International Telecommunication Union

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

International Telecommunication Union

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/.

Table of Contents

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].

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

IWF	Interworking Function
IWMSC	Interworking Mobile Switching Centre
LTE	Long Term Evolution
M2M	Machine-to-Machine
MITM	Man-in-the-Middle
MME	Mobile Management Entity
MSC	Mobile Switching Centre
MTC	Machine Type Communication
NAS	Network Access Server
NGN	Next-Generation Network
NNI	Network-to-Network Interface
NSE	Network Services Entity
OSI	Open Systems Interconnection
P-GW	Packet Data Network Gateway
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAN	Radio Access Network
RFID	Radio Frequency Identifier
SCS	Services Capability Server
SDO	Standards Development Organization
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SME	Short Message Entity
SMS-SC	Short Message Service – Service Centre
SIM	Subscriber Identity Module
TC	Technical Committee
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated Circuit Card
UN	Ubiquitous Networking
UNI	User-to-Network Interface
USN	Ubiquitous Sensor Network
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network

5 Conventions

None.

6 High-level security framework for ubiquitous networking

[ITU-T Y.2002] states that one of the ultimate objectives of ubiquitous networking (UN) is to meet the challenge of seamless communications of "anything" (e.g., persons and objects). UN will have to encompass the following characteristics:

- ubiquitous connectivity allowing for whenever, whoever, wherever, and whatever types of communications;
- pervasive reality for effective interface to provide connectable real world environments;
- ambient intelligence allowing for innovative communications and providing increased value creation;

There are security threats and challenges when "anythings" (e.g., persons and objects) communicate with each other; security requirements vary to a great extent for different UN applications. Many of the security threats can be mitigated with the implementation of traditional security processes and mechanisms. However, objects in UN have their own identities and their inter-communication in a dynamic and heterogeneous environment requires more interactivity. Accordingly, it is crucial that secure information discovery and secure information delivery to users (including persons and objects) should be carefully considered in the design of security framework for UN. Security measures should take into account all use cases that rely on NGN capabilities while at the same time be in line with the guidelines and principles for UN.

Based on these identified security threats and challenges, security requirements are derived to mitigate security threats and address security challenges for UN.

This Recommendation aims to provide a high-level security framework for UN, which is shown in Figure 1, based on the high-level architectural model for UN in NGN specified in [ITU-T Y.2002].

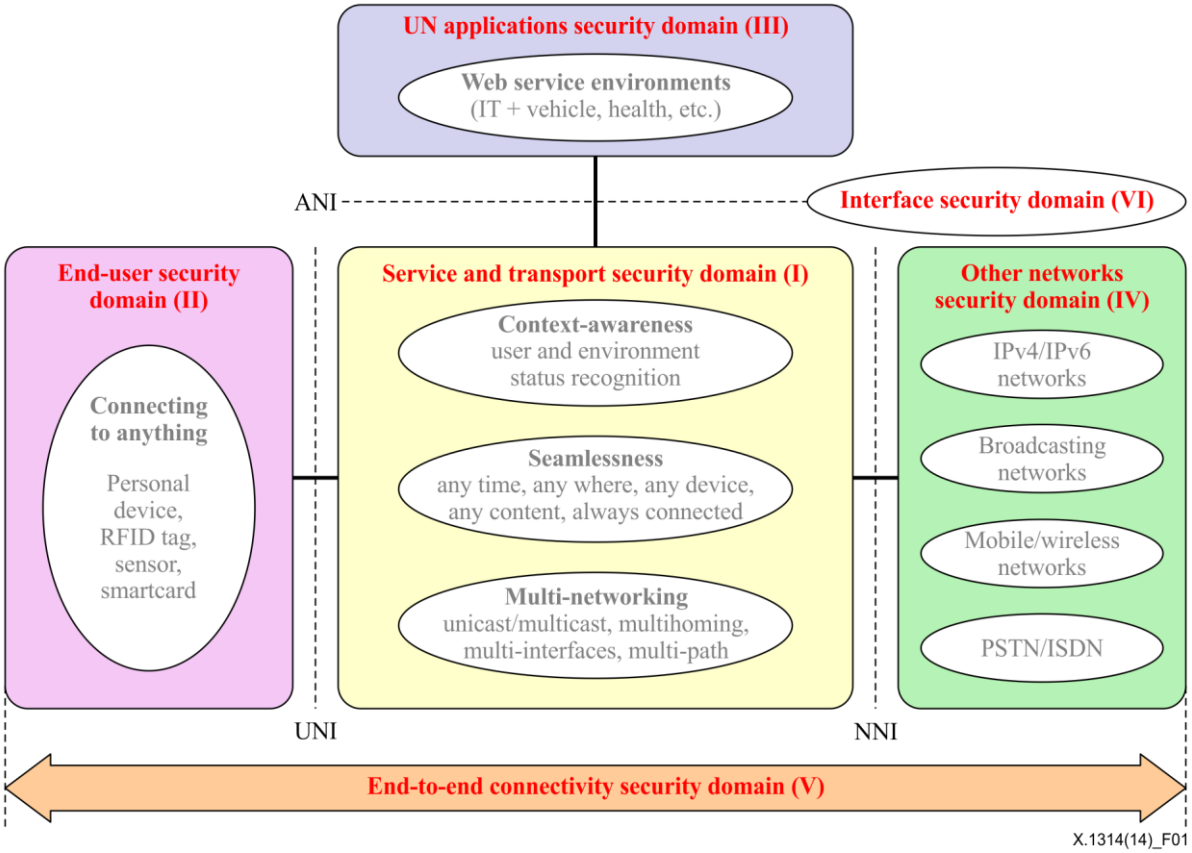

Figure 1 – High-level security framework for UN

In this framework, six security domains are defined. Each of these domains contains a group of security features that will meet certain threats and accomplishes certain security objectives.

