ETSI TR 102 725 V1.1.1 (2013-06)

Technical Report

Machine-to-Machine communications (M2M); Definitions

Reference

DTR/M2M-00004

Keywords

M2M, taxonomy, vocabulary

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Machine-to-Machine communications (M2M).

The present document is designed to be referenced by the other Technical reports and Technical Standards (TS) developed by ETSI TC M2M. This is a TR and therefore the content is informative, but when the present document is referenced by a TS, the referenced definitions become normative with respect to the content of the referencing TS.

1 Scope

The purpose of the present document is to identify specialist technical terms used within the ETSI TC M2M for the purposes of specifying the M2M system. The motivations for this are:

- To ensure that editors use terminology that is consistent across specifications.
- To provide a reader with convenient reference for technical terms that are used across multiple documents.
- To prevent inconsistent use of terminology across documents.

The present document is a collection of terms, definitions and abbreviations contained in the baseline documents of the ETSI TC M2M framework. The present document provides a tool for further work on ETSI TC M2M technical documentation and facilitates their understanding.

The terms, definitions and abbreviations as given in the present document are either imported from existing documentation (ETSI, 3GPP, ITU or elsewhere) or newly created by the ETSI TC M2M experts whenever the need for precise vocabulary was identified.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (MID - Measuring Instruments Directive).

NOTE: Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0022:EN:NOT.

[i.2] IETF RFC 5789: "PATCH Method for HTTP".

3 Terms and definitions

0-9

Void

A

Abstract Application Information Model: Information Model of common functionalities abstracted from a set of Device Application Information Models.

Abstraction: the process of mapping between a set of Device Application Information Models and an Abstract Application Information Model according to a specified set of rules.

Access Right: permission to control resources for operations like creation, deletion, retrieval, update and discovery.

AccessRight Resource: specialized resource dedicated to store lists of identifiers associated to permission flags, enabling access control to resources for operations like creation, deletion, retrieval, update and discovery. Resources are access controlled by means of an AccessRight resource identified by a URI.

Accounting: refers to the tracking of network resource consumption for the purpose of capacity and trend analysis, cost allocation, billing, etc. In addition, it may record events such as authentication and authorization failures, and include auditing functionality, which permits verifying the correctness of procedures carried out based on accounting data. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user or other entity, the nature of the service delivered, when the service began, and when it ended, and if there is a status to report.

Actuator: is an object which performs actions. Actuation is the mechanism by which an application can act upon an environment. An actuator might act on the flow of a gas or liquid, on the electricity distribution, through a mechanical operation for example. Dimmers and relays are examples of actuators. The decision to activate the actuator may come from any Object or M2M Device (including the M2M Gateway).

Additional Functionality (in the context of smart metering): in the context of the Smart Metering Mandate M/441 "Additional Functionality" means functionality, that a smart metering system provides, over and above what is already covered by the Measuring Instruments Directive [i.1]. Basically this refers to the capabilities that are provided by a smart meter, over and above what a conventional meter can provide.

Announced Resource: the content of this resource refers to a resource hosted by the Hosting SCL (Master/original Resource).

Announced-to SCL: an SCL that contains the announced resource (a resource could be announced to multiple SCLs).

Application: entity (typically in software) designed to perform specific tasks on behalf of /in order to help a user to operate for a specific goal.

Application Information Model: the information model of an Application, including data and methods. An Application Information Model may have Representations expressed in specific operational protocols.

Attribute: is meta-data that provides properties associated with a resource representation.

B

Void

C

Caching: a mechanism for the temporary storage of data to increase performance.

Certificate: in cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind a public key with an identity.

Collection: a collection is a set of resources of the same type and with the same parent resource.

Common Procedures: common procedures describe stage 3 protocol operations that are common to more ETSI M2M procedures. They are referenced in the respective procedure descriptions.

Computational Objects: are containers for functionality. Computational objects could comprise of software, hardware or combinations thereof. Among other possibilities, a computational object could be a client, a server, or a combination thereof.

Connected Objects: objects that are accessible by or can communicate with other objects are termed connected objects.

Container: a container is a resource used for storing M2M data/objects (in Content Instance Resources) in an organized way following specific access rules.

Content Instance: is a resource specialized to store M2M data, under a content instances collection resource belonging to a parent container resource.

Controller: a controller is an object which controls actuators. Control decisions may be based on sensor readings, sensor events, scheduled actions or incoming commands from the Internet or other backbone networks. A gateway may be a controller.

D

Data type: is the definition of an information storage format.

