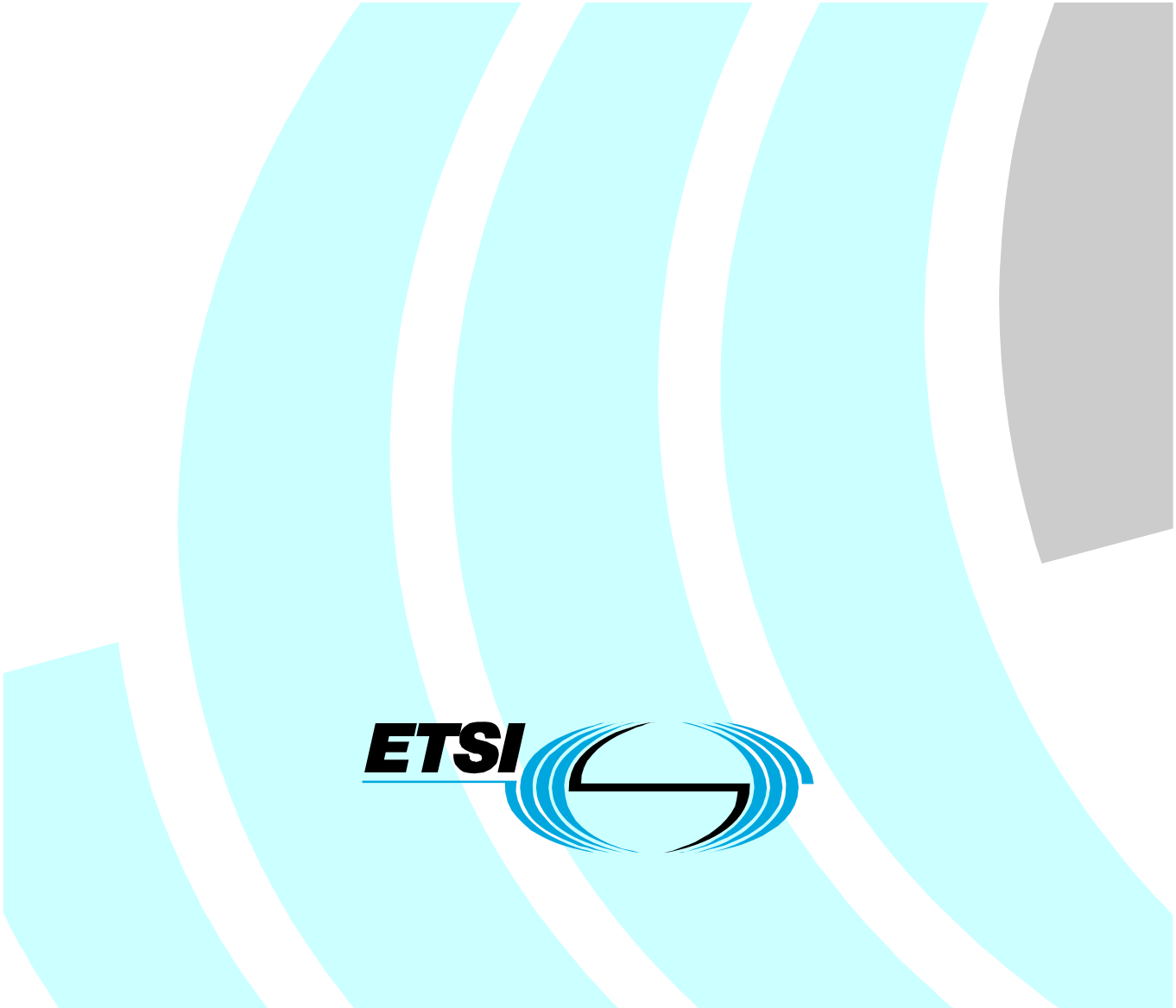
ETSI TR 103 167 V1.1.1 (2011-08)

Technical Report

Machine-to-Machine Communications (M2M); Threat analysis and counter-measures to M2M service layer



Reference
DTR/M2M-00012ed111

Keywords
M2M, security

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

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 may be referenced by other TRs and Technical Standards (TS) developed by ETSI TC M2M. The present document is a TR and therefore, the content is informative.

1 Scope

1.1 General

Below are reproduced some of the terms of reference concerning security handling in ETSI TC M2M [i.1].

- "*Requirements pertaining to detailed security analysis (such as the analysis of threats, risks and counter-measures) are within the scope of ETSI TC M2M.*
- *Wherever possible, detailed solution work based on other SDOs' existing mechanisms shall be performed by those SDOs, based on input which TC M2M may provide. Identified solution gaps which are not addressed by other SDOs can be handled in ETSI TC M2M.*
- *Security aspects which are part of the current architecture document shall remain with the current architecture document for the purpose of Release 1, because of the tight integration needed to provide a solid basis for Release 1. Note: this requirement is intended to avoid the creation of separate security architecture specifications for Release 1".*

1.2 Specific

Below are the terms of reference in the WI description [i.2].

In the present document, threats against M2M functional architecture, Service layer and interfaces are identified and analysed for impact and for likelihood. The need for countermeasures is determined.

The threat analysis considers only the following two types of threat (with the following order of priority):

1) Type 1 threats: threats that are specific to M2M service layer or interfaces for the service layer.
2) Type 2 threats: threats that may not be specific to M2M service layer but which have a significant impact upon M2M functional requirements.

The level of risk (i.e. combined likelihood and impact) of identified threats is also evaluated. As a result of that, there is a prioritisation of threats and therefore of countermeasures and security requirements.

Concerning countermeasures identified in the present document, the scope includes:

- consideration of merits and demerits (i.e. pros and cons) of identified countermeasures;
- evaluation of countermeasures to determine:
    1) the need for a standardised solution/implementation,
    2) availability of existing standardised solutions (e.g. from other SDOs),
    3) the need for a new standardised solution (either from another SDO or from ETSI M2M).

Additionally:

- Threats against, or originating from, any stakeholders may be considered.
- Countermeasures which are normal practice in IT systems (e.g. maintenance logs, firewalls) are out of scope.

