Technical Sciences
Brassersplein 2
2612 CT Delft
P.O. Box 5050
2600 GB Delft
The Netherlands

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO report

35575 | Final report

Report ETSI M2M-14bis JTC March 2011 meeting

Date	25 November 2011
Author(s)	Iko Keesmaat
Copy no	
No. of copies	
Number of pages	24 (incl. appendices)
Number of appendices	
Sponsor	VP P702 Toekomstig internetgebruik KAV
Project name	Standaardisatie 2011
Project number	055.01112

Summary

The ETSI Technical Committee (TC) M2M focuses on the development of a generic M2M architecture and underlying protocols suitable for a wide range of M2M environments. Whereas in the past effort has been put in the development of several use cases, the focus of this M2M 14bis meeting – held in Sophia Antipolis from March 28 until April 1 – was on completion of the *functional architecture*.

Major topics related to the functional architecture were *security* and *remote entity management (REM)*. Before and during the meeting the security discussion focused mainly on two opposing proposals for bootstrapping. The discussion on remote entity management focused for a large part on the best way to structure the management object so that it can be used to map existing remote management techniques from the BroadBand Forum (i.e. TR-069) and OMA-DM onto the functional architecture.

There were also a number of discussions on minor topics related to the functional architecture. Notably one about location and privacy and another on the best way to address applications.

In addition to the work on the functional architecture before and during the meeting effort was put into the stage 3 work on interfaces, into a threats analysis document and into a document on reuse of core network functionality. Some minor changes and updates were made to the M2M Requirements document, the M2M Definitions document and on a document on Use cases for e-Health.

Apart from the work on the TSs and TRs during the meeting the following other topics were discussed:

- a split of the TC into separate working groups;
- a new work item on Zigbee as an access network technology;
- the creation of a M2M Partnership project similar to the well-known 3GPP;

The meeting was held at the same location as an ISO meeting on Sensor Networks. During the meeting a joint meeting was held in order to discuss possible cooperation.

Finally reports were presented about several cooperations and liaisons with other groups. Most notably of these was the attendance by members of the ETSI M2M group of a workshop from the ETSI ITS (Intelligent Transport Systems) group.

Contents

1 Introduction

Machine-to-Machine (M2M) is about communication among machines without (or only limited) human intervention. Typical fields of M2M are:

- Buildings: Home automation, Office automation;
- Production: Production line management, Quality control;
- Healthcare: E-Health, Assisted Living;
- Security: Electronic monitoring, Military applications;
- Energy: Smart meters, Smart grids, Green energy;
- Retail: Goods tracking, Supply chain automation;
- Transport: Intelligent transport systems, E-Vehicles, Goods tracking.

Typically the network architecture for M2M consists of M2M devices that connect via a communication network to M2M servers. For instance,

- smart meters communicating with a smart meter application at the smart meter company;
- navigation devices in cars communicating with the server of the navigation company;
- printers communicating with the server of the printer manufacturing company, etc.

Direct communication between M2M devices without any intermediate role for a M2M server is less common but not explicitly excluded.

Initially M2M occurred mostly in so-called vertical stove-pipes. For a given application area the M2M devices, the M2M network, and the M2M application were all created by a single M2M company. Gradually a trend is visible where the vertical stove-pipes are migrating toward a more horizontal approach, where M2M devices communicate via a generic transport network and a common application infrastructure of a generic M2M service provider to a particular M2M application owned by a particular M2M company.

1.1 The ETSI Technical Committee M2M

Within ETSI the M2M Technical Committee (TC) has the responsibility:

- 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 fulfill 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 center of expertise in the area of M2M;
- to co-ordinate ETSI's M2M activity with that of other standardization groups and fora.

Within the TC a high level M2M architecture has been developed consisting of:

- M2M Application Domain;
- M2M Network Domain, and
- M2M Device Domain,

in which the following entities are distinguished:

- M2M Server;

- M2M Gateway;
- M2M Device.

A further distinction is between:

- Application (outside the M2M core network, inside/outside a M2M gateway or inside a M2M device), and
- Service Capabilities (inside the M2M core network, inside a M2M gateway or inside a M2M device)

In Figure 1.1 an overall diagram including the above items is depicted.

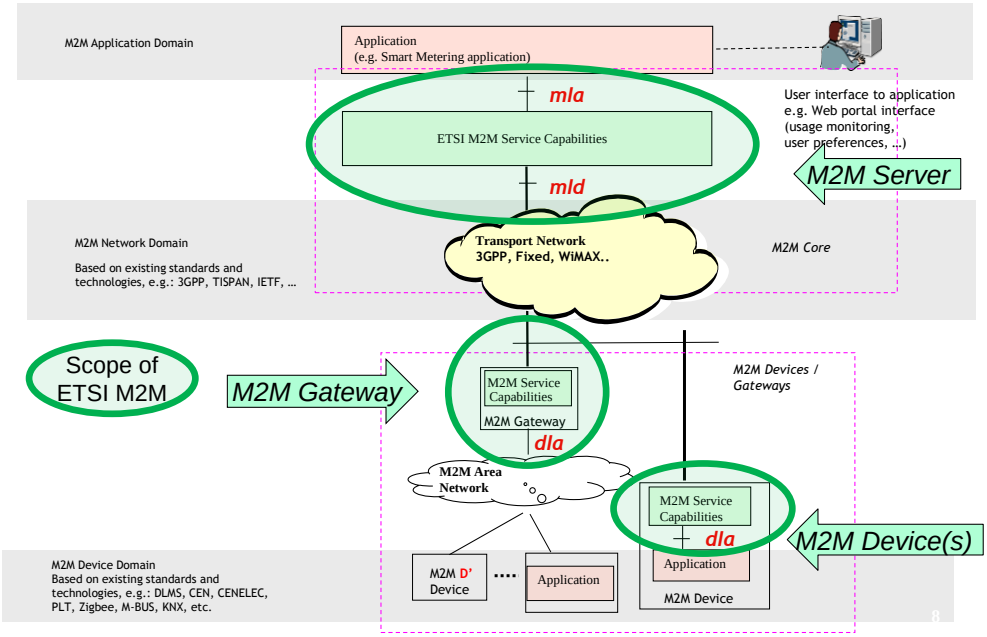

Figure 1.1: M2M high level system overview

On a more detailed level the M2M architecture makes use of three types of interfaces:

- mIa: this is the interface between an application in the M2M Application Domain (next to the M2M Core) and the M2M Service Capabilities inside the M2M Core;
- dIa: this is the interface between an application inside or next to a M2M Gateway and/or M2M Device and the M2M Service Capabilities inside the M2M Gateway or the M2M Device;
- mId: this is the interface between the M2M Service Capabilities inside the M2M Core and the M2M Service Capabilities inside the M2M Gateway or the M2M Device.