Device: an equipment that may collect a set actuators and sensors that have embedded electronic computing and communication capability.

Device Application Information Model: technology (e.g. ZigBee®) specific Information model of the physical device.

Device Service Capabilities Layer: M2M Service Capabilities in the M2M Device.

E

Void

F

Void

G

Gateway: an equipment with electronic computing and communication capability aimed to translating, sharing and transferring information between two types of communicating entities, or aimed to perform some routing and multiplexing function between the two communicating entities.

Gateway Service Capabilities Layer: M2M Service Capabilities in the M2M Gateway.

Group hosting SCL: the SCL where the addressed Group Resource resides.

Group Resource: a resource which defines a collection of resources and provides the links to access the resources in the collection.

H

Hosting SCL: the SCL where the addressed (Master/original Resource) resource resides.

I

Independent Security Element: a discrete hardware component which can be removable and which provides secure storage and secure execution. A Device or Gateway can support one or more Independent Security Elements.

Information Object: an Information Object is a digital item or group of items referred to as a unit, regardless of type or format, which can be addressed or manipulated as a single object. An Information Object provides communicating Application Entities with a common view of the information to be exchanged.

Integrity Validation: a process whereby the integrity of identified internal functions of an M2M Device or M2M Gateway are validated (implicitly or explicitly) such that the M2M Core can be sure of the Device/Gateway integrity. IVal may consist of (a) trustworthy measurements of identified internal function states, followed by (b) trustworthy verification of the measurements using trusted references. Failed verification is interpreted as unauthorized change to the M2M Device/Gateway integrity.

Issuer: is the actor performing a request.

J

Void

K

Key: in cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Key Hierarchy: when a cryptographic key is derived from others applying algorithms, the result is a hierarchy of keys.

Key Realization: is the derivation of a new key from an existing one applying algorithms.

L

Local SCL: the SCL where an Application or a SCL registers to.

Long Polling: a method which gives an option for non-server capable clients to still receive asynchronous notifications.

M

M2M Applications: applications that run the service logic and use Service Capabilities accessible via open interfaces.

M2M Application Service: an M2M Application Service is realized through the service logic of an M2M Application and is **operated** by the end user or an M2M Application Service Provider.

M2M Application Service Provider: is an entity (e.g. a company) that provides M2M Application Services in the M2M System to the end user.

M2M Area Network: an M2M Area Network provides connectivity between M2M Devices (both compliant and non-compliant to ETSI M2M) and ETSI M2M Gateways.

M2M Authentication Server: a secure server used to store security credentials.

M2M Communications: refer to physical telecommunication based interconnection for data exchange between two ETSI M2M compliant entities, like: device, gateways and network infrastructure.

M2M Communication Module: residing on a M2M Device, the M2M Communication Module implements the communication part of the M2M device.

M2M Device: a device that runs application(s) using M2M capabilities and network domain functions. A M2M device is made at least of one M2M Device Application and one M2M Communication Module. A M2M Device may contain one or more M2M Communication Module(s) and one or more M2M Device Application(s).

M2M Device Application: application residing on the M2M Device that runs the service logic and use Service Capabilities accessible via open interfaces (dIa interface of M2M core).

M2M Gateway: equipments using M2M Capabilities to ensure M2M Devices interworking and interconnected to the Network and Application Domain. The M2M Gateway may also run M2M applications. M2M Gateway functionality can be collocated with M2M Device(s).

M2M Network Applications: applications residing in the Network and Applications domain that run the service logic and use Service Capabilities accessible via open interfaces (mIa interface of M2M core).

M2M Node: is a logical representation of the M2M component in the M2M Device, M2M Gateway or the M2M Core. Such components include one SCL, and optionally a M2M Service Bootstrap function and a M2M Service Connection function.

M2M Root Key: M2M Root Key (Kmr): The master secret key used for mutual authentication and key agreement between the D/G M2M Nodes and M2M Nodes in the M2M Core of the M2M Service Provider. It is also used to derive M2M Service Connection credentials for establishment of secure communication.

M2M Service: is the set of functionalities that a M2M Service Capability Layer makes available through the standardized interfaces.

M2M Service Bootstrap Function: facilitates the bootstrapping of permanent M2M service layer security credentials in the M2M Device (or M2M Gateway) and the M2M Service Capabilities in the Network Domain.

M2M Service Connection Key (Kmc): the shared secret key, derived from M2M Root Key (Kmr), used for setting up secure data sessions between the D/G M2M Node and the Service Provider M2M Network Node.