Service and transport security domain (I): The set of security features that provide the security assurance for signalling traffic and user traffic in the control and transport network of the UN.

For example, one of the key issues of UN is congestion avoidance and control, which is either caused by concurrent services or by malicious attacks such as denial of service (DoS) or distributed denial of service (DDoS) attacks. When many objects are required to report service data in a short period of time, the resulting bulk converged data may overwhelm network capacity and lead to congestion, which in the worst case may cause the ubiquitous network to collapse. Other causes of congestion are mainly from malicious attacks such as DoS/DDoS attacks.

Congestion blocks the normal communication and hence disables the proper functioning of the fundamental services of UN. For this reason, network congestion avoidance and control is one of the most significant problems to be solved in UN.

End-user security domain (II): The set of security features that protect the object itself from malicious attacks, including object integrity, object application software security, privacy as well as communication security between objects and network.

UN applications security domain (III): The set of security features that offer protection for services and applications over UN. Common application domain security features may include application level access control, web security, etc.

Other networks security domains (IV): The set of security features of a neighbouring network. There are two possible cases. If the neighbouring network is also a ubiquitous network, then its network security requirements are in accordance with that of the ubiquitous network. On the other hand, if the neighbouring network is not a ubiquitous network, which might be either a mobile network or a fixed network, then there are different security mechanisms for these two kinds of networks.

End-to-end connectivity security domain (V): The set of security features that provide secure end-to-end communication for UN. These features may include cross domain key management, identity management, etc.

As a cross-domain security assurance, the end-to-end connectivity security domain may cover communication security assurance between end-user security domain and UN applications security domain, end-user security domain and other domains, and in-between end-user security domains. Cross-domain security assurance mainly ensures media plane data security, which includes encryption, integrity, and end-to-end user authentication, etc.

NOTE 1 – When providing end-to-end communication domain security, it is required that any influences from the network domain onto the media plane user data should be avoided. However, the network domain can participate in key management or number assignment, or a third-party key management centre or certification authority (CA) can be introduced to provide key or certificate management. Pre-shared keys or a periodical change of keys can also be used. All these approaches can be used to provide end-to-end communication data security.

NOTE 2 – In general, the end-to-end authentication and authorization, end-to-end data encryption and data integrity can be achieved within the ubiquitous network. However, when the ubiquitous network needs to communicate with or through other network domains, it is possible that end-to-end security protection be jeopardized due to the failure of encryption key negotiation. In these cases, when different network access mechanisms are utilized for accessing ubiquitous networks and other network domains, a common mechanism such as the Internet protocol (IP) access and data protection mechanism (e.g., transport layer security (TLS) or datagram transport layer security (DTLS)) may be utilized to further protect end-to-end communications.

Security technologies for end-to-end communication mainly include encryption technology, digital signature technology, etc. These technologies can all be found in the 'Other networks security domain'.

Interface security domain (VI): This refers to the access security and/or inter-connect security mechanisms of user-to-network interface (UNI), application-to-network interface (ANI) and network-to-network interface (NNI).

UNI access security technologies have been included in the description in domain I and domain II above. ANI access security technologies have also been included in the description in domain I and domain III above. ANI access security and NNI security technologies include extensible authentication protocol (EAP), Internet protocol security (IPSec), etc. These technologies can also be found in the above first three domains.

7 Security threats and requirements

Concerning the specifics of UN, various kinds of terminals, devices and content 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].

7.1 Service and transport security domain

7.1.1 Security threats

The following threats exist in the service and transport domain.

7.1.1.1 Disclosure of privacy information

Some objects may be located in physically exposed sites. This leaves the attackers an opportunity to get user privacy information (such as personally identifiable information (PII)) from these objects, and attack the ubiquitous network from these objects.

7.1.1.2 Secure data transmission

There are generic security issues related to the confidentiality and integrity of signalling in UN.

7.1.1.3 Congestion

Due to the large number of objects, signalling traffic generated from present authentication and authorization mechanism will pose a tremendous pressure on the traffic generated from the network, especially when all these objects need to be logged into the system within a short period of time. This may lead to congestion and hence block normal data communication for legitimate services and applications. If no improvements are implemented, the present authentication and authorization mechanism will lead to vulnerability and an opportunity for the attackers to utilize and attack the system based on DoS/DDoS mechanisms.

In a conventional communication network, the network side authenticates user terminals individually and generates the corresponding encryption and integrity keys. Hence when there are huge numbers of objects (many more than the number of conventional mobile terminals), this one-by-one key generation process will over-consume network-side resources and lead to vulnerability and an opportunity for the attackers to utilize and attack the system based on resource-depletion DoS/DDoS mechanism. Similarly, for the various kinds of services in the future Internet of things (IoT) network, the individual authentication mechanism for authenticating the same user and the same type of service equipment will be an enormous waste of network-side resources.