Note that in the ETSI M2M architecture a M2M Device can be *directly* connected to the M2M Server in the M2M Core via a (generic) Transport Network, but it can also be connected *indirectly* via a so-called M2M Area Network to a M2M Gateway which is then connected via a (generic) Transport Network to the M2M Server in the M2M Core. In the first case the M2M Device is required to support device-level M2M Service Capabilities and a device-level M2M Application. In the second case the M2M Device only consists of a M2M Application and it makes use of the M2M

Service Capabilities of the M2M Gateway. In this case the M2M Gateway also may make use of a gateway-level M2M Application.

By using the M2M Service Capability 'Interworking Proxy' (network-level = NIP, gateway-level = GIP, device-level = DIP), M2M Core Networks, M2M Gateways and even M2M Devices can support legacy M2M device that do not (yet) conform to the ETSI M2M architecture. In Figure 1.2 this is depicted graphically.

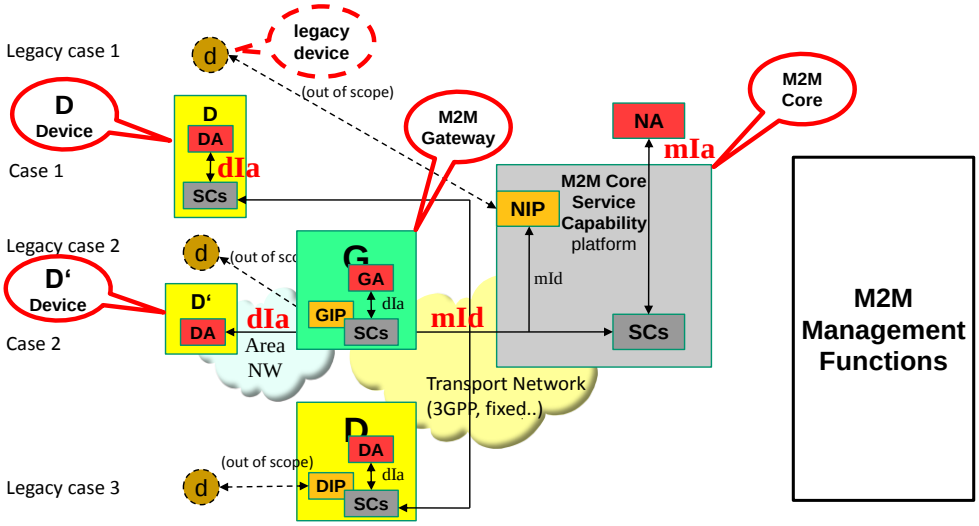

Figure 1.2: Reference M2M architecture

Note the distinction between M2M Devices of type D' (Case 2) that only contain a M2M Application DA and are connected via M2M Gateway G, and M2M Devices of type D (Case 1) that contain both a M2M Application DA and Service Capabilities (SCs). The M2M Gateway may make use of its M2M Application GA and contains M2M Service Capabilities (SCs), and the M2M Core contains M2M Service Capabilities that can interact with network level M2M Application NA.

For Release 1 of the ETSI M2M architecture the legacy cases (Legacy case 1, Legacy case 2, and Legacy case 3 in the diagram) are out-of-scope. Note that the legacy cases are those in which a M2M Device does not have an ETSI M2M Application capable of interacting with ETSI M2M Service Capabilities.

1.2 ETSI M2M work items and (draft) documents

The ETSI M2M Technical Committee has created the following work items (WI) with their associated (draft) documents:

Table 1.1 ETSI TC M2M work items and (draft) documents

WI	Title	Document ID	Version	Remark
00001	Requirements	TS 102 689	V1.1.1	Published
00002	Functional Architecture	TS 102 690	V0.10.4	
00003	Use Cases Smart Metering	TR 102 691	V1.1.1	Published
00004	M2M Definitions	TR 102 725	V0.3.0	
00005	Use Cases eHealth	TR 102 732	V0.3.1	
00006	Use Cases Connected Consumer	TR 102 857	V0.3.0	

00007	Use Cases City Automation	TR 102 897	V0.1.1	
00008	Use Cases Automotive	TR 102 898	V0.4.0	
00009	EU mandate on smart meters M441			Withdrawn
00010	mIa, dIa, mId interfaces	TS 102 921	V0.2.1	
00011	Impact of Smart Grids on M2M	TR 102 935		
00012	Threat Analysis and Counter Measures	TR 103 167	V0.2.1	
00013	Reuse of Core Network Functionality	TR 101 531	V0.1.3	

1.3 References

[M2M(10)0239] *Improvements in Sections 6.1 and 6.2*, source Alcatel-Lucent

[M2M(11)0010r3] *TR 103 167 Text Introducing Stakeholders*, source Qualcomm

[M2M(11)0042] *API Gap Analysis*, source: Vodafone

[M2M(11)0083r1] *Functionalities list & prioritisation*, source France Telecom, Vodafone

[M2M(11)0089r2] *Background material for conf-call ETSI M2M with OMA*, source NEC

