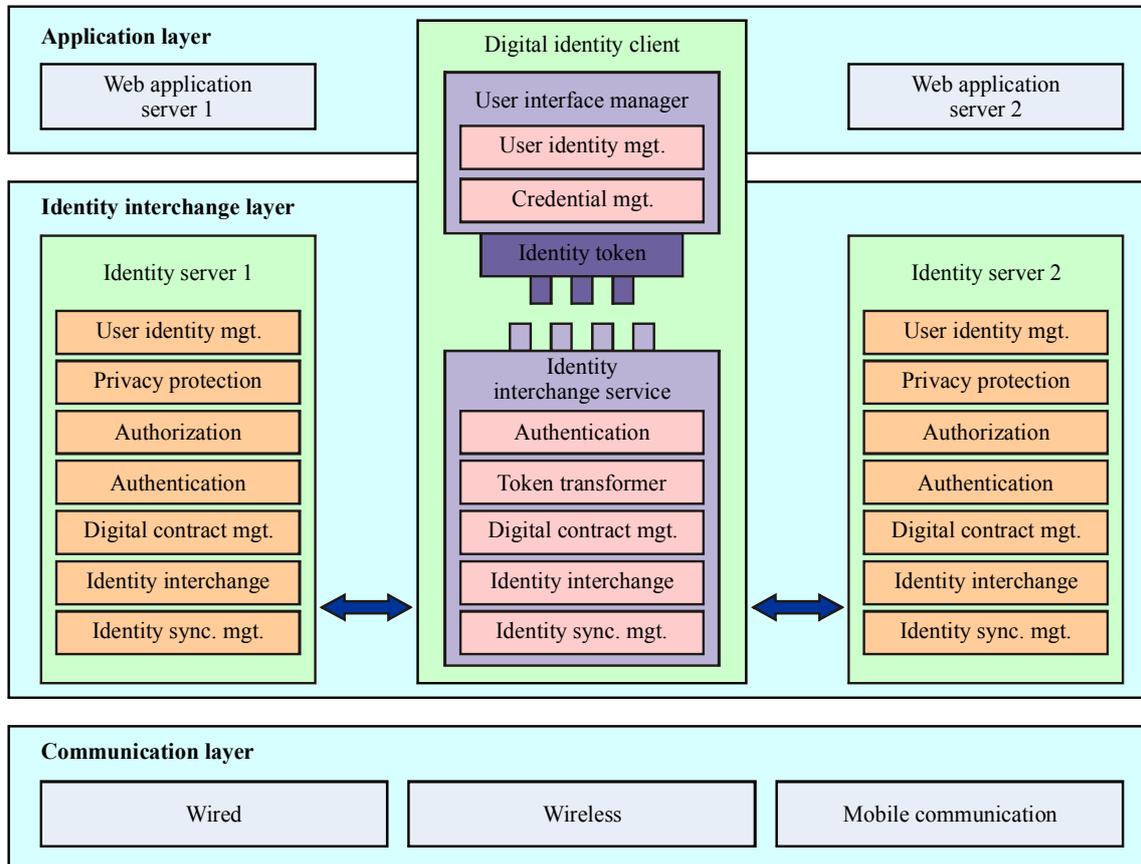
8 Digital identity interchange framework

8.1 Design principles

The framework has the following design principles to provide seamless identity interchange between entities in the computing environment including mobile and ubiquitous computing:

- **Independent** – The framework does not attach to any specific application or network environment. In other words, the framework itself should be adaptable to any environment if necessary.
- **Pluggable** – In a mobile or a ubiquitous computing environment, a user can work with several devices for work or entertainment. In this case, what the user needs is essential identity information that can establish his/her identity. This information should be designed to fit into any device, so that the user can just plug his/her identity information into the device to use it.

- **Flexible** – The framework should be designed to be flexible enough to fit into any device, ranging from a workstation to a small ubiquitous computing device. The framework should be malleable enough to be configurable to adapt to different computing environments.
- **Scalable** – The framework itself has to be operable from a single domain to an inter-domain without needing communication or computing overhead for it to be integrated into an existing system.



X.1251(09)_F04

Figure 4 – Digital identity interchange framework

8.2 Framework components

DIC is the core component in this framework and facilitates the identity link connecting all of the user's identity service providers and relying parties. A user can retrieve and update his/her identity information each time it is needed using the pre-established link.

DIC consists of three parts: user interface manager, identity interchange service and identity token.

Figure 4 represents the functional framework components.

8.2.1 User identity management

This is the component that manages the user's identity information that will be shared by entities. In an IdS, identity management is mainly focused on storage. On the other hand, identity management in the DIC tries to focus on the graphical user interface that presents identity information to the user.

