International Telecommunication Union

ITU-T D.1140/X.1261

(08/2020)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES D: TARIFF AND ACCOUNTING PRINCIPLES AND INTERNATIONAL TELECOMMUNICATION/ICT ECONOMIC AND POLICY ISSUES

Recommendations for international telecommunication/ICT economic and policy issues – Economic and policy aspects of big data and digital identity in international telecommunications services and networks

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Policy framework including principles for digital identity infrastructure

Recommendation ITU-T D.1140/X.1261

ITU-T D-SERIES RECOMMENDATIONS

TARIFF AND ACCOUNTING PRINCIPLES AND INTERNATIONAL TELECOMMUNICATION/ICT ECONOMIC AND POLICY ISSUES

TERMS AND DEFINITIONS	D.0
GENERAL TARIFF PRINCIPLES	
Private leased telecommunication facilities	D.1–D.9
Tariff principles applying to data communication services over dedicated public data networks	D.10–D.39
Charging and accounting in the international public telegram service	D.40–D.44
Charging and accounting in the international telemessage service	D.45–D.49
Principles applicable to GII-Internet	D.50–D.59
Charging and accounting in the international telex service	D.60–D.69
Charging and accounting in the international facsimile service	D.70–D.75
Charging and accounting in the international videotex service	D.76–D.79
Charging and accounting in the international phototelegraph service	D.80–D.89
Charging and accounting in the mobile services	D.90–D.99
Charging and accounting in the international telephone service	D.100–D.159
Drawing up and exchange of international telephone and telex accounts	D.160–D.179
International sound- and television-programme transmissions	D.180–D.184
Charging and accounting for international satellite services	D.185–D.189
Transmission of monthly international accounting information	D.190–D.191
Service and privilege telecommunications	D.192–D.195
Settlement of international telecommunication balances of accounts	D.196–D.209
Charging and accounting principles for international telecommunication services provided over the ISDN	D.210–D.260
Economic and policy factors relevant to the efficient provision of international telecommunication services	D.261–D.269
Charging and accounting principles for next generation networks (NGN)	D.270–D.279
Charging and accounting principles for universal personal telecommunication	D.280–D.284
Charging and accounting principles for intelligent network supported services	D.285–D.299
RECOMMENDATIONS FOR REGIONAL APPLICATION	
Recommendations applicable in Europe and the Mediterranean Basin	D.300–D.399
Recommendations applicable in Latin America	D.400–D.499
Recommendations applicable in Asia and Oceania	D.500–D.599
Recommendations applicable to the African Region	D.600–D.699
Recommendations applicable to the Arab Region	D.700–D.799
Recommendations applicable to the Eastern Europe, Central Asia and Transcaucasia Region	D.800–D.899
RECOMMENDATIONS FOR INTERNATIONAL TELECOMMUNICATION/ICT ECONOMIC AND POLICY ISSUES	
Charging and accounting/settlement mechanisms for international telecommunications services	D.1000–D.1019
Economic and policy factors relevant to the efficient provision of international telecommunication services	D.1020–D.1039
International Internet connectivity; and Tariff, Charging Issues of Settlements Agreement of Trans-multi-country Terrestrial Telecommunication	D.1040–D.1059
International mobile roaming issues	D.1060–D.1079
Alternative calling procedures and misappropriation and misuse of facilities and services	D.1080–D.1099
Economic and regulatory impact of the Internet, convergence (services or infrastructure) and new services	D.1100–D.1119
Definition of relevant markets, competition policy and identification of operators with significant market power (SMP)	D.1120–D.1139
Economic and policy aspects of big data and digital identity in international telecommunications services and networks	**D.1140–D.1159**
Economic and policy issues pertaining to Mobile Financial Services (MFS)	D.1160–D.1179

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

Recommendation ITU-T D.1140/X.1261

Policy framework including principles for digital identity infrastructure

Summary

Recommendation ITU-T D.1140/X.1261 sets out a policy framework including principles for digital identity infrastructure while recognizing the sovereign right of each Member State to regulate its Telecommunications.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T D.1140/X.1261	2020-08-28	3	11.1002/1000/14270

Keywords

Digital identity.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had 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/.

Introduction

As the world is getting more connected, more services are being made available online by governments and service providers. While it is encouraged to be a part of this digital revolution, the underlying conundrum of identification remains a barrier. Enabling access to all sections of the society – to the economy, its infrastructure, and its institutions – can be a challenge due to absence of an identity mechanism that is accepted across all domains. Individuals need to identify one another and to identify themselves for access to a host of government and non-government services. Absence of easily verifiable identity mechanism can contribute towards exclusion, as an individual maybe unable to prove his/her identity, which can prove to be a barrier that may prevent the individual from accessing telecommunication services/other services (banking, access to credit)/benefits and subsidies being provided by governments. Thus, proof of identity becomes a prerequisite for socio-economic development.