[M2M(11)0095] *Privacy mechanism consideration*, source Huawei

[M2M(11)0096] *Privacy and Location*, source Alcatel-Lucent

[M2M(11)0103r1] *Presentation to BBF BoF 7. March in Boston*, source NEC

[M2M(11)0108r1 *TR103 167: two new threats re AN credentials*, source InterDigital]

[M2M(11)0112r3] *TR103 167: updates to threats 3 through 19*, source InterDigital

[M2M(11)0113] *SCL Discovery in 3GPP cellular case*, source Alcatel-Lucent

[M2M(11)0120] *Report on M441 Smart Metering Mandate*, source France Telecom

[M2M(11)0121] *Status of EV Charging mandate M468 and eMobility Focus Group*, source France Telecom

[M2M(11)0122] *Report of TC ITS Workshop 9th-11st February 2011*, source France Telecom

[M2M(11)0123] *Report of IOT Expert group*, source France Telecom

[M2M(11)0124] *Liaison Letter to ITU-T JCA-IOT*, source France Telecom

[M2M(11)0128r1] *Application management modifications*, source Ericsson

[M2M(11)0136r3] *introducing long-polling HTTP*, source Ericsson

[M2M(11)0137] *introducing the m2mPoc in the resources and the procedures*, source Ericsson

[M2M(11)0140r1] *Addition of Interference Management Functionality in TS 102 690*, source Fujitsu

[M2M(11)0143] *Gap Analysis showing mapping to use cases*, source Fujitsu

[M2M(11)0146] *Discussion on ETSI M2M business - information/data model of Devices aspects*, source NEC

[M2M(11)0149] *M2M PoC for Application addressing and routing*, source Ericsson

[M2M(11)0150] *Informative Annex*, source Ericsson

[M2M(11)0165r1] *TR102 690 clarification of key storage and Secured Environment in xSEC r1*, source InterDigital, LG, Gemalto

[M2M(11)0166r1] *Privacy and location consideration*, source Huawei

[M2M(11)0168] *Leveraging existing management data model*, source Huawei, InterDigital

[M2M(11))0169r1] *General principal of leveraging existing data model for REM*, source Huawei, InterDigital

[M2M(11)0170r2] *Procedures_for_Management*, source Huawei, InterDigital

[M2M(11)0171r2] *RESTful method extension*, source Huawei, InterDigital

[M2M(11)0172r1] *REM Work Summary*, source Huawei

[M2M(11)0174] *Protection Profile for the Gateway of a Smart Metering System*, source Cinterion Wireless Modules

[M2M(11)0175r3] *Common Framework for Automatic Service Bootstrapping Procedure*, source Samsung, Toshiba

[M2M(11)0177] *Functionalities Gap Analysis: Status Overview*, source France Telecom, Vodafone

[M2M(11)0178r1] *r1 of WI0012: summary report of rapporteur's GoToMeetings since M2M#14*, source Rapporteur

[M2M(11)0180] *High Level APIs for Device Management*, source Alcatel-Lucent

[M2M(11)0184] *TR 103 167 Motivating Factors Methodology*, source Qualcomm

[M2M(11)0187] *TR 103 167 Combined Stakeholders and Motivating Factors Text*, source Qualcomm

[M2M(11)0190] *Management Layers and MgmtObjs Structure for ETSI M2M xREM*, source InterDigital

[M2M(11)0191r1] *TR 103 167 Motivating Factors Worked Example*, source Qualcomm

[M2M(11)0192r1] *Support Multiple Management Protocols for ETSI M2M xREM*, source InterDigital

[M2M(11)0196] *introducing the m2mPoc in the procedures*, source Ericsson

[M2M(11)0203] *Location support in functional architecture*, source Alcatel-Lucent

[M2M(11)0204] *Privacy support in functional architecture*, source Alcatel-Lucent

[M2M(11)0215] *SCL Configuration Management Requirements Analysis*, source Huawei

[M2M(11)0217] *ETSI M2M Management Functions*, source Huawei, NEC

[M2M(11)0219] *Status of security rapporteurs sessions since M2M 14*, source Rapporteur

[M2M(11)0221] *Rapporteur contribution, status of Stage 2 architecture document*, source Rapporteur

[M2M(11)0224] *Status M2M Stage 3 TS 102 691*, source Telecom Italia

[M2M(11)0233] *LS from OMA DM WG on joint F2F meeting*, source OMA

[M2M(11)0234] *Liaison statement out to ISO/IEC JTC1*, source Orange Labs, ETRI

[M2M(11)0235r2] *Report of Security Adhoc Sessions during M2M 14 bis*, source Rapporteur

[M2M(11)0236] *r1 WI0012: report of rapporteur sessions at M2M#14bis*, source Rapporteur

[M2M(11)0238r1] *LS out to OMA-DM regarding joint meeting in San Diego (M2M#15)*, source Huawei

[M2M(11)0239r2] *Management Layers and MgmtObjs Structure for ETSI M2M xREM*, source InterDigital

[M2M(11)0240r1] *Structure of resource <mgmtObj> for ETSI M2M xREM (Revised from 0190 - 2nd Part)*, source InterDigital

[M2M(11)0242] *WI0012 threat analysis: recommended and prioritised countermeasures*, source Rapporteur

[M2M(11)0243r3] *Introducing location resource*, source Huawei, Telecom Italia, Ericsson

[M2M(11)0245] *M2M Well-Known SCL Discovery Procedures*, source InterDigital

[M2M(11)0246] *M2M Well Known SCL Discovery Message Flows*, source InterDigital

[M2M(11)0247r3] *Report of Management Adhoc Sessions during M2M 14 bis*, source Rapporteur

[M2M(11)0248] *Presentation to joint with JTC1 WG11 at M2M 14bis*, source Telecom Italia

[M2M(11)0251r2] *M2M#14bis meeting report*, source: ETSI

[M2M(11)0257] *TR103 167 v0.3.1*, source Rapporteur

2 ETSI M2M-14bis

The ETSI report of this meeting can be found in [M2M(11)0251r2].