8.2.2 Privacy protection

This is the component that manages the privacy-related function that protects a user's identity information. It keeps track of audit information related to the usage and purpose of the user's identity. The function also enforces the privacy constraints described in a digital contract whenever the user's identity is used unintentionally or on purpose. Privacy protection in accordance with applicable regional/national privacy legislation must be provided.

8.2.3 Authorization

The authorization service is designed to make decisions regarding the user's access rights and enforce authorization decisions according to the user's privileges. Authorization is an optional service; it is only provided when access to resources needs to be controlled based on the user's rights.

8.2.4 Authentication

This is the component that provides a generic authentication framework that supports various kinds of authentication mechanisms. The authentication service includes mutual authentication for both client and servers.

8.2.5 Digital contract manager

This is the component that manages the list of digital contracts made between the user and the identity service provider for authentication, access control and privacy protection. The manager manages the lifecycle of a digital contract that is signed by digital signature.

8.2.6 Identity interchange

This is the core component that provides the identity interchange service. Identity interchange is divided into two services: retrieve and update. If identity information is stored in an entity, a DIC can retrieve his identity from the entity and vice versa. If identity information stored in the entity is changed, the entity can update or push its changed identity information to the DIC and vice versa. A more detailed description of this component is outside the scope of this Recommendation.

8.2.7 Identity synchronization manager

This is the component that manages the identity synchronization process in the DIC. When identity information stored in an IdSP is changed, the IdSP updates the changed identity to the DIC. In the DIC, this component carries out identity update operation in the identity interchange function for every RP, which has been shared the user's identity by the DIC. Note that only the RP that the DIC has ever pushed his identity for once is eligible to receive the updated identity.

8.2.8 User interface manager

This is the component that presents the graphical user interface for the user's identity and credential information. This component has a close relationship with the web application server in general when a user needs to login using authentication or shares his/her identity information for some service.

8.2.9 Credential management

This is the component that manages the entity- or site-generated authentication credential information. A user can have various credentials such as a password, X.509 certificate and biometrics. A common graphical representation of credential information is defined for consistent user experience.

8.2.10 Identity token

The identity token is a data model for the digital identity. It can be plugged into a digital identity client to connect the user interface manager to the identity interchange service in order to enable the DIC to function. The logical representation of the token can be realized when the user interface manager is attached. For instance, when a user switches his/her working environment from a personal computer to a mobile phone, the user only needs to carry the token and plug it into the mobile phone. The hardware that will contain the token can be a smart card, a USB token, etc.

8.2.11 Identity interchange service

This is the service part that is responsible for identity interchange and synchronization. Depending on which network or communication platform is used, this part will need to be modified to fit into the environment. For instance, the identity interchange service module in a personal computer is quite different from that of a mobile phone.

8.2.12 Token transformer

This is the component that transforms a token issued from another existing IdM system into a token that can be understood and processed in the DIIF. This is the gateway component to interoperate with other existing IdM systems for the exchange of various tokens (e.g., identity, security). This is an optional component.

Appendix I

Reference implementation guideline for a framework for user control of digital identity using WS-trust and Information Card technology

(This appendix does not form an integral part of this Recommendation)

NOTE – This appendix provides an example mapping of WS-Trust [b-WS-TRUST] and Information Card [b-IS-INTEROP] against the capabilities of this Recommendation.

I.1 Introduction

This appendix describes how the requirements described in this Recommendation can be satisfied by WS-Trust and Information Card technology as described in [b-CARDSPACE].

I.2 Background

I.2.1 Digital identity client

Clause 7.3.2 describes "the concept of digital identity client that can control the interchange of digital identity".

I.2.2 Identity interchange layer

Clause 7.5.2 describes the "identity interchange layer to facilitate identity interchange between entities and to give an entity full control to enforce his security and privacy policies".

I.2.3 WS-Trust

The WS-Trust specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships. A Requestor, usually on behalf of an entity, sends a RequestSecurityToken (RST) message to a security token service (STS) and receives back a RequestSecurityTokenResponse (RSTR) usually containing a security token. The security token, containing a set of claims, may then be sent to a web service as proof of the requestor's identity. Optionally, a security token service may be sent an RST with a request to validate or cancel a previously issued security token. These interactions are shown in Figure I.1.

