ETSI TR 102 966 V1.1.1 (2014-02)

Technical Report

Machine-to-Machine communications (M2M); Interworking between the M2M Architecture and M2M Area Network technologies

Reference
DTR/M2M-00014ed111

Keywords
interworking, M2M, service

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).

1 Scope

The present document collects and evaluates implementation profiles for interworking with M2M Area Network technologies.

An implementation profile is defined, for the purpose of the present document, as the description on how the ETSI M2M architecture can be used to achieve interworking. Each implementation profile is evaluated against deployment scenarios and applicable technologies in order to identify the most suitable for the specific conditions.

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

[i.2] ETSI TS 102 921: "Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces".

[i.3] IEEE 802.15.4-2003: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)".

[i.4] CEN EN 13757: "Communication systems for meters and remote reading of meters".

[i.5] CEN EN 13757-3: "Communication systems for and remote reading of meters - Part 3: Dedicated application layer".

[i.6] ISO 8601:2004: "Data elements and interchange formats -- Information interchange -- Representation of dates and times".

[i.7] IETF RFC 1006: "ISO Transport Service on top of the TCP Version: 3".

[i.8] IETF RFC 5023: "The Atom Publishing Protocol".

[i.9] ISO/IEC 14543-3-10:2012: "Information technology -- Home Electronic Systems (HES) -- Part 3-10: Wireless Short-Packet (WSP) protocol optimized for energy harvesting -- Architecture and lower layer protocols".

[i.10] OASIS.OBIX_1_1: "OASIS oBix semantic conventions, version 1.1".

[i.11] ASHRAE.CSML_1_0: "ASHRAE 135 annex am Control System Modelling Language (CSML) semantic conventions".

[i.12] IETF RFC 4287: "The Atom Syndication Format".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AN	Area Network
ASHRAE	American Society of Heating, Refrigeration, and Air-conditioning Engineers
ATOM	XML document format defined in RFC 4287 [i.12]
COV	Change Of Value
CSML	Control System Modelling Language
DA	Device Application
DDNS	Dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DIF	Data Information Field
DIP	Device Interworking Proxy
DNS	Domain Name System
DPT	Data Point Type (KNX™ standard)
DSCL	Device Service Capability Layer
GA	Gateway Application
GENA	General Event Notification Architecture
GIP	Gateway Interworking Proxy
GSCL	Gateway SCL
HAN	Home Area Network
IN	INPut
IP	Internet Protocol
IPA	Interworking Proxy Application
IPU	Interworking Proxy Unit
ISO	International Standard Organization
KNX™	Konnex protocol maintained by the KNX™ Association
LAN	Local Area Network
MAC	Medium Access Control (Layer)
MAN	M2M Area Network
NA	Network Application
NA/DA	Network Application/Device Application
NIP	Network Interworking Proxy
NSCL	Network SCL
OASIS	Organization for the Advancement of Structured Information Standards
OUT	OUTput
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
REST	REpresentational State Transfer
RF	Radio Frequency
SCL	Service Capability Layer
SLIP	Serial Line IP
TBD	To Be Defined
TC	Technical Committee
UCP	User/Universal Control Point
UDN	Unique Device Name
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VIF	Value Information Block

WAN	Wide Area Network
XML	Extensible Markup Language
ZC	ZigBee® Coordinator
ZCL	ZigBee® Cluster Library
ZED	ZigBee® End Device
ZGD	ZigBee® Gateway Device
ZR	ZigBee® Router

4 Scenarios for interworking

Interworking is one of the main caracteric of the exploitation of the usage of the ETSI M2M solution. The scenarios for interworking described in the present document make use of the ETSI TC M2M architecture as shown below. The interworking makes use of GIP, NIP and DIP capabilities which are seen by the SCLs as specialized applications dedicated to the semantic data model interworking.