2.1 Results from ad-hoc conference calls

In the period between the previous official ETSI meeting (#14) and this meeting a number of ad-hoc conference calls have occurred on a number of topics:

- Gap analysis & mapping of use cases on gap analysis;
- Architecture (stage 2);
- Remote Management (stage 2);
- Security (stage 2);
- Protocols (stage 3).

In the following sections a short summary is given about the status and results of these ad-hoc meetings.

2.1.1 Gap analysis & mapping of use cases on gap analysis

A status report on the conference calls held about functionalities gap analysis between #14 and this meeting was presented [M2M(11)0177]. The information provided in the M2M Requirements document (TS 102 689) and contribution [M2M(11)0042] has been used to create a draft document which was subsequently used as the basis for the conference calls and resulted in a output document of the conference calls [M2M(11)0083r1], see below. In the conference calls also documents [M2M(11)0096], [M2M(11)0095], and [M2M(11)0113] on Privacy, Privacy & Location, and Bootstrapping, respectively, were discussed.

The output document [M2M(11)0083r1] of the conference calls contains a list of requirements on functionalities and a prioritization. The goal is to determine if in Release 1 the necessary functionalities for deployment and implementation of the M2M architecture are covered. The functionalities have been divided in:

- resource related;
- value added services;
- security related; and
- management related.

During the presentation of the work done in the conference calls before the meeting also contribution [M2M(11)0143] was discussed. It attempts to map the requirements/functionalities listed in [M2M(11)0083r1] onto the M2M use cases defined within ETSI M2M. The use cases that were used for the mapping are:

- eHealth, and within this use case:
  - Remote Patient Monitoring (RPM)
  - Patient-Provider secure Messaging
  - Measurement of Very Low voltage Body Signals (MVLBS)
  - Telecare over IP-WAN use case' of Continua Health Alliance
- Connected Consumer, and within this use case:
  - Photo uploading from still camera
  - Content download to eBook reader device
  - Remote Control of Home Appliance
  - Surveillance data uploading
  - Inventory Management

- City Automation, and within this use case:
  - Traffic Flow Management System in combination with Dynamic Traffic Light Control
  - Street Light Control
  - Passenger Information System for Public Transport
- Automotive Use Cases, and within this use case:
  - Electric Vehicle Charging
  - Fleet Management / Theft Tracking
  - Vehicle-to-Infrastructure communications

2.1.2 Architecture (Stage 2)

A status update was presented in [M2M(11)0221] on the work done in conference calls before the meeting on the Functional architecture (TS 102 690).

The following topics were discussed during the conference calls:
- Functionality: location, privacy;
- Architecture: template for procedure flows, agreement on handling of addressing.

A decision was made to split the functional architecture in a Release 1 part (all stable sections) and Release 2 (= Release 1 plus non-stable sections).

A number of issues on security were collected and handed over to the security group within ETSI M2M.

2.1.3 Remote Management (Stage 2)

A status report on the work done on Remote Entity Management (REM) between the previous meeting and this meeting in a number of conference calls was presented [M2M(11)0172r1].

The work on REM concerns itself about the way Devices and/or Gateways can be remotely managed from the core network. To this aim it seeks to reuse existing remote management techniques from the BroadBand Forum (BBF) with its TR-069 approach, and from OMA Device Management (OMA-DM).

In the conference calls between meeting #14 and this meeting #14bis the following has happened:
- meeting with BBF and OMA;
- discussion about REM API Gap Analysis;
- discussion about REM Functionality Gap Analysis;
- discussion about the Data Model for Service Capability Layer (SCL) Managed Objects (MO);
- discussion about the general principle for adopting the existing OMA-DM/TR-069 within ETSI M2M

The conclusion after the conference calls is that the following work is to be done (at #14bis meeting or later):
- Complete the REM API requirements analysis;
- Decide on the general principle of implementing REM functionality with existing OMA-DM/TR-069
- Make a number of improvements in the ETSI M2M Functional Architecture;
- Work on stage 3 aspects of REM.

From the above the discussion on the general principle of implementing REM functionality was considered the most important.

2.1.4 Security (Stage 2)

A status report on the work done on Security (Stage 2) between the previous meeting and this meeting in a number of conference calls was presented [M2M(11)0219].

The main topics of the conference calls were:

- bootstrapping/provisioning negotiation mechanism;
- authentication protocols and algorithms;
- privacy/confidentiality.

On the bootstrapping/provisioning negotiation mechanism two more or less opposing proposals have been discussed:

- a Samsung/Toshiba proposal based on EAP and PANA for automated bootstrapping selection;
- a Qualcomm proposal based on using TLS negotiation to select between automatic certificate-based bootstrapping and access network based GBA-based bootstrapping.

The decision between these two proposals was postponed to the current meeting (#14 bis).

On the authentication protocols and algorithms there was a proposal by Qualcomm for a flexible SCL (Service Capabilities Layer) authorization framework but this met with some discussion related to the assumptions on trust relationships and scope. It was decided that a discussion between security and architecture experts was needed during the #14 bis meeting in order to decide on a way forward.

On the topic of privacy and confidentiality no contributions were received, but instead a number of questions were discussed:

- Shall solutions like TLS over TCP over the mIa interface be standardized within the ETSI M2M architecture?
- Is there a general agreement that secure messaging over the dIa interface is necessary?
- Are PSK/TLS sessions between SCLs suitable, given the mId framework?

It was the intention to finalize the issues described above and then go on to stage 3 work. The stage 3 work should as much as possible be based on existing IETF protocols.

2.1.5 Protocols (Stage 3)

A status report on the work done on Protocols (Stage 3) between the previous meeting and this meeting in a number of conference calls was presented [M2M(11)0224].

In the conference calls the following four topics were discussed:

- Container Management SCL Primitive Description;
- Resource Discovery SCL Primitive Description ;
- Application Management SCL Primitive Description ;

- announce/deannounce Primitives.

The first three topics had been incorporated into the input draft of TS 102 691 to this meeting.