Content in the present document may lead to new requirements in future releases of TS 102 689 [i.5] and normative text in TS 102 690 [i.6].

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] Document M2M(10)0278r1: "Security Handling in ETSI TC M2M".

[i.2] Work Item Description for WI00012.

[i.3] CPNI (Centre for the Protection of National Infrastructure) criteria.

NOTE: See http://www.cpni.gov.uk/.

[i.4] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.5] ETSI TS 102 689 (V1.1.1): "Machine-to-Machine communications (M2M); M2M service requirements".

[i.6] ETSI TS 102 690: "Machine-to-Machine communications (M2M); M2M functional architecture".

[i.7] ETSI TR 102 725: "Machine to Machine Communications (M2M); M2M definitions".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

NOTE: References have been included where definitions have been obtained from other sources. Where appropriate, additional text has been added in square brackets.

asset: anything that has value to the [stakeholder], its business operations and its continuity [i.4]

Device Lower Layer (DLL): component of the Lower Layer in a M2M Device

Lower Layer (LL): allows DSCL, GSCL and NSCL Components to exchange data on behalf of applications, and perform other appropriate communication

Gateway Lower Layer (GLL): component of the Lower Layer in a M2M Gateway

impact: result of an [unwanted] information security incident, caused by a threat, which affects assets [i.4]

incident: event relevant to the analysed system

M2M area network layer: provides the communication between DA/GA components and DSCL/GSCL components

M2M service provider's domain: domain which includes the Network Application Domain and any standardised systems under the control of the M2M Service Provider which interact with the M2M Service Capabilities

M2M System: comprises Network Application Domain, M2M Devices Domain and any interfaces or networks required to connect those entities

mitigation: limitation of the negative consequences of a particular event [i.4]

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [stakeholder] [i.4]

Reference Integrity Value (RIV): data used in the (optional) integrity checking of functions in M2M Devices/Gateways

NOTE: An actual integrity measurement is compared with the corresponding Reference Integrity Value, to produce a pass/fail result. RIVs are made trustworthy, e.g. by the use of verifiable signatures.

threat: potential cause of an incident that may result in harm to a system or organization [i.4]

NOTE: A Threat is enacted by a Threat Agent and may lead to an Unwanted Incident breaking certain pre-defined security objectives [i.4].

threat agent: entity that can adversely act on an asset [i.4]

unwanted incident: incident such as loss of confidentiality, integrity and/or availability [i.4]

3.2 Abbreviations

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

DA	Device Application
DAMAN	Device Application M2M Area Network (Component)
DLL	Device Lower Layer (Component)
DSCL	Device Service Capability Layer
DSMAN	DSCL M2M Area Network (Component)
GA	Gateway Application
GAMAN	Gateway Application M2M Area Network (Component)
GLL	Gateway Lower Layer (Component)
GSCL	Gateway Service Capability Layer
GSMAN	GSCL M2M Area Network (Component)
ISE	Independent Security Element
MAS	M2M Authentication Server
MFF	M2M Form Factor (UICC)
MSBF	M2M Service Bootstrapping Function
NA	Network Application
NAD	Network Applications Domain
NSCL	Network Service Capability Layer
OMTP	Open Mobile Terminal Platform
RIV	Reference Integrity Value
SCs	Service Capabilities
SDO	Standards Development Oranisation
TCG	Trusted computing Group
UICC	Integrated Circuit Card

4 Methodology Used for Analysis of Threats and Risks

The technique used here (based on [i.3] and [i.4]) is to:

1) Describe a threat and list the:
   - References of M2M use cases for which the analysis applies
   - References of M2M use cases for which the analysis does not apply
   - Targets of the attack
   - Stakeholders affected
2) Assign a weight to the likelihood of the threat by considering the:
   - Threat Agent(s):
     a) Individual Criminal: Opportunistic individual with simple profit motive
     b) Hacker: Derives thrills from intrusion or destruction of property, without strong agenda
     c) Disaffected employee: Current or former employee with intent to harm the company
     d) Commercial Competitor: Business adversary who competes for revenues or resources (acquisitions, etc.)
     e) Organised Crime syndicates: organized crime organization with significant resources
     f) Extremist and Hacktivist: Highly motivated but non-violent supporter of cause or Highly motivated, potentially destructive supporter of cause
     g) Terrorist: Person who relies on the use of violence to support personal socio-political agenda
     h) Nation State: State-sponsored attacker with significant resources to affect major disruption on national scale:
        - 0 = No Agent
        - 1= Individual criminal, Hacker, Disaffected employee
        - 2= Commercial Competitor
        - 3= Organised crime syndicates, Extremist, Hacktivist
        - 4 = Terrorist, Nation State
   - Motivation: Examples are Financial, Political, Revenge, Gratification) and potential inhibitors such as risk of detection, attitude to risk:
     - 0= No Motivation
     - 1= Low motivation
     - 2= Moderate motivation
     - 3= Substantial motivation
     - 4= High motivation
   - Opportunity. Examples are Physical Proximity, Electronic Proximity, Protocol Standards Architectural Standards, Communications Security, Sustainability (minutes, hours, weeks days, months), needed for attack:
     - 0= No opportunity
     - 1= little opportunity

- 2= limited opportunity
- 3= Substantial opportunity
- 4= High opportunity

- Capability: Examples are Education levels, Intelligence gathering/ targeting, Social engineering ability, Knowledge/ expertise (laymen, proficient persons, experts), Equipment Access, Access to training manuals and procedures, Information Assurance skill levels, Reverse engineering ability, Financial resources, Equipment required (standard, specialised, custom):
  - 0 = No capability
  - 1= little capability
  - 2= limited capability
  - 3= Substantial capability
  - 4= High capability

3) Assign a weight to the seriousness of the impact of a successful attack, by considering:

- **Effect on the stakeholder** from no impact or minor localised inconvenience to severe damage to systems/processes that support important national security/defence requirements.
- **Detect-ability** as a relative measure of the potential for the provider of a service to become aware of an attack or attempted attack before stake holder is impacted. This potential is increased by such factors as:
  - Need for physical proximity to mount attack
  - Need for an attackers sustained presence/proximity
  - Effective audit and event management highlighting evidence of attack pre-planning e.g. social engineering or pre-probing, attempts to thwart recovery and the complexity and diversity of approach
  - Provision of alarms and an effective response to them

  This potential is decreased by such factors as:
  - Requirement for Electronic Proximity only
  - Sustained presence by attacker not required e.g. attack by "single" shot commands "De-resister all M2M devices"
  - Lack of audit and event management and effective analysis
  - Provision of alarms and effective response is not possible
- **Recoverability** as a relative measure of the potential for the provider of a service to minimise the impact of an attack, to the consumer of the service. Usually only applies to loss of integrity and availability, as once confidentiality is lost, it is lost for good. This potential is increased by such factors as:
  - Segregation containment (impact can be limited to a small numbers of devices, etc.)
  - Effective audit and event management highlighting what was changed by what and when
  - Need for an attackers sustained presence/proximity
  - Mechanisms for proof of system integrity
  - Mechanisms to restore to secure state requiring electronic proximity only

  This potential is decreased by such factors as:
  - No segregation or containment - millions of devices/consumers impacted

- Ineffective audit and event management - rebuild all from scratch as no evidence that incident was contained
- No mechanisms to restore to secure state or procedures require ALL devices to be returned, re-manufactured and then re-installed and configured

4) Multiply the two weights (likelihood x impact) together to arrive at an overall risk score. The level of risk determines whether or not counter-measures are required.

5) Describe and evaluate the Potential counter-measures.

6) Decide on the responsibility for mitigation, if any is required.

NOTE 1: **The methodology assumes an unprotected system**, i.e. that no counter-measures have been implemented. This is because [i.6] is still a work-in-progress at the time of writing. Thus, the present document provides an absolute set of recommendations which is independent of the current version of [i.6].

NOTE 2: The M2M service layer has to be able to be operate over a wide variety of access network technologies, so few assumptions can be made as to the level of security provided by such networks.

NOTE 3: Threats against public communications network operators and other stakeholders are considered only if they have a direct impact (other than simple non-availability) upon the M2M Service Layer or the M2M functional requirements.

NOTE 4: Counter-measures in the Threats sections are described in the present tense, e.g. "keys are stored in a Secured Environment". Words like "should" or "may" are not used until the Recommendations section.

Likelihood:

- Weight 1 "low likelihood". Threat Agent with low motivation and little opportunity and capability for launching and sustaining an effective attack.
- Weight 2 "moderate likelihood". Threat Agent with medium motivation, limited opportunity and capability.
- Weight 3 "substantial likelihood". Threat Agent with High motivation, limited opportunity and capability Or medium motivation, significant opportunity and capability.
- Weight 4 "severe likelihood". Threat Agent with High motivation, high opportunity and capability.

Seriousness of the impact of a successful attack:

- Weight 1 "minor impact" Minor or no effect on the stakeholder, with resulting inconvenience very localised. No external impact or visibility of problems.
- Weight 2 "serious impact" Failure of important revenue generating systems/processes and/or support systems/ processes. Impact would be noticeable to parties other than the stakeholder. Possible repercussions for revenue, penalty payments, market share and customer confidence.
- Weight 3 "Enterprise" Irreparable damage to key systems/processes with probable widespread impact. Ability of the enterprise to continue operations would be in jeopardy; major regulatory, licensing and legal implications. Impact would be very visible and would cause very severe cash flow problems and large-scale defection of major customers of the stakeholder.
- Weight 4 "National" National Infrastructure - Severe damage to systems/processes that support important infrastructure requirements. National Security - Severe damage to systems/processes that support important national security/defence requirements.

Risk = likelihood x seriousness:

- Score 1, 2, 3 "minor risk". No primary need for counter measures.
- Score 4, 6, 8 "major risk". Counter measures are required to minimize this risk as soon as possible.
- Score 9, 12, 16 "critical risk". Counter measures are required to minimize this risk, with a high priority.

- Score multiples 5, 7, 10, 11, 13, 14 are not possible in this scheme.

Responsibility for mitigation is assigned as follows:

1) Mitigation requires new functionality in ETSI M2M specifications.

2) Mitigation can be addressed by existing functionality in other SDOs' specifications.

3) Mitigation requires new functionality in the specifications of another SDO (requires liaison).

4) The threat can be avoided (e.g. by changes to architecture).

5) Mitigation is not necessary (where risk is small, or if it is out of scope for standardisation, or if the mitigation is already taken into account in service layer specifications).