7.1.1.4 Man-in-the-middle attack

Attackers may initiate a man-in-the-middle (MITM) attack which results in the objects becoming disconnected from the ubiquitous network. Attackers may also trick the objects by sending spoofed requests or responses towards the ubiquitous network, resulting in the ubiquitous network making wrong judgements and hence damaging the network security.

7.1.1.5 Spoofed network messages

Attackers may utilize the security mechanisms of objects and send spoofed signalling commands to them to disconnect them from the ubiquitous network, or trick them to make wrong operations or wrong responses.

7.1.2 Security requirements

The security requirements for the service and transport security domain mainly include:

- authentication and authorization for network access;
- secure transmission of voice, data and multimedia service data;
- establishment of the virtual private network (VPN) over the Internet public infrastructure;
- secure storage of privacy information including personal or company information;
- countering measures against viruses, network-based attacks, etc.

Although different communication networks have different characteristics and security requirements, most security issues on UN can be solved by the existing common and enhanced protection measures.

For this reason, UN should provide the following security capabilities.

7.1.2.1 Overall security requirements

The overall security requirements of UN shall not be lower than that of NGN.

More specifically, the security requirements of ubiquitous network abide by those of NGN. However, in certain UN services or under certain UN architectures, there may be new security requirements that are unique to UN, such as the congestion avoidance and control requirement of UN and other security requirements that are induced by certain trigger services in UN.

7.1.2.2 Confidentiality requirement

The confidentiality of signalling in UN shall be guaranteed. This refers to the confidentiality requirements of control plane data so that control plane data are properly secured from eavesdropping, etc. In this way, it is ensured that UN can process the services normally.

7.1.2.3 Integrity requirement

The integrity of signalling information and user data in UN shall be guaranteed. This refers to the data integrity requirements of both UN signalling information and user data, so that the signalling information is properly secured and the user data integrity requirements are met. In this way, it is ensured that UN can process the services normally.

7.1.2.4 Privacy requirement

The privacy information such as user identity and node location shall be protected. This refers to the protection of the PII from being eavesdropped or disclosed, as well as the protection of user location information, etc., from being obtained by attackers. Once this information is obtained by attackers, they may launch illegal attacks to objects.

7.1.2.5 General requirement on authentication

Multiple mechanisms of mutual authentication between objects and ubiquitous networks shall be supported so as to ensure that only legal objects may access the ubiquitous network.

7.1.2.6 Group authentication requirement

The number of UN terminals can be huge and based on the classification of all kinds of applications and services, there can be many UN terminal groups. UN needs to implement a unified management, and a unified resource allocation to these terminal groups. Therefore, it is necessary for UN to implement group authentication for these terminal groups.

Group authentication of objects shall be supported. For group authentication, a group of objects may have a common UN group identity (ID) for authentication and authorization. The ubiquitous network or the UN application domain may authenticate and authorize the whole group of objects with this group ID, or may authenticate and authorize them individually.

The authentication of group objects may be performed by an authentication agent or gateway, or by master equipment.

Through a unified terminal gateway, mutual authentication can be implemented between the objects and the ubiquitous network. Firstly, the gateway shall implement mutual authentication with the ubiquitous network, and calculate the corresponding key materials. Secondly, the gateway shall implement mutual authentication with objects and, if successful, it shall send the above calculated key materials to the objects. In the meantime, the gateway shall inform the ubiquitous network and the authenticated object group. Thirdly, the objects shall generate authenticated encryption traffic keys based on the hash of its root key and the received key materials from the gateway, meanwhile the ubiquitous network shall also generate the authenticated encryption traffic key based on the hash of key materials and the root key of the authenticated objects. In this way, the communication security between the UN object group and the ubiquitous network is guaranteed.

7.1.2.7 General requirement for the keys

Based on the group authentication requirement, shared keys between objects and network-side entities shall be supported.

Based on the open systems interconnection (OSI) protocol stack, shared keys of the same protocol layer between objects and network-side entities shall be supported.

Based on the OSI protocol stack, keys of part or of all protocol layers may be generated by the ubiquitous network equipment.

7.2 End-user security domain

7.2.1 Security threats

The following threats exist in the end-user domain.

7.2.1.1 Unauthorized access

When objects are physically or logically compromised, attackers may use simple analytical tools to read confidential data stored on objects.

When objects are physically or logically compromised, attackers may disable the objects from providing services.

7.2.1.2 Fake objects

Through faking legitimate objects, attackers may inject data into legitimate objects and thereby initiate various cyber-attacks. These may include eavesdropping on the communications of objects, announcing spoofed routing information, reporting spoofed data, launching denial of service (DoS) attacks, etc.

7.2.1.3 Threat of selfish nodes among objects

Objects are supposed to collaborate with each other in order to provide more efficient services. However, for various reasons some objects may be reluctant to use their own power or available bandwidth for providing certain (typically data forwarding) services. These behaviours may lead to reduced network efficiency and, in worst cases, to the failure of the network.

7.2.1.4 Trojans, viruses, and spam attacks

These threats originate from application software bugs or operating system bugs.

7.2.1.5 Personally identifiable information disclosure

This information includes personal data, using habit, user location, etc. Attackers may collect these data and undertake comprehensive user behaviour analysis.