2.2 Liaison relations with non-ETSI groups

In the meeting the M2M related activities in non-ETSI groups were presented (in verbal and/or written form):

- **3GPP**
  [Verbal update:] The URI format for M2M and the terminal triggering interface are topics discussed in 3GPP SA2;
- **OMA**
  [Verbal update:] The URI format for M2M is studied in 3GPP;
- **BBF – Broadband Forum**
  [Verbal update:] A presentation from ETSI M2M to BBF was given (see [M2M(11)0103r1]). A presentation from Motorola on service extraction layer showed that there is much overlap with ETSI M2M work;
- **ISO JTC/WG7 – Sensor Networks**
  See Section 2.2.1;
- **TIA – Telecommunications Industry Association (USA)**
  [Verbal update:] During a joint workshop at a TIA TR40 meeting possible harmonization between ETSI and TIA was discussed. it was agreed that further alignment between the two groups shall be examined;
- **CCSA TC10 – China Communications Standards Association (China), – Ubiquitous Network**
  [Verbal update:] CCSA TC10 wish to invite ETSI M2M for discussion about harmonization;
- **HGI – Home Gateway Initiative**
  [Verbal update:] HGI invited ETSI M2M to present their work; initial analysis showed that HGI is working on a lower layer than ETSI;
- **ATIS – Alliance for Telecommunication Industry Solutions (USA)**
  [Verbal update:] Within ATIS a M2M Focus group has been created which covers the horizontal approach; in addition two vertical groups (Connected Vehicle and Smart Grids) exist; the main focus is on markets, use cases and business cases;
- **TTA – Telecommunications Technology Association (South Korea)**
  [Verbal update:] A special M2M group has been created: PG708;
- **ITU-T JCA-IoT – Joint Coordination Activity – Internet of Things**
  [M2M(11)0124] A report was presented about the first JCA-IoT; a draft liaison was presented stating the liaison officer from ETSI M2M to this group. The JCA-IoT is the continuation/renaming of the JCA-NID (Network Aspects of Identification Systems including RFID);
- **OMA DM – Device Management**
  [M2M(11)0089r2], [M2M(11)0233], [M2M(11)0238r1] On 22nd February 2011 a conference call took place with ETSI M2M and OMA DM attendance discussing the possible relationships between OMA DM and Remote Entity Management within ETSI M2M; OMA DM invited ETSI M2M to a face-to-face joint session in San Diego (24th May 2011) and ETSI M2M accepted this invitation.

2.2.1 Joint session with ISO/IEC JTC1 WG7

During the meeting there was a special joint session with ISO/IEC JTC1 WG7 which is the ISO/IEC working group on sensor networks. The chairman of ETSI M2M gave a presentation [M2M(11)0248] detailing a lot of the work of ETSI M2M (such as the functional architecture, etc.). Next the chairman of ISO/IEC JTC1 WG7 gave a short presentation. This presentation was very disappointing as it only stated some procedural fact (such as number of members, number of documents, process of getting documents, structure of ISO/IEC). The intention was next to have a discussion with both groups about relations, similarities, cooperation, etc. Due to the fact that the ISO/IEC group did not reveal any content about there work this discussion was not very fruitful. Eventually it was decided that ETSI M2M shall formally start a liaison with the ISO/IEC group as this is the only way that the documents from the ISO/IEC group can be obtained by ETSI [M2M(11)0234]

2.3 ETSI groups

In the meeting the M2M related activities in other ETSI groups were presented (in verbal and/or written form):

- **ETSI OCG – Operational Co-ordination Group**
  [Verbal update:] There is a proposal to create an OCG subgroup to deal with coordination of EC mandates;
- **ETSI Board**
  [Verbal update:] A MoU has been signed with T&D Europe (European Association of the Electricity Transmission and Distribution Equipment and Services Industry) on Smart Grids standards cooperation. EC mandate M490 (Smart Grids) has been accepted. The ITS (Intelligent Transport Systems) Partnership Project is delayed due to resistance of some parties;
- **ETSI eHealth**
  [Verbal update:] The ETSI EP eHealth plans to have a workshop in October 2011 close to the workshop of M2M. ETSI M2M suggested having a session dedicated to Health at the M2M workshop. The EP (ETSI Project) eHealth seems to be coming to a close in 2011;
- **ETSI ITS – Intelligent Transport Systems**
  [M2M(11)0122] An ITS workshop in February 2011 was attended by several ETSI M2M members. In the meeting the main points from the workshop were reported. The ETSI ITS architecture is a convergence of three other ITS architecture (ISO SC204 WG16 CALM, Car-2-Car, and IEEE). It proposes to use IEEE 802.11p for car-to-car and for car-to-roadside communication. In ETSI ITS three types of services are included: cooperative road-safety, cooperative traffic-management, and global internet service. It was observed by the ETSI M2M attendants that the ITS architecture is similar to the ETSI M2M architecture. Personally I tend to disagree. It was further observed that the choice of IEEE 802.11p for car-to-roadside communication seemed not very suitable. IEEE 802.11p is a short-range communication technique most suitable for car-to-car communication. It was finally observed that the ITS group did not contain many Telco people and this resulted in the group redoing stuff already developed in 2G/3G networks (such as the TDD technique for preventing collision).

2.4 EC mandates

The EC regularly issues so-called mandates. In a mandate European standardization organizations (such as ETSI, CEN, CENELEC) are invited to take up responsibility for certain standardization activities. Some of the mandates relate to ETSI M2M.

2.4.1 M/441 Smart Meters

[M2M(11)0120] Presentation by Marylin Arndt about the status of the Smart Meter M441 mandate work.

The mandate M441 Smart Meters has focused its work on two topics:

- Technical Document;
- Use Cases.

The Technical Document (version 0.4.3) is currently under final review. It contains the functional architecture of the Smart Meter environment. The work on Use Cases is supposed to produce a first draft at the end of 2011. The work on this mandate requires a lot of coordination as both ETSI, CEN and CENELEC technical committees are supposed to work on it.