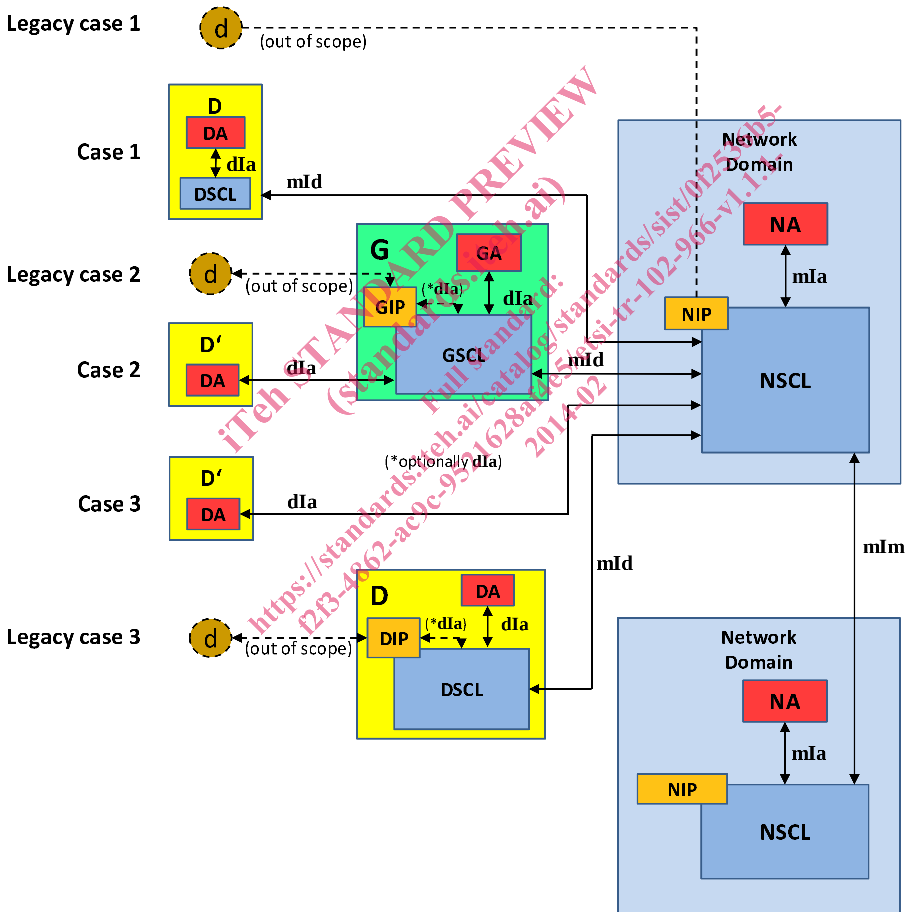

Figure 4.1: Mapping of reference points to different deployment scenarios

5 scenarios for interworking have been identified in the following table, each one applicable to different deployment context. Guidelines for data model interworking between ETSI M2M and specific area network technologies are provided in the rest of the present document.

Scenario 1: transparent retargeting		
Type of device	**d**	**Notes**
Application on device (d, non using dIa)	Specific technology aware	
Application on Network	Specific technology aware	The application is specific for the interworked technology, A specific adaptation is needed to use mIa.
Mechanism	Interworking at the G/D with simple retargeting	
Security impact	Use technology-specific security to the Gateway, independently of M2M Service layer security	Decryption(/reencryption) required at Gateway, i.e. Gateway acts as Aggregator, to extend Service Layer security end-to-end.
Leverage on M2M architecture capabilities	minimum	GIP/DIP is an application using standard dIa towards the G/DSCL.
Deployment scenario example	This interworking scenario is using ETSI M2M as a sort of pipe to carry the specific protocols, so the level of interaction with the ETSI M2M resource management capabilities (Access Rights, security, management, etc.) is limited by visibility on the objects in the interworked technology, but with the relevant advantage but that interworked protocols are preserved. One typical scenarios is the deployment of a specific technology on top of a consolidated ETSI M2M deployment, to leverage of already massively installed ETSI M2M D/G.	

Scenario 2: Retargeting with elements interworking		
Type of device	**d**	**Notes**
Application on device (d, non using dIa)	Specific technology aware	
Application on Network	Specific technology aware	The application is specific for the interworked technology, A specific adaptation is needed to use mIa.
Mechanism	Interworking at the G/D based on retargeting and use of ETSI compliant resources	GIP/DIP is an application using standard dIa towards the G/DSCL.
Security impact	Use technology-specific security to the Gateway	Decryption(/reencryption) required at Gateway, i.e. Gateway acts as Aggregator, to extend Service Layer security end-to-end.
Leverage on M2M architecture capabilities	Yes, level depends on specific solutions	
Example of applicability	This interworking scenario is similar to scenario 1 but is leveraging on the functionality offered by ETSI M2M by means of a more detailed mapping of elements (sensors. Actuators, etc) on ETSI M2M resources. It also allows other applications (e.g. native ETSI M2M application) to interact actively with the elements of the interworked technology that are stored and manipulated by the SCLs. Also in this case the interworked protocols are preserved. One typical scenario is the deployment of a specific technology that leverages on ETSI M2M for the interaction with the communication system.	