5 System Architecture

5.1 High-Level Architecture

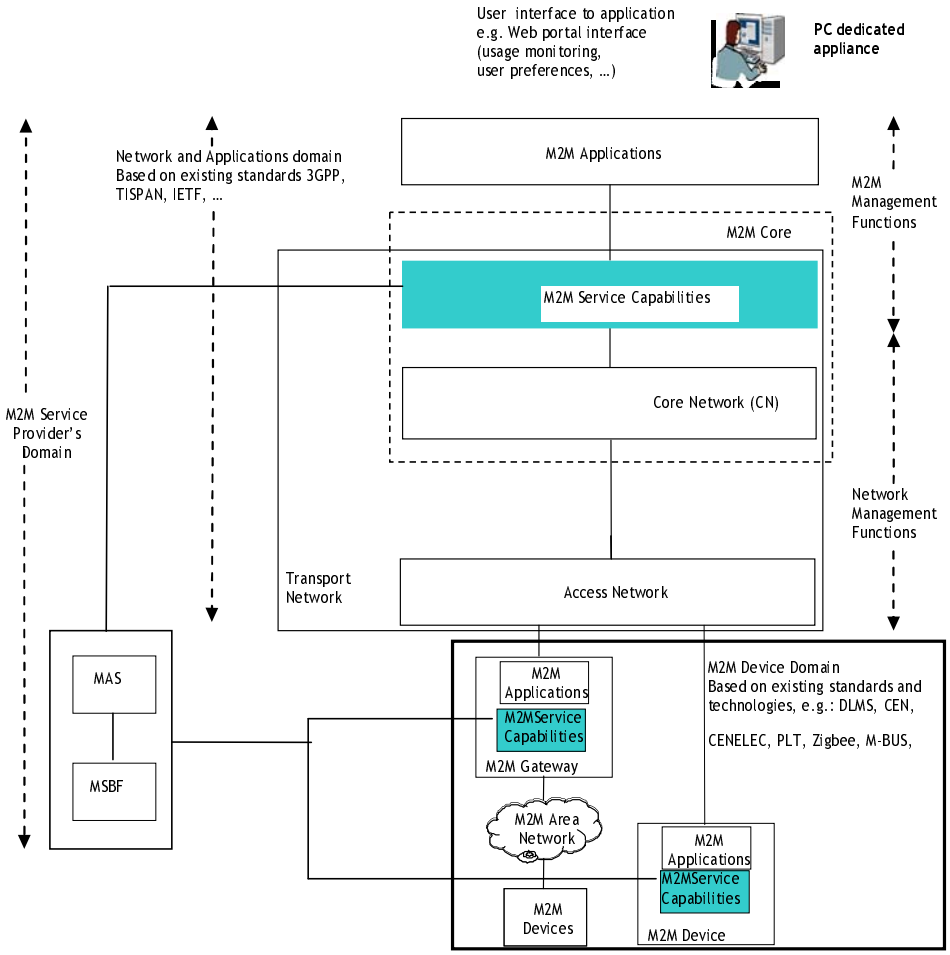


Figure 1: M2M high level system overview

Figure 1 shows the high-level system architecture [i.6]. Threats directly against the highlighted M2M Service Capabilities are the focus of threats described in clause 7. Threats against the other parts of the system architecture, but which have an impact on the M2M Service Capabilities, are the focus of threats described in clause 8.

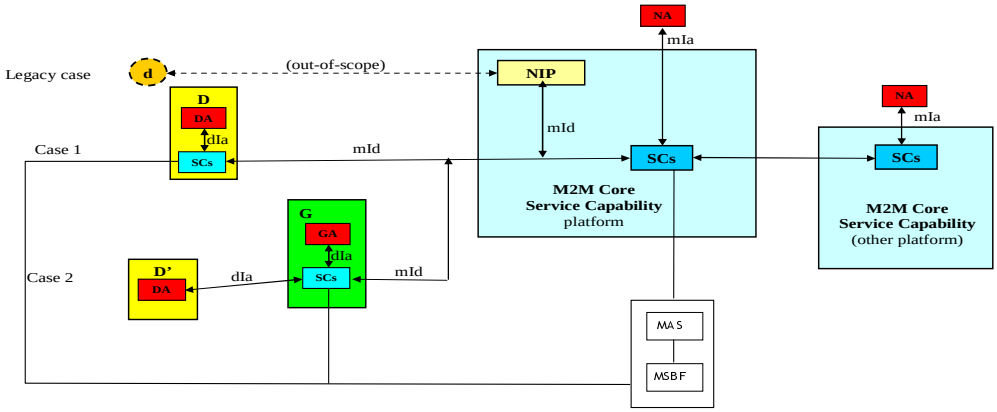


Figure 2: Service Capabilities functional architecture framework

Figure 2 above shows the interfaces between elements of the M2M service layer [i.6]. Only those aspects which are in scope for Release 1 of [i.6] are included.

NOTE: Figures 1 and 2 may need to be updated from time to time, in order to track the development of the system architecture in [i.6].

5.2 Layered Model for the M2M System

This clause is intended to as background information providing a model for the M2M system that provides common terminology for effectively communication of details of threats. This model is believed to be consistent with the current M2M architecture (TS 102 690 [i.6]). Where existing terminology was considered inadequate, this model adds new definitions.

The M2M system is modelled as being components within layers. Unless otherwise noted, a component may reside in the Network domain or the Device domain:

- The top layer is the Application Layer. The DA/GA/NA Components rely on the Service Layer for abstracting the connectivity layer.
- Below this layer lies the M2M Service Layer. The Service layer is an abstraction layer between the Application Layer and the Lower Layer. The Service Layer relies on the Lower Layer for communication between DSCL, GSCL and NSCL components. The Service Layer relies on the M2M Area Network Layer for communication between DA/GA components and the DSCL/GSCL components.
- Two parallel connectivity layers:
  - The M2M Area Network Layer provides the communication between DA/GA components and DSCL/GSCL components. The component of the M2M Area Network layer in a M2M DA/GA/DSCL/GSCL is called the DA/GA/DSCL/GSCL M2M Area Network component for which we use the notation DAMAN, GAMAN, DSMAN, GSMAN.

NOTE: This description assumes that the following options are possible for the location of the DAMAN/GAMAN and corresponding DSMAN/GSMAN:

- Co-located on a single physical component.
- Located on distinct physical components with direct communication between components (e.g. USB).
- Located on distinct physical components communicating via a wired network (e.g. Ethernet).
- Located on distinct physical components communicating via a wireless technology.

- The Lower Layer allows DSCL or GSCL to exchange data with NSCL Components on behalf of applications, and perform other appropriate communication. The Access Network and Core Network (of Figure 1 above) form the NAD side of the Lower Layer. The component of the Lower Layer in a M2M Device/Gateway is called the Device/Gateway Lower Layer (DLL/GLL) component.

The focus of the analysis is the M2M Service layer, but it is important to consider how threat agents may abuse the M2M Service layer to have a negative impact on stakeholders in the other layers, and vice versa.

6 Stakeholders

Stakeholders are entities who facilitate and/or participate in the legitimate operation of the M2M ecosystem. A stakeholder may also be involved in threats to the M2M ecosystem, either as the target of an attack or as an attacker. The stakeholders who may be relevant to the threat/risk analysis are, in alphabetical order.