7.2.2 Security requirements

The security requirements for objects can be very different depending on their types and corresponding characteristics. Different types of objects have distinct characteristics, and hence they have peculiar vulnerabilities and may face specific security threats. Consequently, different security requirements should be identified and the corresponding protection measures should be applied on these different types of objects. All these must be based on an in-depth analysis of the respective object characteristics, which include:

- different physical characteristics including the storage capacity, communication and processing abilities of objects;
- different services provided by objects;
- different service environments of objects;
- different service requirements of users, etc.

Based on the above analysis, these differences in object characteristics will lead to differences in the security requirements of objects. These requirements are detailed in the following subclauses.

7.2.2.1 Physical protection requirements

Measures should be taken to protect objects from theft or from being physically acquired by attackers.

Measures should be taken to prevent the universal integrated circuit card (UICC) or the subscriber identity module (SIM) card from being illegally removed or replaced by attackers.

7.2.2.2 Anti-virus, firewall protection requirements

Anti-virus software and firewall should be installed to prevent the objects from being attacked by Trojans, viruses and spam email.

7.2.2.3 Access control requirements

Access control mechanisms should be applied on objects to prevent them from being logically compromised, and to prevent them from disclosing user or objects information to other objects or network equipment.

7.2.2.4 Authentication requirement

Authentication should be required for users and other network equipment which require access to the sensor nodes.

7.2.2.5 Non-repudiation requirement

Logging should be provided for read and write operations on objects so that access to the ubiquitous network and usage of services can be identified.

7.2.2.6 Confidentiality requirement

The data stored on, and transmitted by, objects should be encrypted.

7.2.2.7 Data integrity requirement

Measures should be taken to prevent data on objects from being tampered with. More specifically, this refers to the protection of transmitted and received data on objects from tampering so that the proper functioning of UN services is guaranteed.

7.2.2.8 Availability requirements

Measures should be taken to protect sensor nodes from being logically compromised or from being attacked by viruses, both of which may lead to their being taken out of service. Measures should also be taken to ensure that objects collaborate with each other so that while network resources are being consumed, objects can contribute at the same time in the enhancement of their own resources.

7.2.2.9 Privacy requirement

Measures should be taken to protect user privacy information stored on objects, and to prevent personally identifiable information from being disclosed.

Table 1 – Relationship between security threats and security requirements of the end-user domain

Threat / Requirement	Unauthorized access of object data	Disable objects from service	Fake objects	Selfish nodes among objects	Trojans, viruses and spams attacks	Information disclosure
Physical protection	√	√	√			
Anti-virus, firewall protection					√	
Access control	√	√	√			√
Authentication	√	√	√			√
Non-repudiation	√	√	√			√
Confidentiality	√	√	√			√
Data integrity			√			
Availability		√		√	√	
Privacy	√					√

7.3 UN application security domain

7.3.1 Security threats

The following threats exist in the UN application domain.

7.3.1.1 Privacy threats

Extensive use of wireless communications, electronic tags (e-tags) and large amount of unattended equipment are three fundamental characteristics of UN, which make it outstanding for the privacy disclosure threat. In telemedicine, electronic payment, and positioning, etc., scenarios, user privacy information might be obtained by attackers and hence users will face a potential security threat of privacy disclosure and consequently hidden troubles.

There are two types of privacy threats: privacy disclosure and malicious tracking:

- Privacy disclosure: Privacy disclosure refers to the situation where important or valuable user information is directly or implicitly disclosed to attackers. This PII may include user's medical records, identity, hobbies, trade secrets, etc.
- Malicious tracking: The user privacy information may be used by the attacker for malicious tracking of the user. For example, the privacy violator may track the user's whereabouts by utilizing the location information of e-tags. Robbers may identify the number and track the location of the valuables by utilizing their identification information.

7.3.1.2 Service abuse

The potential threats of service abuse should be mitigated in UN. These may include illegal access to services by unauthorized users, and illegal access to non-customized services by authorized users, etc.

7.3.1.3 Identity impersonation

There are large numbers of physically exposed and unattended objects in ubiquitous networks. These devices might be hijacked and used to masquerade as a client or application server to send data and perform operations. For example, in the intelligent home scenario attackers may hijack an UN device

to masquerade as an application server so as to remotely compromise automatic door access control systems. Then the attackers may disable the alarm systems of the house, open the door and break in without any access card.

7.3.1.4 Application layer information eavesdropping/tampering

The ubiquitous network is a multi-domain, heterogeneous network. Each domain has its own specific issues. Therefore the security mechanisms for these network domains are relatively independent, leading to the potential risk and threat that the application layer data might be eavesdropped, injected and tampered.

7.3.1.5 Repudiation

Any user who has participated in a communication session may deny or repudiate the operations and commitments he or she had made.

7.3.1.6 Replay

Attackers may send a received message from the ubiquitous network to deceive the system.

7.3.1.7 Signalling congestion

As in conventional communication networks, the authentication between objects and ubiquitous network servers is currently performed individually. Due to the large number of objects, when these objects are required to participate in providing a service in a short period of time, they will produce massive amounts of authentication requirement messages towards the ubiquitous network application server. These massive messages may cause an overload of the ubiquitous network application server, which will ultimately lead to a congestion in the ubiquitous network signalling channel, and result in DoS of the application server.