There are many benefits that can be derived from a mechanism that uniquely identifies a legal form of data including, inter-alia, an individual or entity and ensures instant identity verification and authentication. The ability to prove one's identity easily and instantaneously can reduce transaction costs and improves user satisfaction. One of the ways to achieve this goal is through digital identity (digital ID) programmes, central registries storing personal data in digital form and credentials that rely on digital, rather than physical, mechanisms to authenticate the identity of their holder.

However, views on protection of digital identity tend to take one of the two extremes: (i) Create powerful safeguards to keep private information private or (ii) let businesses and governments do what they need to do in order to realize the economic potential of the big data arising out of the digital identity implementation. Member States, regulators, advocacy groups and individuals are concerned about misuse of private information. There is clearly a need to create a balance, which maximizes economic output and at the same time protects the privacy of the individuals. In the current situation, having a policy framework including principles for digital identity programmes has become a key priority area for ITU Member States.

Recommendation ITU-T D.1140/X.1261

Policy framework including principles for digital identity infrastructure

1 Scope

This Recommendation proposes a policy framework for digital identity, including principles for designing digital identity infrastructure.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

3.1.3 authorization [b-ITU-T Y.2720], and [b-ITU-T X.800]: The granting of rights and, based on these rights, the granting of access.

3.1.4 digital identity [b-ITU-T X.1252]: A digital representation of the information known about a specific individual, group or organization.

3.1.5 entity [b-ITU-T X.1252]: Something 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 entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.1.6 identification [b-ITU-T X.1252]: The process of recognizing an entity by contextual characteristics.

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

3.1.8 personally identifiable information (PII) [b-ITU-T X.1252]: Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 digital identity infrastructure: A system that has a set of functions (e.g., issuance, administration, management and maintenance, discovery, communication exchanges, policy enforcement, authentication and assertions, security) for identification, authentication and authorization of the digital identity of an entity (e.g., identifiers, attributes, etc.).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

DII Digital Identity Infrastructure

PII Personally Identifiable Information

PKI Public Key Infrastructure

5 Conventions

None.

6 Policy framework and principles for digital identity infrastructure

6.1 Policy framework

6.1.1 Member States are encouraged to establish a digital identity infrastructure (DII) for the issuance of digital identities that can be used for the targeted delivery of public services which may include subsidies, benefits and services. The DII can be used by various social welfare programmes. Commercial enterprises, service providers and others may also use DII for the targeted delivery of their services. Member States should work to ensure that there is coordination amongst the relevant government agencies and stakeholders involved in the roll-out and management of DII.

6.1.2 Member States should encourage the issuance of digital identities which are secure, robust enough to eliminate fake and duplicate identities, and can be verified and authenticated in a cost-effective way.

6.1.3 Member States should encourage the availability of digital identities for a wide range of services through open and secure interfaces.

6.1.4 Member States should ensure that DII performs three main functions:

- Identification (in order to establish identity);
- Authentication (in order to assert identity); and
- Authorization (in order to authorize the use of the digital identity).

6.1.5 Digital identity programmes established by Member States should ensure that every resident/user, who is otherwise entitled to obtain a digital identity, does so when they submit necessary information.

6.1.6 Member States should also consider promoting special measures for, and facilitating the issuance of digital identities to vulnerable sections of the society, in particular, senior citizens, persons with disabilities, as well as residents living in underserved areas that may not have a permanent address.

6.1.7 Member States should take adequate measures to safeguard digital identities from cyber threats.

6.1.8 It is the sovereign right of each country to regulate its telecommunications and, as such, to regulate the provision of digital identity infrastructure (DII) in the context of national laws, regarding data-protection.

6.2 Guiding principles for digital identity infrastructure

6.2.1 When creating digital identity infrastructure, Member States should apply principles and policy considerations on universality, accessibility, auditability and protection of personally identifiable information (PII) throughout the technology design and development stages.

6.2.2 The design of digital identity infrastructure should take into consideration the following principles:

- Simplicity
  - Easy to implement and use
- Unbundling
  - Attributes are unbundled from the entity
- Minimization
  - The attributes used for creating digital identity should be necessary and proportionate
- Uniqueness
  - Member State issue only one digital identity per user/resident for access to government services
- Openness
  - Based on open application programming interfaces (APIs)
- Security
  - Infrastructure should be secure from unauthorized access, leaks, breaches, theft, etc. via the use of public key infrastructure (PKI) amongst others.

6.2.3 The design of DII must be flexible and scalable to meet the future requirements as digital technology evolves further.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for open systems interconnection for CCITT applications*.

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

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

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

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information.*

[b-ITU-T X.1258] Recommendation ITU-T X.1258 (2016), *Enhanced entity authentication based on aggregated attributes.*

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

[b-ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – cloud computing based requirements and capabilities.*

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	**Tariff and accounting principles and international telecommunication/ICT economic and policy issues**
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020