Scenario 3: Interworking at the Device/Gateway		
Type of device	**d**	**Notes**
Application on device (d, non using dIa)	Specific technology aware	
Application on Network	Independent from Specific technology	The application is ETSI M2M native and independent for the interworked technology.
Mechanism	Full Interworking at the G/D	GIP/DIP is an application using standard dIa towards the G/DSCL.
Security impact	May rely on technology-specific security over MAN, but interworking with M2M service layer security is possible	Gateway may act according to any of the scenarios in clause 6.
Leverage on M2M architecture capabilities	Full	
Example of applicability	This interworking scenario is making the network applications independent from the area network technologies. One typical scenarios is the case of an application that has to deal with multiple area network technologies (e.g. in case of long term deployments when the available technologies are changing), so the interworking is confinated to the new deployments.	

Scenario 4: Native interworking on dIa		
Type of device	**D'**	**Notes**
Application on device	Independent from Specific technology	The application is ETSI M2M native and independent for the interworked technology.
Application on Network	Independent from Specific technology	The application is ETSI M2M native and independent for the interworked technology.
Mechanism	dIa transport on binding layer between D' and G	Natively supported in ETSI M2M.
Security impact	Enables End-to-end encryption to/from D' devices	Gateway may act according to any of the scenarios in clause 6.
Leverage on M2M architecture capabilities	Full	
Example of applicability	This is the case of a technology supporting HPPT/COAP in case of deployment of ETSI M2M compliant DA and NA. It allows a complete independence of applications from area network technology. Typical.	

Scenario 5: Network based interworking		
Type of device	**d**	**Notes**
Application on device (d, non using dIa)	Specific technology aware	
Application on Network	Independent from Specific technology	The application is ETSI M2M native and independent for the interworked technology.
Mechanism	NIP interworking	Application needs to be able to handle encrypted data in containers.
Security impact	Use technology-specific security over MAN	Limited confidentiality as interworking may require application-related information to be exposed in the service layer.
Leverage on M2M architecture capabilities	low, level depends on specific solutions	
Example of applicability	This is to interwork with completely specific solutions already deployed without touching the G/D. One typical scenario is the introduction of ETSI M2M compliant solution for new services reusing already deployed legacy D/G.	

5 Interworking with legacy devices (d)

5.1 Implementation profile 1

5.1.1 Entity-relation representation of the M2M area network

Figure 5.1 provides a resource-entity model that represents an M2M area network as well as its relationship to an Interworking Proxy Application (IPA).