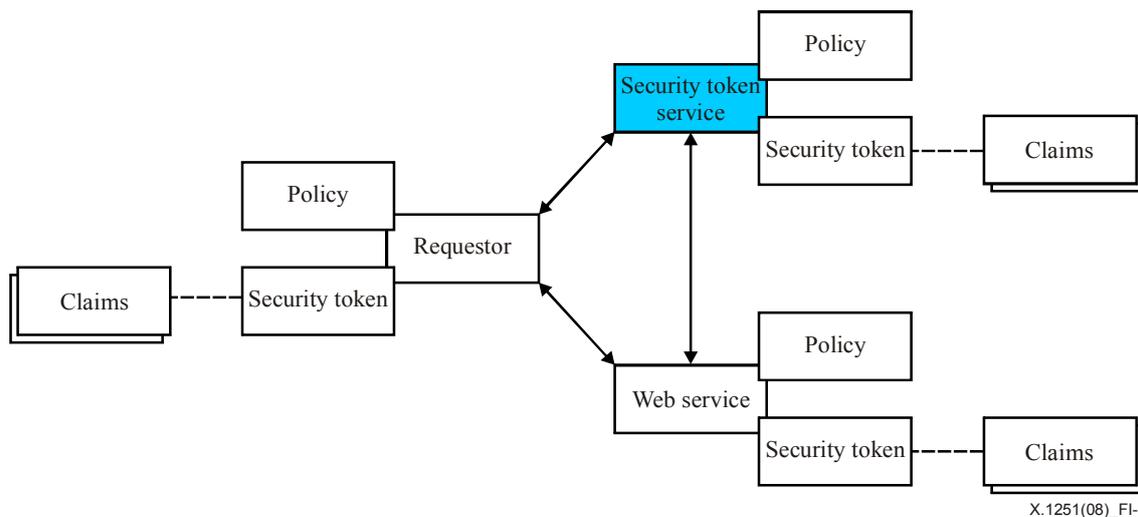


Figure I.1 – WS-Trust direct trust

WS-Trust may be used to implement a variety of models other than the simple direct trust model. In some cases an indirect model would be used where the IP/STS (identity service provider/security token service) sends an RST to another STS in order to satisfy the original RST, as in Figure I.2.

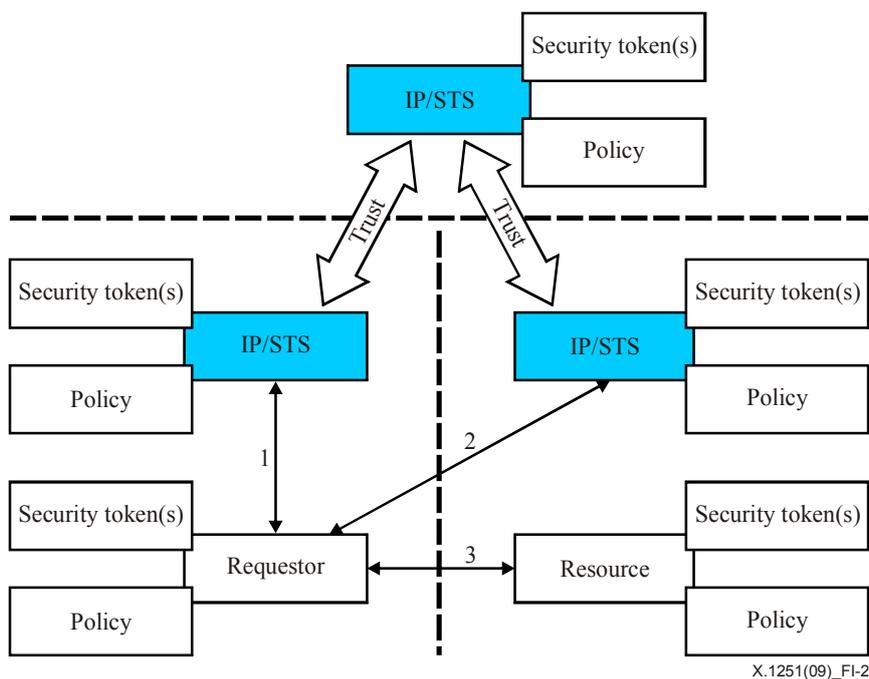


Figure I.2 – WS-Trust indirect trust

I.2.4 Information Card

Information Card technology is described in the Identity Selector Interoperability Profile [b-IS-INTEROP]. With Information Card technology, an identity selector and associated identity system components allow entities to manage their digital identities from different identity service providers, and employ them in various contexts to access online services.

When entities establish a relationship with IdSPs, they receive Information Cards; these Information Cards contain metadata which describes the potential security tokens that can be requested via WS-Trust as well as the security mechanisms used to protect and authenticate the message exchange. An entity typically installs their Information Cards into a card store accessible from their identity selector. The relying party security policy is specified via WS-SecurityPolicy [b-WS-SECURITY] and can be retrieved in a variety of ways, including embedded in web pages. The security policy typically specifies mechanisms defined in WS-Security for authentication and message protection. The identity selector evaluates the relying party policy and the set of Information Cards installed in the user card store and allows the entity to select from the set of Information Cards that match (are capable of getting a security token conforming to the policy). The identity selector then prompts the entity for authentication information, if necessary, and sends an RST to the STS specified in the selected Information Card. The security token from the resulting RSTR can then be attached to a message sent to the relying party. In the case where a website is the relying party, the security token can be posted as a response to the form which contained the policy [b-IS-GUIDE].