M2M Service Provider: is an entity (e.g. a company) that provides M2M Services of the M2M System to a M2M Application Service Provider or to the end user.

M2M System: indicates in a general way M2M entities like: device, gateway and network infrastructure, equipped with M2M Service Capabilities.

Mapping Functions: are Service Capabilities functionalities specialized to map request/indication primitives into messages for M2M communications. Also received messages are mapped to response/confirm primitives.

Member Hosting SCLs: one or multiple SCLs where member resources of a group resource reside.

Member Resource: a resource belonging to the collection defined by a Group Resource.

Methods: in a RESTful architecture, there are four basic methods - so called "Verbs" - that could be applied to resources: CREATE, RETRIEVE, UPDATE and DELETE.
In addition the following additional verbs were introduced inM2M: NOTIFY and EXECUTE.

N

Network Service Capabilities Layer: M2M Service Capabilities in the Network Domain.

Notification: is a message sent when a subscribed to resource is modified according to specific filter criteria condition. The Notification is sent to the URI indicated at the subscription.

O

Objects: are abstract containers for information and/or functionality within a M2M system. For instance information objects could be containers for measured quantities (temperature, consumed energy) or status information (switch is ON/OFF). Furthermore, objects can be containers for functionality, also known as computational objects. Computational objects could comprise of software, hardware or combinations thereof. Among other possibilities, a computational object could be a client, a server, or a combination thereof. As a client the object receives services from servers; as a server the object offers services to other objects via well-defined interfaces. Examples of computational objects are remote devices, e.g. sensors, actuators, RFID tag, RFID readers, displays, etc. Other examples for objects containing functionality are service objects as e.g. a weather service, a conversion service, etc.

P

Partial Addressing: the parts of the resource are identified using normal URIs, where the components correspond to the names of the attributes.

Primitive: is a structured information set by an Application or Service Capability Layer that is mapped into messages transferred across an M2M Communication path.

Primitive Attribute: is meta-data that provides properties associated with a Primitive.

Proxy: a server that acts as an intermediary for requests from clients seeking resources from other servers.

Q

Void

R

Re-targeting: technique applied to RESTful request that modifies the target URI to a virtual resource outside the initially address Service Capability Layer. The purpose of this is to enable the access to non ETSI M2M standardized systems aiming at facilitate the interworking with them, e.g. wireless sensor networks.

Receiver: represents the actor that receives a request from an issuer. A receiver is a SCL or an Application.

Representation: expression of an Application Information Model in terms of the operational protocol of a specific technology (e.g. ETSI M2M, ZigBee®, etc.).

Representation Interworking: is the process of mapping and synchronizing multiple Representations of an Application.

Requesting entity: the requesting entity is the original issuer of a RESTful request. It can be either an Application or a Service Capability Layer.

Resource: is a uniquely addressable entity in the RESTful architecture. A resource has a representation that can be transferred and manipulated with the verbs.

Resource Attribute: the information field of a resource with structured data content.

REST: the REpresentational State Transfer is a style of software architecture for distributed hypermedia systems such as the World Wide Web. RESTful architectures consist of clients and servers. Clients initiate requests to servers; servers process requests and return appropriate responses. Requests and responses are built around the transfer of representations of resources.

S

Secured Environment: a functionality enabling secure execution of Sensitive Functions and tamper-resistant storage of Sensitive Data, such as for the provisioning, derivation, storage and management of cryptographic keys which are used at the M2M service layer.

A Secured Environment can be implemented as an Independent Security Element or as an integrated function in a microprocessor system. A Secured Environment can support multiple independent Secured Environment Domains, corresponding to concurrently supported, cryptographically isolated Sensitive Data and Sensitive Functions controlled by different stakeholders.

The security properties of the Secured Environment are provided by certain functions which are secure, for instance protected by secure hardware.

Within an M2M Device or M2M Gateway, one or several components can support a Secured Environment functionality.

Secured Environment Domain: a logical entity that is securely isolated from other Secured Environment Domains, whether they are inside different Secured Environments or are inside a single Secured Environment. Sensitive Functions (including the storage and handling of sensitive data such as credentials and key material) are protected inside a Secured Environment Domain controlled by its stakeholder. The M2M Service Provider owning an M2M Node on an M2M Device/Gateway controls its own Secured Environment Domain. Providers of M2M applications may control an independent Secured Environment Domain on an M2M Device/Gateway.

Sensitive Data: data which require protection from unauthorized disclosure or modification.