7.3.2 Security requirements

The basis of all UN applications is to achieve wide range information exchange between persons and UN terminals, as well as between UN terminals. These UN applications include various industry applications as well as public-serving applications, all of which fall in the category of the UN application domain security. Research works on security issues and security requirements need to be carried out in combination with a variety of application scenarios respectively, which include smart city, intelligent transportation, intelligent logistics, intelligent monitoring and control of the environment, smart community and intelligent home, smart health care, etc.

There are commonalities and differences in security issues and security requirements for these applications scenarios. Common security requirements include:

- identity authentication and access control for operating users;
- source encryption and integrity protection for sensitive industrial data;
- use of certificates and application of public key infrastructure (PKI) for identity authentication;
- use of digital signature for non-repudiation and security audit, etc.

Besides, application-specific security requirements should be identified in combination with the corresponding intelligent applications, for which the following aspects of targeted research should be carried out:

- the characteristics of these intelligent applications;
- the application scenarios;
- the service clients of these intelligent applications;
- the user-specific requirements of these intelligent applications, etc.

Regarding the common security issues in the UN application domain, the following security requirements can be mainly identified.

7.3.2.1 Identity authentication requirement

The true identity of both the UN server and the objects should be authenticated so that identity impersonation and cloning of object attacks can be avoided.

7.3.2.2 Service authentication requirement

The UN application server should authenticate the objects for the right to use the service, so that illegal, unauthorized access to services can be avoided. Rigorous service authentication must be enforced before objects are permitted to use the services.

7.3.2.3 Group authentication requirement

Ubiquitous network applications typically rely on the support of a large number of objects, and these terminals may be classified into a group. Hence a group authentication capability is an essential requirement for the ubiquitous network application server.

7.3.2.4 Privacy protection requirement

This UN capability ensures that user behaviour and communication contents are not disclosed. This information includes the communication content, user location, and user identity, etc.

7.3.2.5 Integrity protection requirement

In ubiquitous networks, malicious objects may inject or tamper application layer messages. Therefore, it is required that unauthorized deletion, insertion and copy operations cannot be performed in the UN application layer. Since the ubiquitous network is a heterogeneous network and the security mechanisms for this network are independent and inconsistent, end-to-end application layer integrity protection is therefore required for the communications crossing the ubiquitous network.

7.3.2.6 Confidentiality protection requirement

In ubiquitous networks, the variety of data and messages should only be viewed by authorized users. Confidentiality protection mechanisms provide UN with the capability to prevent unauthorized access to UN applications and prevent unauthorized reading of the application layer data. Since the ubiquitous network is a heterogeneous network and the security mechanisms for this network are independent and inconsistent, end-to-end application layer confidentiality protection is therefore required for the communications crossing the ubiquitous network.

7.3.2.7 Key protection requirement

The protection of keys can be achieved by dynamically downloading key parameters and dynamically updating login passwords.

7.3.2.8 Non-repudiation requirement

Non-repudiation mechanisms ensure that the communicating parties cannot falsely deny their actions or the time when they conducted these actions. For example, identity authentication, digital signature and time stamp mechanisms can be utilized to provide non-repudiation capability for the ubiquitous network.

7.3.2.9 Anti-replay requirement

This a mechanism that provides UN with the capability to resist replay attacks.

Table 2 – Relationship between security threats and security requirements of UN applications domain

Threat / Requirement	Eavesdrop	Tamper	Service abuse	Privacy disclosure	Replay attack	Signalling congestion	Repudiation attack
Integrity		√					
Confidentiality	√			√			
Authentication			√			√	
Privacy				√			
Anti-replay					√		
Non-repudiation							√

7.4 Other network security domains

7.4.1 Security threat

The security threat for other network domains is consistent with those of the existing mobile network and fixed network.

7.4.2 Security requirements

The security requirements for other network domains should satisfy those of the existing mobile network and fixed network.

7.5 End-to-end connectivity security domain

7.5.1 Security threats

The security threat for the end-to-end communication domain mainly includes MITM attacks, eavesdropping, illegally obtaining end-to-end encryption keys or impersonating end users or objects, etc. All these attacks may impair the security for end-to-end communication.

The following threats exist in the end-to-end communication domain.

7.5.1.1 Disclosure of privacy information

Through number analysis or location trace software, etc., it is not difficult to trace the user's location information or the user's home location information in the communication process of a ubiquitous network. Attackers may hence obtain and utilize this privacy information and launch position-associated attacks and endanger end-to-end communication security.

7.5.1.2 Man-in-the-middle attack

By means of MITM attack in an end-to-end communication process, the attackers from their intermediate nodes may launch attacks on any one end of the communication process. Through MITM attacks, communication data may be eavesdropped or sabotaged, leading to failure of providing regular UN services. For example, if the application domain is attacked the application domain services and applications may be compromised. If terminals are attacked, their ability to support applications and services may be compromised.

7.5.2 Security requirements

The security requirements for the end-to-end communication domain should be able to prevent MITM attacks, prevent illegally obtaining of encryption keys, and prevent illegal end users and fake objects from accessing the ubiquitous network.

7.5.2.1 Confidentiality requirement

The confidentiality of data in end-to-end communications should be ensured. For example, in order to protect the confidentiality of end-to-end media data communication, encryption algorithms should be used.