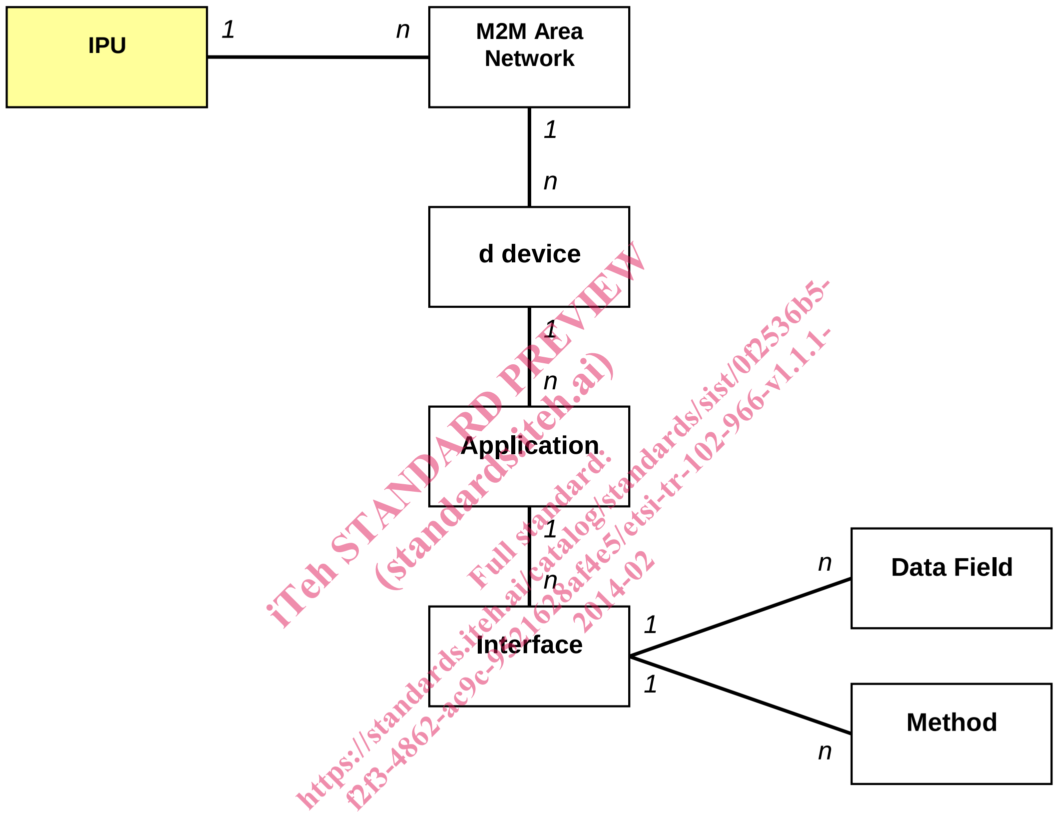

Figure 5.1: Generic entity-relation diagram for an IPU and an M2M Area Network running legacy d devices

This entity-relation diagram is applicable to the following M2M Area Networks:

- ZigBee®
- DLMS/COSEM
- Zwave
- BACnet
- ANSI C12
- mBus

5.1.2 Mapping principles

NOTE: The mapping principles proposed in the present document are initial ones, some others may exist.

This clause describes the mapping principles that are used to map a generic M2M Area Network into a structured tree of ETSI M2M resources in this implementation profile.

More specifically, the IPU is responsible to:

- discover the M2M Area Network structure;
- create an ETSI M2M resource structure representing the M2M Area Network structure in the ETSI M2M Service Capability Layer; and
- manage the ETSI M2M resource structure in case the M2M Area Network structure changes.

In order to facilitate the navigation through the various resources representing the M2M Area Network structure, created by the IPU, a specific format for the searchString attribute of the resources is used. This specific format is referred to as a Tag, and it is specified in annex A. These tags help locate M2M Area Network elements modeled as ETSI M2M resources.

The rules the IPU follows to create the ETSI M2M resource structure are the following:

- The IPU is modeled with an ETSI M2M <application> resource. The "searchString" attribute of this resource contains an ETSI.ObjectType/ETSI.IP tag which identifies it as an IPU. The URI used to access this <application> resource has the following format:

    <sclBase>/applications/< interworking_proxy_application>

    The <application> resource contains an ETSI M2M <container> sub resource. The "searchString" attribute of this sub resource contains a tag of category ETSI.ObjectSemantic which indicates the semantic conventions used in the representation of this object. The URI used to access this <container> resource has the following format:

    <sclBase>/applications/< interworking_proxy_application>/containers/descriptor

    The <container> resource contains one or more <contentInstance> sub resource. The "content" attribute of this sub resource contains the representation of the IPU. In particular, since a single IPU can give access to multiple M2M Area Networks, each of them modeled with an ETSI M2M resource (see next bullet for description), the "content" attribute of the <contentInstance> resource may contain the URIs of the ETSI M2M resources representing these M2M Area Networks. The URI used to access the <contentInstance> resource containing the current representation of the IPU has the following format:

    <sclBase>/applications/< interworking_proxy_application>/containers/descriptor/contentInstances/latest

    The reason is that a new <contentInstance> resource is created each time the IPU representation changes (e.g. a new M2M Area Network is created, or an old one is deleted). So, in case a new <contentInstance> resource is created and the old ones are kept in order to maintain an history, there can be more than one <contentInstance> resources. But, in any case, the <contentInstance> resource pointed by the "latest" attribute of the contentInstances resource contains always the current representation of the IPU.

- Each M2M Area Network controlled by an IPU is modeled with an ETSI M2M <application> resource. The "searchString" attribute of this resource contains an ETSI.ObiectType/ETSI.AN_NWK tag which identifies it as an M2M Area Network. The URI used to access this <application> resource has the following format:

    <sclBase>/applications/<networkX>

    The <application> resource contains an ETSI M2M <container> sub resource. The "searchString" attribute of this sub resource contains a tag of category ETSI.ObjectSemantic which indicates the semantic conventions used in the representation of this object. The URI used to access this <container> resource has the following format:

    <sclBase>/applications/<networkX>/containers/descriptor