Sensitive Functions: functions which require protection from monitoring or tampering or unauthorized execution. Secure execution and storage of Sensitive Data are both examples of Sensitive Functions.

Sensor: is a device that measures a physical quantity and converts it to numeric value that can be read by a program or a user. Sensed data can be of many types: electromagnetic (e.g. current, voltage, power, resistance) , mechanical (e.g. pressure, flow, liquid density, humidity), chemical (e.g. oxygen, carbon monoxide, etc.), acoustic (e.g. noise, ultrasound).

Service Bootstrap Procedure: is a procedures used to provision a secret key called M2M Root Key in the D/G M2M Node and in the M2M Authentication Server (MAS). In addition to provisioning the M2M Root Key, the M2M Service Bootstrap procedures may result in provisioning any combination of the following parameters to the D/G M2M Node:

- An M2M-Node-ID.
- An SCL-ID.
- A list of one or more NSCL identifiers that the D/G M2M Node uses as the next point of contact.

Service Capabilities: Service Capabilities provide functions that are to be shared by different applications. Service Capabilities expose functionalities through a set of open interfaces. Additionally, Service Capabilities use Core Network functionalities. Service Capabilities also allow to simplify and optimize applications development and deployment and to hide network specificities to applications. Service Capabilities may be M2M specific or generic, i.e. providing support to other than M2M applications. Examples include: Data Storage and Aggregation, Unicast and Multicast message delivery, etc.

Service Capability Feature: a set of function provided by a service Capability, exposed to application via an application service interface.

Service Capabilities Layer: refers to any of the following: Network Service Capabilities Layer, Gateway Service Capabilities Layer, Device Service Capabilities Layer.

Service Primitive: abstract, implementation independent interaction between a (service-) user and a (service-) provider which conveys parts of or a complete service capability feature.

Set Of Things Representation: it is a group of Thing Representations that share a common property or functionality. A Thing Representation can belong to several Set Of Things Representations.

As an example, it can contain Thing Representations of:

- Things that radiate heat (radiators, electric appliances and even human beings).
- Things that provide lighting (lights, display screens and windows).

Status Code: a Service Primitive attribute present in confirm/response primitives to report the status of corresponding request/indication primitive processing.

Sub-Resource: also called child resource. It is a resource that has a containment relationship with the addressed (parent) resource.

T

Target ID: URI of an addressed resource in a request/indication Service Primitive.

Thing: an element of the environment that is individually identifiable in the M2M system.

Thing Representation: it is the instance of the informational model of the Thing in the M2M System. A Thing Representation provides means for applications to interact with the Thing.

Translation: is the combination of Abstraction and Representation Interworking.

Trusted Environment: a logical entity in an M2M Device or M2M Gateway which performs Sensitive Functions, specifically for the purpose of Integrity Validation. A Trusted Environment (TrE) requires a root of trust which is implemented as an integrated function in an M2M Device or M2M Gateway, so as to initiate the chain of trust for computation of software integrity values. The verification part of software integrity validation (IVal) is performed in a Secured Environment which can either be integrated in the Trusted Environment or securely connected to it.

The security properties of the TrE are provided by certain functions which are secure, for instance protected by physically non-removable secure hardware. Relying parties that trust the Root of Trust can also trust the functions of the TrE.

A TrE is initialized in a secure start up process when an M2M Device or M2M Gateway is initialized.

An M2M Device or M2M Gateway can support one or more TrEs.

U

Use Case: Use Cases describe a system from the actor/user point of view. An actor/user in this sense may be:

- an end-user (people);
- an organization like a service provider or an operator;
- another system interacting with the system being defined.

Use Cases treat the system as a black box, and the interactions with the system, including system responses, are perceived as from outside the system. A (System-) Use Case describes what the actor achieves interacting with the system. For this reason it is recommended that a (System-) Use Case description begins with a verb (e.g., create voucher, select payments, exclude payment, cancel voucher).

Use Cases should not be confused with the functionalities, features, requirements of the system under consideration. A Use Case may be related to one or more functionalities, requirements. A functionality or requirement may be related to one or more Use Cases.

V

Verbs: see Methods.