7.5.2.2 Integrity requirement

The integrity of the end-to-end communication data should be ensured. For example, in order to protect the integrity of end-to-end media data communication, integrity algorithms should be used.

7.5.2.3 Privacy requirement

User privacy information should be protected and illegally obtaining user privacy information should be prohibited. The user privacy information includes the user location information and the user identity information. The assurance of using legal terminals and using legal applications can effectively protect user privacy information from disclosure.

7.5.2.4 General requirement on authentication

Authentication and authorization mechanisms should be introduced to ensure end-to-end communication safety. Terminals should be able to authenticate legal services and applications, while services and applications should be able to authenticate legal terminals.

7.5.2.5 Key management requirement

Keys for end-to-end communication may be distributed from the network domain, or from the third-party key management centre or CA. Communication parties should ensure the safety of the communication keys through pre-shared keys or through a periodical change of encryption keys.

7.6 Interface security domain

7.6.1 Security threat

The security threat for the interface domain mainly includes illegal end users trying to access ubiquitous networks; using illegal or impersonation applications to try to access ubiquitous networks; other illegal networks trying to access ubiquitous networks; attackers from end-user domains; and network domains and other network domains trying to attack the ubiquitous network. All these attacks may impair the stability and security of the ubiquitous network.

7.6.2 Security requirements

The security requirements for the interface domain should be able to ensure that legal users have safe access to ubiquitous networks, legal applications have normal access to ubiquitous networks, and other legal networks have normal access to ubiquitous networks. The security requirements should be able to clean/cut off abnormal traffic attacks originating from the end-user domain, the network domain and other network domains.

Appendix I

Security framework progress from other SDOs

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

I.1 3GPP M2M security framework (b-3GPP TR33.868)

3GPP has defined M2M security framework in [b-3GPP TR33.868]. The detailed architecture is described in Figure I.1.

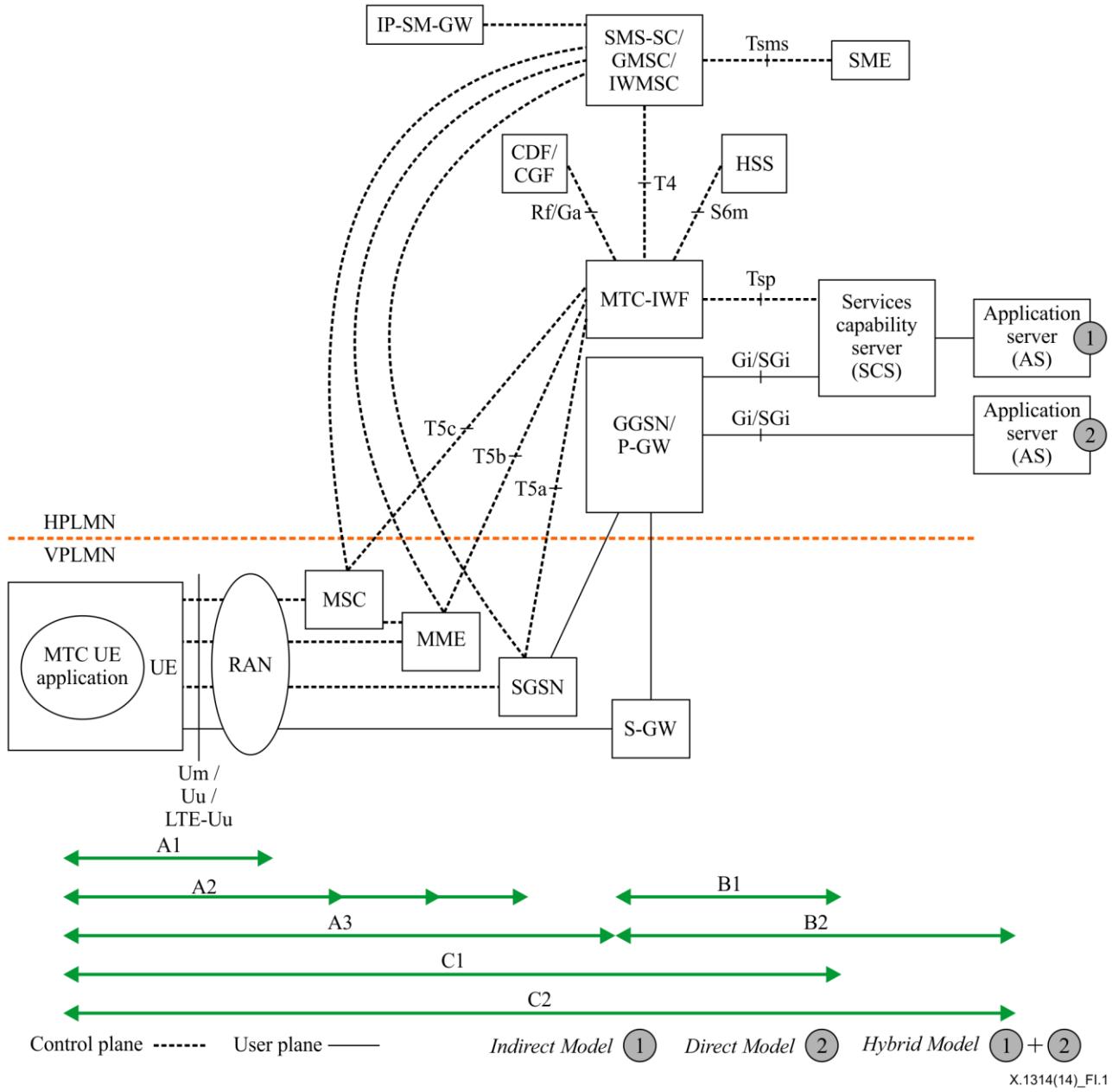

Figure I.1 – Potential high-level security architecture for 3GPP architecture for machine type communication (MTC)

The following defines potential high-level security architecture for MTC non-roaming architecture. Three different areas are defined. When analysing the security aspects of the key issues, the area(s) being impacted by the key issues should be considered. It should also be noted that the key issues analysed could be related to more than one area, e.g., items A and B.