At the end of 2010 the Smart Meter Coordination Group (SM-CG) issued its final report on the analysis of the mandate. In this report (among other things) it formulated a particular Additional Functionality

- F5: "*Communicating with (and where appropriate directly controlling) individual devices within the home/building*".

The EC did not like this functionality which it viewed as an undesirable bundling of metering and control, as it feared that it would have undesirable implications for market access, device costs, and conformance testing. As a result of this comment the SM-CG reformulated the functionality into

- (new) F5: "*To provide secure communication enabling the smart meter to export metrological data for display and potential analysis to the end consumer or a third party designated by the end consumer*".

In addition it added the following functionality

- "*to enable communication of AMI (Advanced Metering Infrastructure) components with devices or gateways within the home / building used in the provision of energy efficiency and demand-side management services*"

so that some part of the original functionality remained, but it stated that this functionality is not part of the current mandate. It may be part of the mandate on smart grids (M490).

For ETSI M2M the M441 work had the following tentative impact:

- a mapping should be made between the M441 architecture and the M2M architecture; it was proposed to start a new Work Item for this; during the meeting, however, this Work Item was not created;
- it was proposed to harmonize the Use Case template used in the Use Case Work items within ETSI M2M.

2.4.2 M/468 Charging of Electronic Vehicles

[M2M(11)0121] Presentation by Marylin Arndt on the status of the Electronic Vehicle Charging M468 mandate, renamed European Electro Mobility.

Part of the work on this mandate (which has a strong focus on CEN/CENELEC, but also includes ETSI M2M and ETIS ITS) is about data communication between an Electronic Vehicle (EV) and an EV Charger. The communication between the charger and the utility network is considered in scope of the Smart Grids M490 mandate. Communication inside the EV is also considered out of scope.

The role of ETSI in this mandate is not so clear. ETSI ITS appears to be the coordinator for the mandate from ETSI side, but there is no centralized mailing list or document repository. The role of ETSI M2M in this not so clear. It appears that all functionalities for EV Charger communication are already supported in ETSI M2M Rel-1.

2.4.3 Upcoming mandate/ IoT Expert Group

[M2M(11)0123] Presentation by Marylin Arndt on the activities of the IoT (Internet of Things) Expert Group.

The Internet of Things (IoT) Expert Group has been formed by the EC in order to discuss about the required policies needed to support a humane yet commercial Internet of Things. One of the outcomes of this group can be a mandate to standardization bodies (expected 2H2011).

The group has met a couple of times (and will continue to do so for more meeting in 2011). Topics discussed in the group are:

- Privacy and (Personal) Data Protection;
- Trust and Acceptability;
- Security;
- Identification/Addressing/Authenticaiton;
- Governance of IoT (how is identification done; who is assigning identifications, how is security ensured, which stakeholders are accountable, etc);
- Standardization;
- Interoperability.

The group is discussing a so-called Martyr Paper containing the impact assessment of the costs/benefits of government intervention.

2.5 Incoming and outgoing liaisons

2.5.1 Incoming liasions

There were two liaisons from OMA. The first was a confirmation to have a joint session between OMA-DM and ETSI M2M. The second was in informational liaison informing ETSI M2M about the OMA RESTful API for Telco Operator Exposure.

There was one liaison from ETSI TC ATTM (Access, Terminals & Transmission, Multiplexing) about the willingness of this group to work together with ETSI M2M on the EC Smart Metering mandate.

2.5.2 Outgoing liaisons

There was one liaison to OMA-DM stating the wish for a joint meeting in May 2011 and a number of conference calls before this joint meeting.

There was one liaison which is the response to the received liaison from ETSI TC ATTM.

There was one liaison to ITU-T JCA IoT proposing Marylin Arndt as liaison officer to this group.

2.6 Work on draft documents (TS and TR) from ETSI M2M

During the meeting the following TS and TR documents have been handled:

- *M2M service requirements*, ETSI TS 102 689 (WI-00001);
- *M2M functional architecture*, ETSI TS 102 690 (WI-00002);
- *mIa, dIa, mId interfaces*, ETSI TS 102 921 (WI-00010);
- *M2M definitions*, ETSI TR 102 725 (WI-00004);
- *Use cases of M2M applications for eHealth*, ETSI TR 102 732 (WI-00005);
- *Threat analysis and counter-measures to M2M service layer*, ETSI TR 103 167 (WI-00012);
- *Reuse of core network functionality by M2M service capabilities*, ETSI TR 101 531 (WI-00013).

There were no contributions on the other TS and TR documents.

2.6.1 M2M service requirements

Work Item WI-00001, ETSI TS 102 689

This document has already been approved in the past. During this meeting there were two (minor) Change Requests (CRs):

- Security Terminology;
- addition of Interference Management Service Requirement.

These two CRs were the first CRs to be approved in the ETSI M2M group.

2.6.2 M2M functional architecture

Work Item WI-00002, ETSI TS 102 690

The following areas were discussed during the meeting:

- Security;
- GAP analysis;
- Architecture, resources, and procedures;
- Management aspects.

The majority of contributions were classified under Architecture, resources, and procedures.

Security

During the week the security group within ETSI M2M had a number of ad-hoc sessions (see [M2M(11)0235r2] for a report on this). All of these ad-hoc session discussed the two proposals for bootstrapping that were already discussed before the meeting. At Thursday there was still no solution: Qualcomm was in favor of one proposal and many other companies were in favor of another one. Only on Friday a compromise was reached (see [M2M(11)0175r3]).

A document [M2M(11)0165r1] clarifying key storage and Secured Environment in xSEC was discussed by email. It was proposed to handle this in the upcoming conference calls before the next meeting.

GAP analysis

Under this topic only one document [M2M(11)0140r1] was discussed. It was agreed to be included in the draft.