- Applications Developer
- Consumer of M2M Services
- ISE Supplier
- Manufacturer of MAS/MSBF
- Manufacturer of M2M Devices and/or M2M Gateways
- Manufacturer of M2M Core
- M2M Device/Gateway Manager
- M2M Service Provider
- M2M (W)LAN Operator
- Public Communications Network Operator
- System Administrator

7 Trust Model

NOTE: The following statements only apply to trusted instances of the stakeholder. For example, the statement about "Trusted manufacturer" does not apply to manufacturers who are not trusted.

Any entity (such as a trusted Manufacturer of M2M Devices and/or M2M Gateways), who is trusted by the M2M Service Provider and who is responsible for handling sensitive information such as cryptographic keys is trusted to protect such information while in possession of it and not to use it for unauthorised purposes.

A trusted M2M Service Provider is trusted by other stakeholder not to use sensitive information, such as cryptographic keys or privacy-related data, for unauthorised purposes.

A Trusted Environment [i.7] is trusted by relying parties to perform its Integrity Validation measurements [i.7] according to specification, without providing proof of its own integrity.

In an M2M Device or M2M Gateway, any function whose Integrity Validation is anchored in the Trusted Environment is trusted by relying parties after its integrity has been validated. Such trust may have to be periodically re-established, according to policy.

A Secured Environment [i.7] is trusted by relying parties to perform its functions (i.e. storage, management, execution, Integrity Validation comparisons) according to specification, without providing proof of its integrity, unless its integrity is required to be validated by the Integrity Validation process.

Stakeholders who operate IT systems are trusted by other stakeholder to configure, operate and maintain them in accordance with accepted good practice. This trust may be subject to periodic review, e.g. by audit.

M2M service-layer functions are trusted not to have access to access-network credentials.

NOTE: More work is required to describe the trust relationships between the various stakeholders.

8 Type 1 Threats, Specific to the M2M Service Layer and its Interfaces

8.1 Threat 1: Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways

8.1.1 Description

Long-term service-layer keys are discovered while they are stored in M2M Devices or M2M Gateways and are copied. Discovery may be achieved e.g. by the monitoring of internal processes (e.g. by Differential Power Analysis), or by reading the contents of memory (by hardware probing or by use of local management commands). Copied keys may then be used to impersonate M2M Devices and/or M2M Gateways. This attack may be perpetrated against the key-storage functions of D-type Devices or Gateways.

References of M2M use cases for which the analysis applies: All

References of M2M use cases for which the analysis does not apply: None

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device (no)

Stakeholders affected: Consumer of M2M services, M2M Service Provider, ISE manufacturer, M2M Device/Gateway Manufacturer.

8.1.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Criminal, Hacker, Disaffected employee, Commercial Competitor, therefore 2.
  - Their motivation: Commercial competitor therefore, financial, but inhibited by risk of detection and damage to reputation , therefore 2.
  - Their opportunity: has physical access and electronic proximity, known architectural and protocols and can sustain the attack but only one device at a time. Therefore limited opportunity = 2.
  - Their capability: Commercial competitor has knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore limited capability = 2.
- Maximum score in 1 to 4 above is 2 therefore the likelihood of a successful attack: 2 (moderate on an unprotected Device/Gateway - depends on level of protection in Device/Gateway implementation).
- Impact assumptions:
  1) Effect on stakeholders(s): minor localised inconvenience.
  2) Detect-ability: increased by need for physical proximity to mount attack but decreased as sustained presence by attacker not required and the potential lack of audit and event management on device gateways and alarms and effective response for devices may not be practical.
  3) Recoverability: increased as impact is limited to a small numbers of devices but decreased by potential lack of segregation or containment - millions of devices/consumers impacted if keys are non unique and may need to rebuild all from scratch due to lack of evidence that incident was contained. May be no mechanisms to restore to secure state or procedures require ALL devices to be returned, re-manufactured and then re-installed and configured.

- Seriousness of Threat at M2M Service Layer: 2 (serious impact).
- Risk (i.e. priority) = seriousness x likelihood = 4 (at the low end of "major risk").
- Is mitigation required?: yes. Counter measures are required to minimize this risk as soon as possible.

8.1.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes. However good protection also requires implementation techniques (e.g. SPA/DPA protection) that are out of scope of standardization and which may be better addressed by some level of device certification (e.g. Common Criteria or FIPS).
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided: no.
- Accepted: no.

8.1.3.1 Potential Counter-Measures

CM1: M2M long-term service-layer keys (other than public keys) are stored in a Secured Environment [i.7] (whose tamper-resistance may be certified) which renders it infeasible for the attacker to discover the value of keys by logical or physical means.

Advantages:

- Resists the attack.
- A lot of prior art exists in the form of specifications of OMTP, TCG, ETSI SCP, etc.

Disadvantages:

- Cost penalty (development cost and per-item cost), may or may not be significant.
- Need to specify and demonstrate the level of security assurance across the range of manufacturers and their products.
- Difficult to test.
- May require a certification process.

CM2: The Secured Environment will not reveal the value stored keys, even to a management system or to an authorised representative of the M2M Core Operator, such as a System Administrator.

Advantages:

- Resists the attack.
- A lot of prior art exists in the form of specifications of OMTP, TCG, ETSI SCP, etc.

Disadvantages:

- None.

CM4: the execution of Sensitive Functions (e.g. the derivation of further keys from M2M long-term service-layer keys) never causes long-term service-layer keys to be exposed outside of the Secured Environments in which they are stored.

Advantages:

- Resists the attack.
- A lot of prior art exists in the form of specifications of OMTP, TCG, ETSI SCP, etc.

Disadvantages:

- Increases the cost and complexity of the Secured Environment.

CM6: The Secured Environment containing the M2M long-term service keys is bound to the M2M Device or M2M Gateway, using physical and/or logical means.

Advantages:

- Resists the attack. Keys cannot be stolen (and Device/Gateway rendered inoperable) by removal of Secured Environment.

Disadvantages:

- Cost penalty due to mechanical complexity if the secured environment is a removable ISE. If it is a soldered-on MFF UICC, this may not be a problem.
- Not easy to specify the degree of non-removability.
- Standards for logical binding of UICC to Device/Gateway are of limited effectiveness.