A) Security for MTC communication between the user equipment (UE) and 3GPP network can be further divided into:

A1) Security for MTC communication between UE and radio access network (RAN);

A2) Security for MTC communication between UE and network access server (NAS);

A3) Security for MTC communication between UE and MTC-interworking function (IWF).

B) Security for MTC communication between the 3GPP network and an entity outside the 3GPP network can be further divided into:

B1) Security for MTC communication between the MTC server and 3GPP network in indirect deployment model. This can be further divided into security aspects when the MTC server is within the 3GPP network and when it is outside the 3GPP network;

B2) Security for MTC communication between the MTC application and 3GPP network in direct deployment model.

The communication between MTC server and MTC application is out of 3GPP scope.

C) Security for MTC communication between an entity outside the 3GPP network and UE can be further divided into:

C1) Security for MTC communication between the MTC server and UE in indirect deployment model;

C2) Security for MTC communication between the MTC application and UE in direct deployment model.

I.2 oneM2M security framework (b-oneM2M-TS-0003)

I.2.1 oneM2M functional architecture

The oneM2M functional architecture in Figure I.2 comprises of the following functions:

- Application Entity (AE): The AE represents an instantiation of application logic for end-to-end M2M solutions. Each AE is identified with a unique AE-ID. Examples of the AEs can be an instance of a fleet tracking application, a remote blood sugar monitoring application, a power metering application, or a controlling application.
- Common Services Entity (CSE): A CSE represents an instantiation of a set of "common service functions" of the M2M environments. Such service functions are exposed to other entities through reference points Mca and Mcc. Reference point Mcn is used for accessing underlying network service entities. Each CSE is identified with a unique CSE-ID.
- Examples of service functions offered by CSE include: data management, device management, M2M subscription management, and location services. Such "sub-functions" offered by a CSE may be logically and informatively conceptualized as common services functions (CSFs). The normative resources which implement the service functions in a CSE can be mandatory of optional.
- Underlying Network Services Entity (NSE): A NSE provides services from the underlying network to the CSEs. Examples of such services include device management, location services and device triggering. No particular organization of the NSEs is assumed.

NOTE – Underlying networks provide data transport services between entities in the oneM2M System. Such data transport services are not included in the NSE.

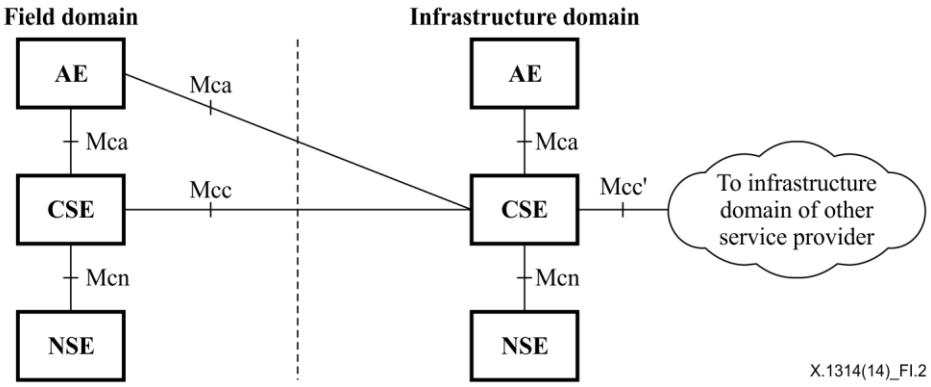

Figure I.2 – oneM2M functional architecture

I.2.2 High level overview of the security architecture in oneM2M

The architecture consists of following layers:

- Security functions layer

  This layer contains a set of security functions that are exposed at reference point Mca and Mcc. These security functions can be classified into six categories; they are identification, authentication, authorization, security association, sensitive data handling and security administration.

- Security environment abstraction layer

  This layer implements various security capabilities such as key derivation, data encryption/decryption, signature generation/verification, security credential read/write from/to the secure environments, and so on. The security functions in the security functions layer invoke these functions in order to do the operations related to the secure environments. In addition this layer also provides physical access to the secure environments. Implementation of this is out of scope of the present document. This layer is not specified in the initial release but is expected to be considered in future releases.

- Secure environment layer

  This layer contains one or multiple secure environments that provide various security services related to sensitive data storage and sensitive function execution. The sensitive data includes SE capability, security keys, local credentials, security policies, identity information, subscription information, and so on. The sensitive functions include data encryption, data decryption, and so on. Implementation of secure environments is out of scope of the present document.