Architecture, resources, and procedures
After a number of editorial contributions a considerabsle number of contributions were accepted that were introducing message flows (for Announce/Deannounce, Access Rights Management, Container Management, Access Status, Application Management, Collection Management, SCL Management, Subscription Management, Group Operation Management, and Resource Discovery Procedure). Also a number of contributions introducing (minor) modifications were accepted (Access Rights Management, Group Management, SCL Management).

A contribution introducing HTTP like Long Polling was accepted (see [M2M(11)0136r3]). Long polling is a technique to enable servers to push information to clients by letting the client to repeatedly issue a poll request which is then kept unanswered by the server until it has something to push.

Considerable discussion arose around
- SCL Discovery procedure (see [M2M(11)0245], [M2M(11)0246]); discussion focused on security issues;
- Application Management modification (see [M2M(11)0128r1], [M2M(11)0137], [M2M(11)0149], [M2M(11)0196]); discussion was about the way applications shall be addressed.

The above discussions were to be continued after this meeting in subsequent conference calls.

Two contributions on privacy and location from Huawei were accepted (see [M2M(11)0166r1], [M2M(11)0243r3]), but two other contributions on location and privacy from ALU were not accepted (see [M2M(11)0203], [M2M(11)0204]). The contributions by ALU were discussed extensively, but no conclusions could be drawn.

A generic information model for M2M naming, numbering, and addressing from Ericsson was accepted as part of the TR (see [M2M(11)0150]).

Management aspects
During this meeting in a number of ad-hoc sessions a set of contributions on Remote Entity Management (REM) was treated (see [M2M(11)0247r3] for a report of these ad-hoc sessions) on the following topics:
- REM API analysis;
- Generic principle for REM discussion;
- Architecture improvements.

The documents on *REM API analysis* [M2M(11)0217], [M2M(11)0215] contained an initial list of REM functions and APIs to be supported by an ETSI M2M SCL. These documents were noted and contributions on this topic were invited for future incorporation in the TS.

The documents on the *generic principle for REM* consisted of two groups:
- a group ([M2M(11)0146], [M2M(11)0168], [M2M(11))0169r1]) supported by NEC, Huawei, and InterDigital proposing to incorporate into the ETSI M2M data

model existing data models for remote management as already defined by e.g. OMA-DM and BBF in its TR-069;
- a group ([M2M(11)0180]) supported by ALU proposing to define a high level interface to the ETSI M2M data model used for remote management.

During the meeting a compromise was reached consisting of a data structure containing a “Basic” part and an “Advanced” part. The basic part resembled the ALU approach and provides only a number of basis elements of devices (such as battery level, memory available, etc.). The advanced part contains one or more mappings from the existing remote management data models (OMA-DM/TR-069) and caters for the ideas expressed by Huawei, InterDIgital and NEC. The compromise was included in a revised version of a document included in the ‘architecture improvements’ group of contributions (see [M2M(11)0240r1] below).

The group of documents on *architecture improvements* contained
- a contribution [M2M(11)0170r2] on using the standard RESTful commands (CREATE, RETRIEVE, UPDATE, DELETE) in relation with the resource <mgmtObj>,
- a contribution [M2M(11)0171r2] on introducing the commands EXECUTE, SUBSCRIBE, and NOTIFY to the standard RESTful commands in order to be able handle the mapping on existing commands of e.g. OMA-DM and TR-069;
- a contribution [M2M(11)0192r1] on a mechanism to negotiate the management protocol used for remote element management (e.g. in order to choose between OMA-DM and TR-0690).

In addition this group of documents contained a contribution [M2M(11)0190] proposing a separation of the various management layers (application, service, network, device management) and proposing a restructuring of the <mgmtObjs> (containing multiple <mgmtObj>s) and <mgmtObj> resources. This contribution was split up in a first contribution [M2M(11)0239r2] proposing the separation of the various management layers and a restructuring of <mgmtOjbs> and a second contribution [M2M(11)0240r1] dealing with the structure of <mgmtObj>. This latter contribution was used to included the compromise on data models discussed under the topic ‘generic principle’ above.

2.6.3 mIa, dIa, mId interfaces

Work Item WI-00010, ETSI TS 102 921

For this technical specification 9 contributions were treated, about the following topics
- SCL Primitive Descriptions (for Container Management, Resource Discovery, and Application Management);
- Introduction of the announce and deannounce primitives;
- Introduction of aPoC (application point of contact) related attributes;
- Editorial changes of attributes;
- Extension of a PermissionFlag in order to support privacy;
- Introduction of a new data type PrimitiveType in order to indicate the type of primitive;
- Introduction of a new data type PrivacySupport (not Stage 3 but Stage 2!).

Apart from the contribution on the PermissionFlag, all contributions were accepted.

2.6.4 M2M definitions

Work Item WI-00004, ETSI TR 102 725

For the TR containing M2M definitions there was 1 contribution adding some missing definitions and updating some others. The contribution was noted and shall be developed in upcoming conference calls.

2.6.5 Use cases of M2M applications for eHealth

Work Item WI-00005, ETSI TR 102 732

The rapporteur reported on the status of this TR. There were no new contributions since [M2M(10)0239] (2010). The changes introduced by this contribution were incorporated. It was expected that for Release 2 there will be some new requirements.

2.6.6 Threat analysis and counter-measures to M2M service layer

Work Item WI-00012, ETSI TR 103 167

Between ETSI M2M #14 and this meeting a number of conference calls were held on this topic (see [M2M(11)0178r1]). During the meeting a number of ad-hoc meetings were held. The rapporteur reported the progress on this TR in [M2M(11)0236].

The TR is supposed to contain text on the following topics:

- methodology for analyzing threats and determining risk;
- analysis of threats and their risk level;
- countermeasures for the identified threats;
- recommendations to ETIS M2M for assurance of the countermeasures and potential requirements for standardization.

In the conference calls a number of documents on methodology by Qualcomm were discussed and revised (see [M2M(11)0010r3], [M2M(11)0184], [M2M(11)0187], [M2M(11)0191r1]), but postponed in order to give members the opportunity to see via a working example if the methodology is sound. At this meeting these documents were further postponed in order to obtain a complete draft TR at the end of the meeting.