8.1.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM1	Gateway, D-type Device	ETSI M2M. Material from OMTP, TCG, ETSI SCP specifications may be useful.
CM3	Gateway, D-type Device	ETSI M2M. Material from OMTP, TCG, ETSI SCP specifications may be useful.
CM4	Gateway, D-type Device	ETSI M2M. Material from OMTP, TCG, ETSI SCP specifications may be useful.
CM6	Gateway, D-type Device	If it is an ISE such as UICC, then the SDO which standardises the ISE (e.g. ETSI SCP for UICC and 3GPP for logical binding), otherwise ETSI M2M.

8.2 Threat 2: Deletion of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways

8.2.1 Description

Long-term service-layer keys are deleted or deprecated while they are stored in M2M Devices or M2M Gateways, in order to prevent operation. It may be achieved by use of management commands (including impersonation of a system Manager) or by removal of the ISE [i.7] if present and if removable. This attack may be perpetrated against the key-storage functions of D-type M2M Devices.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device: (no).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, M2M Device/Gateway Manager, System Administrator.

8.2.2 Assessment of Risk

- Likelihood assumptions:

  1) Threat agents: Criminal, Hacker, Disaffected employee, Commercial Competitor, therefore 2.

  2) Their motivation: Commercial competitor therefore, financial, but inhibited by risk of detection and damage to reputation, therefore 2.

  3) Their opportunity: has physical access and electronic proximity, known architectural and protocols and can sustain the attack but only one device at a time. Therefore limited opportunity = 2.

  4 Their capability: Commercial competitor has knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore limited capability = 2.

- Maximum score in 1) to 4) above is 2 therefore the likelihood of a successful attack: 2 (moderate likelihood if unsecured remote commands can be used).

- Impact assumptions:

  1) Effect on stakeholders(s): minor localised inconvenience.

  2) Detect-ability: increased by need for physical proximity to mount attack but decreased as sustained presence by attacker not required and the potential lack of audit and event management on device gateways and alarms and effective response for devices may not be practical.

  3) Recoverability: increased as impact is limited to a small numbers of devices but decreased by potential lack of segregation or containment - millions of devices/consumers impacted if keys are non unique and may need to rebuild all from scratch due to lack of evidence that incident was contained. May be no mechanisms to restore to secure state or procedures require ALL devices to be returned, re-manufactured and then re-installed and configured.

- Seriousness of Threat at M2M Service Layer: 2 (serious if it becomes widespread. Can be detected and new keys can be provisioned but the attack could then re-occur).

- Risk (i.e. priority) = seriousness x likelihood = 4 (at the low end of "major risk").

- Is mitigation required?: yes. Counter measures are required to minimize this risk as soon as possible.

8.2.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes

- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no

- Avoided: no

- Accepted: no

8.2.3.1 Potential Counter-Measures

CM8: access to and/or the modification of stored Sensitive Data requires strong (i.e. cryptographic) authentication of the accessing/modifying party, followed by authorisation.

- Advantages:

  - Resists the attack

- Disadvantages:
  - Cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms, which may or may not be significant
  - Communications overheads for remote management

8.2.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	Gateway, D-type Device	ETSI M2M. Material from OMA specifications may be useful

8.3 Threat 3: Replacement of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways

8.3.1 Description

Long-term service-layer keys are replaced while they are stored in M2M Devices or M2M Gateways, in order to modify its operation. It may be achieved by use of management commands (including impersonation of a system Manager) or by removal of the ISE [i.7] if present and if removable. This attack may be perpetrated against the key-storage functions of D-type M2M Devices.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, M2M Device/Gateway Manager, System Administrator.

8.3.2 Assessment of Risk

- Likelihood assumptions:
  1) Threat agents: Criminal, Hacker, Disaffected employee, Commercial Competitor, therefore 2.
  2) Their motivation: Commercial competitor therefore, financial, but inhibited by risk of detection and damage to reputation , therefore 2.
  3) Their opportunity: has physical access and electronic proximity, known architectural and protocols and can sustain the attack but only one device at a time. Therefore limited opportunity = 2.
  4) Their capability: Commercial competitor has knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore limited capability = 2.

Maximum score in 1) to 4) above is 2 therefore the likelihood of a successful attack: 2 (moderate likelihood if unsecured remote commands can be used).

- Impact assumptions:
  1) Effect on stakeholders(s): minor localised inconvenience.
  2) Detect-ability: increased by need for physical proximity to mount attack but decreased as sustained presence by attacker not required and the potential lack of audit and event management on device gateways and alarms and effective response for devices may not be practical.

3) Recoverability: increased as impact is limited to a small numbers of devices but decreased by potential lack of segregation or containment - millions of devices/consumers impacted if keys are non unique and may need to rebuild all from scratch due to lack of evidence that incident was contained. May be no mechanisms to restore to secure state or procedures require ALL devices to be returned, re-manufactured and then re-installed and configured.

- Seriousness of Threat at M2M Service Layer: 2 (serious if it becomes widespread. Can be detected and new keys can be provisioned but the attack could then re-occur).
- Risk (i.e. priority) = seriousness x likelihood = 4 (at the low end of "major risk").
- Is mitigation required?: yes. Counter measures are required to minimize this risk as soon as possible.

8.3.3 Mitigation of Risk

This risk should be:

- mitigated by ETSI M2M specifications: yes
- transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no
- avoided: no
- accepted: no

8.3.3.1 Potential Counter-Measures

CM8: the modification of stored Sensitive Data requires strong (i.e. cryptographic) authentication of the modifying party.

- Advantages:
  - Resists the attack.
- Disadvantages:
  - Cost, e.g. of providing crypto authentication means to System Administrators, which may or may not be significant.
  - Communications overheads for remote management.

8.3.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	Gateway, D-type Device	ETSI M2M. Material from OMA specifications may be useful.

