

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1314

(11/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Ubiquitous sensor
network security

Security requirements and framework of ubiquitous networking

Recommendation ITU-T X.1314

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
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1314

Security requirements and framework of ubiquitous networking

Summary

Recommendation ITU-T X.1314 provides a high-level security framework for ubiquitous networking, analyses security threats and defines the security requirements to mitigate these threats in ubiquitous networking environment.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1314	2014-11-13	17	11.1002/1000/12345

Keywords

Object, security framework, security requirement, security threats, ubiquitous networking.

* 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/>.

© ITU 2015

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

Table of 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 and acronyms	2
5	Conventions	4
6	High-level security framework for ubiquitous networking	4
7	Security threats and requirements.....	6
	7.1 Service and transport security domain	6
	7.2 End-user security domain	9
	7.3 UN application security domain.....	11
	7.4 Other network security domains.....	14
	7.5 End-to-end connectivity security domain.....	14
	7.6 Interface security domain	15
	Appendix I – Security framework progress from other SDOs.....	16
	I.1 3GPP M2M security framework (b-3GPP TR33.868)	16
	I.2 oneM2M security framework (b-oneM2M-TS-0003).....	17
	Bibliography.....	21

Introduction

The ETSI Board 69 meeting approved to establish a machine-to-machine (M2M) Technical Committee (TC) in October 2009. ETSI TC M2M has the following responsibilities:

- to collect and specify M2M requirements from relevant stakeholders;
- to develop and maintain an end-to-end overall high level architecture for M2M;
- to identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps, where existing standards bodies or groups are unable to do so;
- to provide the ETSI main centre of expertise in the area of M2M;
- to co-ordinate ETSI's M2M activity with that of other standardization groups and forums.

3GPP has initiated a series of study items on machine-to-machine communications. 3GPP network improvements for machine type communications will be studied. The objectives of these work items are to:

- identify and specify general requirements for machine type communications;
- identify service aspects where network improvements (compared to the current human-to-human (H2H) oriented services) are needed to cater for the specific nature of machine type communications;
- specify machine type communication requirements for these service aspects where network improvements are needed for machine type communication;
- study the architecture aspects based on the above requirements.

ITU-T Study Group 13 approved Recommendation ITU-T Y.2002 on 29 October 2009. [ITU-T Y.2002] provides an overview of ubiquitous networking and of its support in next-generation networks (NGNs). The security considerations of ubiquitous networking were addressed as follows:

- Basic considerations on the security architecture for NGN are addressed in [b-ITU-T Y.2001], while the security requirements of NGN are described in [b-ITU-T Y.2701]. Concerning the specifics of ubiquitous networking, the various kinds of terminals, devices and contents that can be involved will have to conform to the security requirements of the network they are willing to attach to. When attaching to NGN, the corresponding authentication and authorization requirements are described in [ITU-T Y.2702].
- Objects involved in ubiquitous networking have their own identities and are interconnected involving more interactions throughout a dynamic and heterogeneous environment. Accordingly, security as well as the design of the security architecture for a secure information discovery and delivery to users, including persons and objects, is very crucial. Security measures should take into account, for all use, cases that rely upon NGN capabilities but which are in line with the guidelines and principles for ubiquitous networking.

ITU-T Question 6/17 has standardized the security of ubiquitous sensor network (USN). Recommendations ITU-T X.1311, ITU-T X.1312, and ITU-T X.1313 respectively deal with the different security issues of USN:

- Recommendation ITU-T X.1311 | ISO/IEC 29180, 'Information technology – Security framework for ubiquitous sensor networks', describes security threats to and security requirements of the USN. In addition, this Recommendation categorizes security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of the USN. Finally, [b-ITU-T X.1311] presents the security functional requirements and security technologies.
- Recommendation ITU-T X.1312, 'Ubiquitous sensor network middleware security guidelines', provides guidelines for USN middleware security. It analyses security threats on USN middleware and defines security requirements.
- Recommendation ITU-T X.1313, 'Secure routing mechanisms for wireless sensor network', provides the security requirements for wireless sensor network routing. It explains the general network topologies and routing protocols in USNs. In addition, this Recommendation analyses the security threats facing wireless sensor networks.

Ubiquitous networking anticipates a comprehensive and complex system in the future. Meanwhile, some important issues for ubiquitous telecommunication are already being developed by the major standards development organizations (SDOs).

Security is one of the most important issues for ubiquitous networking. Security requirements and measurements to 3GPP network, USN and M2M service layer have already been studied among 3GPP, ITU-T and ETSI. However, there are limited discussions on security of ubiquitous networking so far. Therefore, more detailed security requirements to ubiquitous networking supported by NGN should be researched, and its security architecture should be provided based on the architectural model for ubiquitous networking in [ITU-T Y.2002].

Document ID: 123456789

Recommendation ITU-T X.1314

Security requirements and framework of ubiquitous networking

1 Scope

This Recommendation provides a high-level security framework for ubiquitous networking. This framework is divided into security domains, which include an analysis of security threats. High-level security requirements then are derived based on this analysis.

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 Y.2002] Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and of its support in NGN*.
- [ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 next generation network (NGN) [b-ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.2 object [b-ITU-T Q.1300]: An intrinsic representation of an entity that is described at an appropriate level of abstraction in terms of its attributes and functions.

NOTE 1 [b-ITU-T Y.2002] – An object is characterized by its behaviour. An object is distinct from any other object. An object interacts with its environment including other objects at its interaction points. An object is informally said to perform functions and offer services (an object which makes a function available is said to offer a service). For modelling purposes, these functions and services are specified in terms of the behaviour of the object and of its interfaces. An object can perform more than one function. A function can be performed by the cooperation of several objects. See [b-ITU-T X.902] for further information.

NOTE 2 [b-ITU-T Y.2002] – Objects include terminal devices (e.g., used by a person to access the network such as mobile phones, personal computers, etc.), remote monitoring devices (e.g., cameras, sensors, etc.), information devices (e.g., content delivery server), products, contents, and resources.

3.1.3 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.4 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organisation.

3.1.5 ubiquitous networking [ITU-T Y.2002]: The ability for persons and/or devices to access services and communicate while minimizing technical restrictions regarding where, when and how these services are accessed, in the context of the service(s) subscribed to.

3.1.6 ubiquitous sensor network (USN) [b-ITU-T Y.2221]: A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at anytime, and where the information is generated by using context awareness.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
AE	Application Entity
ANI	Application-to-Network Interface
AS	Application Server
CA	Certification Authority
CDF	Charging Data Function
CGF	Charging Gateway Function
CSE	Common Services Entity
CSF	Common Service Functions
DoS	Denial of Service
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
H2H	Human-to-Human
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
ID	Identity
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IP-SM-GW	IP-Short-Message-Gateway
ISDN	Integrated Services Digital Network