I.3 DIIF capabilities

This clause restates the capabilities from DIIF and describes how WS-Trust and/or Information Card technology could be used to satisfy them.

I.3.1 General capabilities

I.3.1.1 User capabilities

DIIF should achieve the following aims:

- 1) *Provision of an identity selector that allows the user to choose which credential is going to be used for authentication.*

The Identity Selector as described in Information Card provides for a secure, intuitive and consistent entity experience and allows an entity to select Information Cards representing a variety of identities provided by different IdSPs with a variety of authentication mechanisms.

- 2) *Provision of an intuitive and consistent interface to manage his/her credential information with maximum security.*

The identity selector, as described in Information Card, provides for a secure, intuitive and consistent entity experience.

- 3) *Support for auto fill-in registration or subscription of a website to minimize the user's interaction with the site including the user's full control to activate and deactivate such mechanisms. This is optional.*

The claim values included in the security token used in conjunction with the identity selector as described in Information Card can provide information that is typically entered by the entity at registration.

- 4) *Provision of identity information at any time a user wishes, and allows the user to fully control the identity interchange with an appropriate privacy protection mechanism.*

The assumption with Information Card technology is that an IdSP will provide identity information only in response to the entity's request. The privacy policy of the relying party and the IdSP are available within the secure identity selector user interface during Information Card selection.

- 5) *Provision of automatic updates for shared identity information when the original source is changed under his/her full control.*

The claim values included in the security token used in conjunction with the identity selector as described in Information Card can provide information that is typically entered by the entity at registration. Because the same security token claim values can be requested by the relying party at each visit, changes to these values are easily propagated.

- 6) *Provision of full user control over how the security and privacy policies are established and how they are enforced to control identity interchange before sharing identity information so that the user can have a direct influence on establishing a policy and enforcing it.*

The security policy of the relying party and the IdSP are available within the secure identity selector user interface as described in Information Card during Information Card selection.

I.3.1.2 Functional capabilities

- 1) *Support integrated credential management that can manage the user's credential information for authentication.*

Information Card technology includes an identity selector and a card management user interface.

- 2) *Support identity interchange link management to provide a user with a full-scale view of which entities the user has connections with for identity interchange.*

In the case where a security token representing a session is returned from an IdSP, the IdSP can provide an interface to allow an entity to view the set of established sessions.

- 3) *Support multiple authentication mechanisms, which can include password-based, PKI-based, and biometric-based authentications.*

WS-Trust and WS-Security provide a consistent and intuitive protocol supporting various authentication mechanisms. Information Card technology implementations provide intuitive APIs to initiate the authentication process.

- 4) *Support the identity interchange mechanisms that can provide a bidirectional link to share the user's identity information between entities using a DIC.*

With Information Card technology the identity selector and card store perform the functionality associated with a DIC.

- 5) *Support the digital contract mechanism to establish a contract for identity interchange and to be used to enforce the security and privacy policies for the release of PII.*

The security policy of the relying party and the IdSP are available within the secure identity selector user interface as described in Information Card during Information Card selection.

- 6) *Support identity information synchronization to update the distributed and shared identity information consistently when the source of disseminated identity information is changed. Identity information that needs to be synchronized is restricted to PII that is changed by a user directly.*

The claim values included in the security token used in conjunction with the identity selector as described in Information Card can provide information that is typically entered by the entity at registration. As the same security token claim values can be requested by the relying party at each visit, changes to these values are easily propagated.

- 7) *Support universal token transformation to make the framework interoperable with existing identity management systems.*

WS-Trust provides a token exchange mechanism. The RST message may include one or more security tokens as well as an indication of the identity of the relying party. The RSTR can include a security token appropriate for the relying party.

I.3.2 Additional capabilities

The DIIF should provide an extensibility mechanism for the identity selector and associated protocols to allow support for entry and transmission of a variety of authentication mechanisms and assurance related information.

This includes (but is not limited to) support for smart card readers and biometric input devices, as well as the data formats associated with them such as those described in [b-NIST].

Bibliography

- [b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.
- [b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.
- [b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.
- [b-CARDSPACE] Microsoft (2006), *Introducing Windows CardSpace*.
- [b-ETSI 133 980] ETSI TR 133 980 V8.0.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking*.
- [b-IS-INTEROP] Microsoft (2007), *Identity Selector Interoperability Profile V1.0*.
- [b-IS-GUIDE] Microsoft (2007), *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers*.
- [b-LA-FF] Liberty Alliance, *Liberty ID-FF Protocols and Schema Specification (ver 1.2)*.
- [b-NIST] National Institute of Standards and Technology (2006), *FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors*.
- [b-WS-SECURITY] OASIS (2007), *WS-SecurityPolicy 1.2*.
- [b-WS-TRUST] OASIS (2007), *WS-Trust 1.3*.

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