8.4 Threat 4: Discovery of Long-Term Service-Layer Keys Stored in the SCs of the M2M Core

8.4.1 Description

Long-term service-layer keys are discovered which are stored in the SCs of the M2M Core and are copied. Copied keys (if they are shared symmetric keys) may then be used to impersonate Devices or Gateways. Discovery of the keys may be achieved e.g. by the monitoring of internal processes, or by reading contents of memory locations. The methods of attack include remote hacking and illicit use of management or maintenance interfaces.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, M2M Service Provider, System Administrator.

8.4.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Hacker, Disaffected employee (with admin access), commercial competitor, organised crime syndicate, therefore score 3.
  - Their motivation: high motivation due to desire to attack a complete eco-system, therefore 4.
  - Their opportunity: may have physical access and/or electronic proximity and can attack the whole eco-system. Therefore score 4.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 4.
- Maximum score above is 4 therefore the likelihood of a successful attack: 4 (severe likelihood if no countermeasures are in place).
- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: without suitable counter-measures, it would be difficult or impossible to detect the attack.
  - Recoverability: moderate. It may be necessary to re-provision the whole eco-system with new keys. The attack could then re-occur.
- Seriousness of Threat at M2M Service Layer: 3 (a successful attack of this type on the M2M core is obviously an "Enterprise" level problem).
- Risk (i.e. priority) = seriousness x Likelihood = 12 (in the middle of the "critical risk" category).
- Is mitigation required? (yes). Counter measures are required to minimize this risk, with a high priority.

8.4.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no
- Avoided (e.g. by changes to specified functionality): no
- Accepted (where risk is small, or if it is out of scope for standardisation): no

8.4.3.1 Potential Counter-Measures

CM1, as in threat 1 but applied to the Secured Environment in the M2M Core.

CM3, as in threat 1 but applied to the Secured Environment in the M2M Core.

CM4, as in threat 1 but applied to the Secured Environment in the M2M Core.

CM6, as in threat 1 but applied to the Secured Environment in the M2M Core.

8.4.3.2 Responsibility for Counter-Measures

See CMs 1, 3, 4, 6 in Threat 1.

8.5 Threat 5: Deletion of Long-Term Service-Layer Keys Stored in the SCs of an M2M Core

8.5.1 Description

Long-term service-layer keys are deleted or deprecated while they are stored in the SCs of an M2M Core, in order to prevent operation. It may be achieved by use of management commands (including impersonation of a System Administrator).

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, System Administrator.

8.5.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Hacker, Disaffected employee (with admin access), commercial competitor, organised crime syndicate, extremist/hacktivist, nation state therefore score 4.
  - Their motivation: high motivation due to desire to attack a complete eco-system, therefore 4.
  - Their opportunity: may have physical access and/or electronic proximity and can attack the whole eco-system. Therefore score 4.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 4.
- Maximum score above is 4 therefore the likelihood of a successful attack: 4 (severe likelihood if no countermeasures are in place).
- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: easy to detect that the keys are no longer present or usable.
  - Recoverability: difficult. It may be necessary to re-provision the whole eco-system with new keys. Then the attack might be repeated.
- Seriousness of Threat at M2M Service Layer: = 4 "National" National Infrastructure - Severe damage to systems/processes that support important infrastructure requirements. National Security - Severe damage to systems/processes that support important national security/defence requirements. This is because a successful attack could bring down a complete eco-system by temporarily preventing the authentication of all Devices and Gateways. The attack could be detected but, without counter-measures, it could be repeated.
- Risk (i.e. priority) = seriousness x likelihood = 16 (at the high end of "critical risk").
- Is mitigation required?: yes. Counter measures are required to minimize this risk, with a high priority.

8.5.3 Mitigation of Risk

This risk should be:

- mitigated by ETSI M2M specifications: yes
- transferred: no
- avoided: no
- accepted: no

8.5.3.1 Potential Counter-Measures

CM8 as above.

8.5.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	M2M Core	ETSI M2M.

8.6 Threat 6: Discovery of Long-Term Service-Layer Keys Stored in MSBF or MAS

8.6.1 Description

Long-term service-layer keys are discovered which are stored in the M2M MSBF/MAS servers, and are copied. Copied keys may then be used to impersonate Devices or Gateways.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, M2M Service Provider, System Administrator.

8.6.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Criminal, Hacker, Disaffected employee, Commercial Competitor, therefore 2.
  - Their motivation: Commercial competitor therefore, financial, but inhibited by risk of damage to reputation , therefore 2.
  - Their opportunity: has physical access and/or electronic proximity, known architectural and protocols and can sustain the attack but only one device at a time. Therefore substantial opportunity = 3.
  - Their capability: Commercial competitor has knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore limited capability = 2.

Maximum score in 1 to 4 above is 3 therefore the likelihood of a successful attack: 3 (substantial likelihood if unsecured remote commands can be used).

- Impact assumptions:

  1) Effect on stakeholders(s): major inconvenience if keys for a whole population of Devices/Gateways are copied.

2) Detect-ability: decreased as sustained presence by attacker not required for a remote attack and the potential lack of audit and event management on device gateways and alarms and effective response for devices may not be practical.

3) Recoverability: decreased: millions of devices/consumers impacted if keys are non unique and may need to rebuild all from scratch due to lack of evidence that incident was contained. May be no mechanisms to restore to secure state.

- Seriousness of Threat at M2M Service Layer: 3 (a successful attack of this type on the MAS/MSBF is obviously an "Enterprise" level problem).
- Risk (i.e. priority) = seriousness x Likelihood = 9 (the low end of the "critical risk" category).
- Is mitigation required? (yes). Counter measures are required to minimize this risk, with a high priority.

8.6.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes (MAS and MSBF are functions defined specifically by ETSI M2M specifications).
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no (MAS and MSBF are functions to be specified by ETSI M2M): no.

8.6.3.1 Potential Counter-Measures

CM1 as in threat 1.

CM3 as in threat 1, but applied to the System Administrators of the MAS/BSBF.

CM4 as in threat 1, but applied to the Secured Environments in the MSBF/MAS.