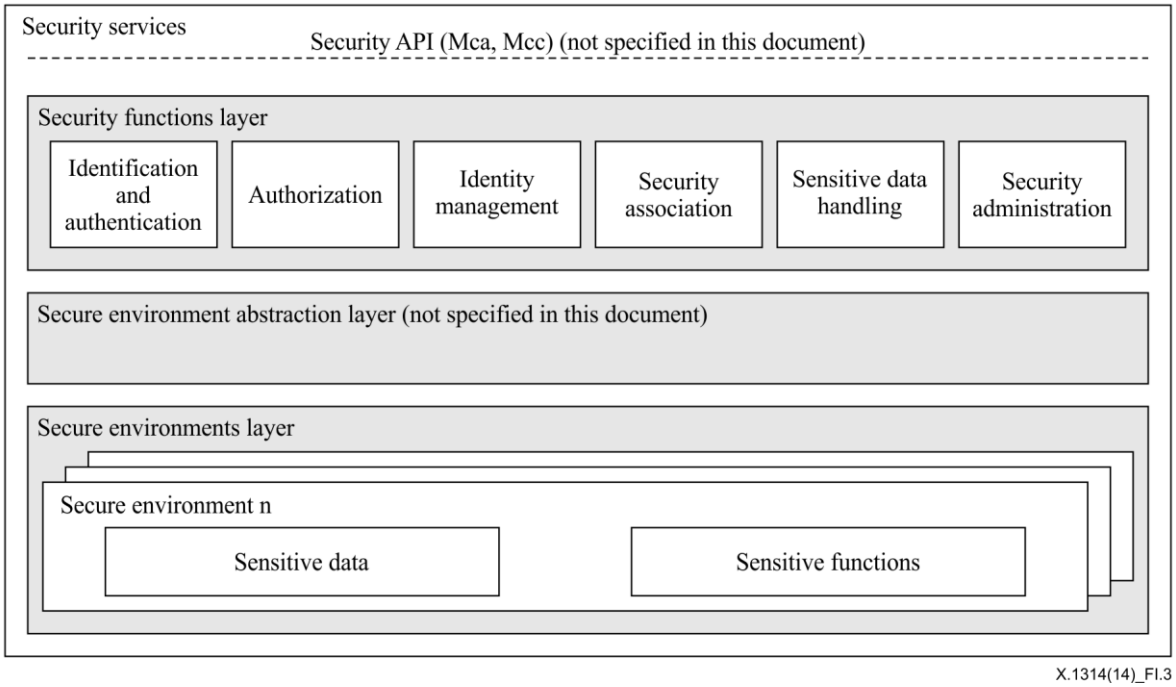

Figure I.3 – High level overview of the Security architecture in oneM2M

Design principles:

- Security services are modular and configurable according to the needs of the hosting CSE, its supported reference points and its purpose.
- The architecture is split into several components and sub-components providing a modular design. With this design, mapping of the architecture to different nodes and entities is enabled.
- Depending on the requirements of each entity, security should consist of components relevant to fulfil the requirements of the respective node or entity and the intended use case.
- The architecture may need to be adapted to be suitable for implementation in different entities. For example, the architecture can be mapped to different device classes.
- The security administration component shall enable administration of all sensitive resources (data and functions) and shall also allow configuration and extension of security services itself.
- The secure environment within the CSE is accessed via the secure environment abstraction layer and shall hold all sensitive resources.

I.2.3 Security layers

I.2.3.1 Security service layer

The security service layer provides the following services:

- Access management:
  - authorization;
  - authentication;
  - access control.
- Sensitive data handling:
  - sensitive functions protection;
  - secure storage.
- Security association establishment:

  - secure connection via secure session establishment;
  - secure connection via object security.
- Security Administration (including remote security provisioning)
- Identity Protection

Each of these services provides functions and resources on the Security Service and Administration API.

I.2.3.2 Secure environment abstraction layer

The secure environment abstraction layer (not specified in the present document) provides access to the secure environment via a general security transport API. A Plug-in associated to the type of secure environment shall provide physical/logical connectivity to the secure environment. The secure environment abstraction Layer shall also be accessible on the service layer.

Bibliography

[b-ITU-T Q.1300] Recommendation ITU-T Q.1300 (1995), *Telecommunication applications for switches and computers (TASC) – General overview*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.902] Recommendation ITU-T X.902 (2009) | ISO/IEC 10746-2:2009, *Information technology – Open Distributed Processing – Reference model: Foundations*.

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks*.

[b-ITU-T X.1312] Recommendation ITU-T X.1312 (2011), *Ubiquitous sensor network middleware security guidelines*.

[b-ITU-T X.1313] Recommendation ITU-T X.1313 (2012), *Security requirements for wireless sensor network routing*.

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.

[b-ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-3GPP TR33.868] 3GPP TR33.868 Release 12 (2013), *Security aspects of Machine-Type Communications (MTC).*

[b-oneM2M-TS-0003] TS-0003-Security_Solutions-V-0.7.1 (2014), *oneM2M Security Solutions*.

[b-oneM2M-TS-0002] oneM2M-TS-0002-V-0.6.2 (2013), *oneM2M Requirements Technical Specification*.

[b-oneM2M-TS-0001] oneM2M-TS-0001-V-1.0.0 (2014), *oneM2M Functional Architecture*.

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

Printed in Switzerland
Geneva, 2015