W

Void

X

Void

Y

Void

Z

Void

4 Abbreviations

0-9

3GPP	3rd Generation Partnership Project

A

AAA	Authentication, Authorization and Access
ACL	Access Control List
ACS	Auto Configuration Server
AE	Application Enablement
AES	Advanced Encryption Standard
API	Application Program Interface
AVP	Attribute Value Pair

B

B-TID	Bootstrapping Transaction IDentifier
BSF	Bootstrapping Server Function

C

CB	Compensation Brokerage
CM	Configuration Management
CN	Core Network
CoAP	Constrained Application Protocol
CRUD	Create, Retrieve, Update and Delete
CS	Communication Selection

D

DA	Device Application
D'A	Device' Application
D/GA	Device or Gateway Application
DA/GA	Device or Gateway Application
D/GSCL	Device/Gateway Service Capabilities Layer
DIP	Device Interworking Proxy
DNS	Domain Name System
DM	Device Management
DSCL	Device Service Capabilities Layer
DSL	x Digital Subscriber Line
DTLS	Datagram Transport Layer Security

E

EAP	Extensible Authentication Protocol
EMSK	Extended Master Session Key
ETAG	Entity Tag
EXI	Efficient XML Interchange

F

FQDN	Fully Qualified Domain Name
FM	Fault Management
FFS	For Further Study

G

GA	Gateway Application
GBA	Generic Bootstrapping Architecture
GC	Generic Communication
GIP	Gateway Interworking Proxy
GSCL	Gateway Service Capabilities Layer

H

HDR	History and Data Retention
HMAC	Hash-based Message Authentication Code
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTP PATCH	PATCH method for HTTP (RFC 5789 on Partial Addressing [i.2])

I

IBAKE	Identity-Based Authenticated Key Exchange
IBE	Identity Based Encryption
IBEEC	IBE Elliptic Curve
IEEE	Institute of Electrical and Electronics Engineers
IMPI	IP Multimedia Private Identity
IP	Interworking Proxy
ISE	Independent Security Element
IVal	Integrity Validation

J

JSON	JavaScript Object Notation

K

KDF	Key Derivation Function
KGF	Key Generation Function
KMC	M2M Connection Key
KMR	M2M Root Key
Ks	M2M Session Key

L

LCS	LoCation Services

M

M2M	Machine to Machine
M2MPoC	M2M Point of Contact
MAC	Media Access Control
MAS	M2M Authentication Server
ME	Mobile Equipment
mIa	M2M application Interface
mId	M2M device Interface
MIME	Multipurpose Internet Mail Extensions
MLP	Mobile Location Protocol
MLS	Mobile Location Service
MO	Management Objects
MTU	Maximum Transmission Unit
MSBF	M2M Service Bootstrap Function
MTOM	Message Transmission Optimization Mechanism
MTOM/XOP	MTOM with XML-binary Optimized Packaging

N

NA	Network Application
NAF	Network Application Function
NAT	Network Address Translation
NIP	Network Interworking Proxy
NIST	National Institute of Standards & Technology
NSCL	Network Service Capabilities Layer

O

OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
OMA-DM	Open Mobile Alliance Device Management
OTA	Over The Air

P

PCI	Peripheral Component Interconnect
PAN	Personal Area Network
PANA	Protocol for carrying Authentication for Network Access
PAR	PANA Authentication Request
PM	Performance Monitoring
PoC	Point of Contact
PPP	Point-to-Point Protocol
PSK	Pre Shared Key
PTA	PANA Termination Answer
PTR	PANA Termination Request

Q

Void

R

RADIUS	Remote Authentication Dial in User System
RAR	Reachability, Addressing and Repository
RCAT	Request Category
REM	Remote Entity Management
REST	REpresentational State Transfer
RFC	Request For Comments
RO	Read-Only by client, set by the server
RPC	Remote Procedure Call
RW	Read/Write by client

S

SAF	Store And Forward
SC	Service Capability
SCL	Service Capability Layer
SEC	Security Capability
SIM	Subscriber Identity Module
SIM/AKA	SIM / Authentication and Key Agreement
SOTR	Set Of Things Representation

T

TCP	Transmission Control Protocol
TrE	Trusted Environment
TLS	Transport Layer Security
TM	Transaction Management
TOE	Telco Operator Exposure
TRPDT	Tolerable Request Processing Delay Time
TTP	Trusted Third Party

U

UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USS	User Security Settings

V

Void

W

WO	Write-once, can be provided at creation, but cannot be changed anymore

X

XCAP	XML Configuration Access Protocol
XDMS	XML (extensible markup language) Data Management Server
XML	Extensible Markup Language
XUI	XCAP User Identifier
XSD	XML Schema Definition

Y

Void

Z

Void

Annex A: Bibliography

ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

ETSI TS 102 690: "Machine-to-Machine communications (M2M); Functional architecture".

History

Document history		
V1.1.1	June 2013	Publication