In the conference calls a number of threats were updated and two new threats were added (see [M2M(11)0108r1], [M2M(11)0112r3]). These contributions were accepted.

During the meeting in the ad-hoc sessions a list of countermeasures with estimated risk level and mapping on requirements has been constructed (see [M2M(11)0242]). This list was accepted and will be included in the next draft of the TR [M2M(11)0257].

2.6.7 Reuse of core network functionality by M2M service capabilities

Work Item WI-00013, ETSI TR 101 531

For this TR 12 contributions from Ericsson on Specification of XDMS Application Usage for various aspects were presented. All of them were accepted without any discussion.

2.7 Other topics discussed during the meeting

In addition to the above also the following topics were discussed during the meeting:

- Proposal for security requirements on smart meters from the German government;
- Creation of separate sub working groups within ETSI TC M2M;
- New work items for ETSI TC M2M;
- Advise to ETSI General Assembly (GA) for the creation of a (worldwide) Partnership Project for M2M (analogous to 3GPP).

2.7.1 Protection Profile for the Gateway of a Smart Meter System

A proposal [M2M(11)0174] was presented created by the German Federal Agency for Security of Information Systems (BSI) about a Protection Profile for the Gateway of a Smart Meter System. In the proposal the security requirements and countermeasures for such a gateway was described. The German government intends to make the described security requirements mandatory for future smart meter deployments in Germany.

The proposal was presented in the ETSI M2M group because it has a relation with the earlier work on smart meters done in the group, but also because it can be used as additional information for the security work to be completed in the group.

Personal note: It is interesting to compare the architecture described in the proposal and in the documents produced by the group. A mapping has been indicated in the presentation, but the mapping is not entirely obvious to me.

2.7.2 Creation of new subworking groups

Due to the increase in work for the group a proposal was put forward to create several separate subworking groups:

- WG1: Requirements and use cases;
- WG2: Architecture and Network interworking;
- WG3: Protocols and interfaces;
- WG4: Security aspects;
- WG5: Management

The proposal was accepted and the working groups will be created in the next (plenary) meeting (of May 2011). The first steps of the working groups will be to create their terms-of-reference.

2.7.3 New work items

One new work item was proposed. The original scope of the work items was the mapping of the ZigBee Profile to the M2M architecture, but during the meeting this scope was expanded to:

- Interworking between the M2M Architecture and M2M Area Network technologies.

In this form the work item was accepted.

Personal note: It is interesting to see that on the one hand ETSI M2M tries to be very generic (“access agnostic”), but still endorses a work item in which a specific technology is considered in relation to the M2M architecture.

2.7.4 Recommendation to ETSI GA about the creation of an M2M Partnership Project

Within the meeting a proposal has been discussed to create an recommendation to the ETSI General Assembly (GA) to create a so-called Partnership Project for M2M.

This would be a similar construct as the existing 3GPP organization: it would have as member the various standards organization bodies such as ETSI, and it would operate world-wide. The ETSI M2M group is only capable of creating a recommendation to the General Assembly as it is the GA that will have to decide on the creation.

Personal note: a lot of discussion went on about the scope and wording of the recommendation. Participants were asked during the meeting and in the mailing list whether they (as organization) were supporting the creation of the construct. TNO has given support and later also KPN could give its support (via TNO).

2.8 Personal impression

Personal impression about the work of the group:
As a first time attendance to this group it was difficult to assess the value and content of the discussions going on. Most of the time of the plenary session was devoted to the functional architecture. This functional architecture appears to be very abstract and generic. It is difficult to match it with actual M2M implementations in networks such as KPN. It is even difficult to match it with developments ongoing in other standardization groups such as 3GPP. An example of this was the apparent mismatch/confusion about the terms M2M Server (from ETSI M2M) and MTC Server (from 3GPP): although they are apparently very similar, the group tends to disagree.

Interesting discussions during the meeting:
During the meeting a lot of discussion (often in a spontaneous ad-hoc meeting way) was devoted to the concept of an Application Identifier. Triggered by [M2M(11)0149] a number of people were actively discussing this topic. Ultimately the discussion was moved to subsequent conference calls after the meeting.

Another active discussion (triggered by [M2M(11)0166]) took place on the concept of Location and the relationship with Privacy. Some conclusions were reached.

In pre-arranged ad-hoc meetings on security (as part of the functional architecture) apparently a hot debate occurred between parties on the best way to realize bootstrapping. Ultimately a compromise was reached.

In pre-arranged ad-hoc meetings on Remote Element Management a discussion has occurred on the best way to create a Managed Object data model for incorporating/mapping existing data model from OMA-DM and BBF. A compromise was reached.

The working of the group:
It was clear that the ETIS M2M group was not yet established long ago. The way of working was somewhat informal and at time chaotic to my eyes. Not all people adhered to the customary practices of issuing contributions and revisions. The group seemed to consist of a relatively small group of enthusiastic people working for some time with each other on this topic.

A lot of the work appears to be ongoing in various ad-hoc conference call meetings. The work on Remote Element Management is somewhat chaotic. The work on

Security is more structured. The work on Stage 3, Reuse of CN functionality, and Threats & Countermeasures appear to be very well structured and efficient.

3 Impact in standardization and impact by standardization

The impact in standardization in this meeting was not high. The attendance of the meeting was primarily used to get acquainted with the work and with the group. It is the intention to start bringing contributions in one of the next meetings. The basic idea of these contributions will most likely be directed in getting the highly abstract work of the group in relation with more concrete practical application areas.

Due to the attendance of the meeting it was observed that there is a natural relation between the ETSI M2M group and the ETSI ITS (Intelligent Transport Systems) group. This has resulted in the author getting in contact with the KPN CIPO project LTR – Connected Car (project leader Paul Spaanderman, contact Igor Passchier). This can be seen as impact by standardization.