CM6 as in threat 1, but applied to the Secured Environments in the MSBF/MAS.

8.6.3.2 Responsibility for Counter-Measures

See CMs 1, 3, 4, 6 in Threat 1.

8.7 Threat 7: Deletion of Long-Term Service-Layer Keys Stored in the MSBF/MAS

8.7.1 Description

Long-term service-layer keys are deleted or deprecated while they are stored in the MSBF/MAS, in order to prevent operation. It may be achieved by use of management commands (including impersonation of a System Administrator).

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, System Administrator.

8.7.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Hacker, Disaffected employee (with admin access), commercial competitor, therefore score 2.
  - Their motivation: low motivation, since it only affects the provisioning process, therefore 2.
  - Their opportunity: would need Physical Proximity, Electronic Proximity, Architectural Standards, short sustainability . Therefore score 2.
  - Their capability: threat agents would have knowledge/ expertise of the MSBF/MAS, therefore score 3.
- Maximum score above is 3 therefore the likelihood of a successful attack: 3 (substantial likelihood if no countermeasures are in place).
- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: loss of keys would be easily and immediately detectable.
  - Recoverability: should not be difficult.
- Seriousness of Threat at M2M Service Layer: 2 (serious if it becomes widespread. Can be detected and new keys can be provisioned but the attack could then re-occur).
- Risk (i.e. priority) = seriousness x Likelihood = 6 (at the mid-point of "major risk").
- Is mitigation required?: yes. Counter measures are required to minimize this risk as soon as possible.

8.7.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided: no.
- Accepted: no.

8.7.3.1 Potential Counter-Measures

CM8 as above.

8.7.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	MSBF/MAS	ETSI M2M

8.8 Threat 8: Discover Keys by Eavesdropping on Communications Between Entities

8.8.1 Description

Keys are discovered by eavesdropping on messages at the M2M service layer between components in the M2M Service Provider's Domain, M2M Devices and M2M Gateways. The eavesdropping may physically occur in:

- a LAN which connects M2M Devices to an M2M Gateway.
- a WAN which connects M2M Gateways and M2M Devices to the M2M Core.
- a WAN which connects provisioning servers to M2M Devices, M2M Gateways and an M2M Core.

This description assumes that the network layer does not provide any protection against this attack. The attack may therefore exploit lack of protection in communications, or vulnerabilities in protected communications, at the M2M service layer. The attack may discover keys from examination of communications used in the provisioning of credentials but also may infer keys by examining normal operational communications which use those keys. The method of attack may involve the exploitation of vulnerable algorithms, or the incorrect usage of algorithms, so as to be able to infer the keys used in encrypted communications.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Consumer of M2M Services, M2M Device/Gateway Manager, M2M Service Provider, M2M (W)LAN Operator, Public Communications Network Operator, System Administrator.

8.8.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: criminal, hacker, commercial competitor, hacktivitist, therefore score 3.
  - Their motivation: financial but limited by threat of detection and damage to reputation, therefore 2.
  - Their opportunity: may monitor IP communications but can attack only 1 Dev ice/Gateway at a time. Therefore score 2.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 2.
- Maximum score above is 3 therefore the likelihood of a successful attack: 3 (substantial likelihood if no countermeasures are in place):
  - Effect on stakeholders(s): minor localised inconvenience.
  - Detect-ability: minimal, as sustained presence by attacker is not required.
  - Recoverability: increased as impact is limited to a small numbers of devices but decreased by potential lack of segregation or containment - millions of devices/consumers impacted if keys are non unique and may need to reprovision keys due to lack of evidence that incident was contained.
- Seriousness of Threat at M2M Service Layer: 3 "Enterprise" (if it results in discovery of Kr and Ks in large numbers).
- Risk (i.e. priority) = seriousness x likelihood = 9 (at the low end of "critical risk").
- Is mitigation required? Yes. Counter measures are required to minimize this risk, with a high priority.

8.8.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no (since we assume that the (W)LAN or WAN cannot be relied on to provide adequate protection).
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.8.3.1 Potential Counter-Measures

CM9: a security association is established between communicating entities, which provides for mutual authentication and confidentiality.

Advantages:

- Resists the attack.
- A well-established counter-measure.

Disadvantages:

- Communications overhead.

CM10: the security association between the communicating entities uses protocols which are proven to resist man-in-the-middle attacks.

Advantages:

- Resists the attack.
- A well-established counter-measure.

Disadvantages:

- Communications overhead.

CM11: M2M service-layer keys in a provisioning message are encrypted for confidentiality, independently of any confidentiality provided by the messaging protocol.

Advantages:

- Resists the attack.
- A well-established counter-measure.

Disadvantages:

- Requires more encryption, more keys; possibly requires PKI.

CM12: during provisioning of M2M service-layer keys, the protocol end-points for the encryption/decryption of those M2M service keys are Secured Environments.

Advantages:

- Resists the attack.

Disadvantages:

- Increases the cost and complexity of the Secured Environment, which may or may not be significant.

CM13: communications whose security is anchored in M2M service-layer keys use session keys, i.e. keys with a limited lifetime which can be set by security policy. Session keys can be derived from M2M service-layer keys.

Advantages:

- Resists the attack.
- A well-established counter-measure.

Disadvantages:

- Requires more crypto operations.

CM14: secured communications use only those cryptographic algorithms which are assessed by cryptography experts as being fit for purpose, e.g. the length and randomness of cryptographic parameters is sufficient to resist a brute-force attack. Note: the details of algorithms used would be decided in the stage 3 specifications.

Advantages:

- Resists the attack
- A well-established counter-measure
- Easy to test

Disadvantages:

- Places restrictions on some stakeholders

CM15: industry-accepted recommendations for the use of cryptographic algorithms in secured communications are followed.

Advantages:

- Resists the attack
- A well-established counter-measure
- Easy to test

Disadvantages:

- Places restrictions on some stakeholders
- Recommendations may change over time
- Possibly difficult to specify a complete set of recommendations

8.8.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM9	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M specifying security associations from existing specifications (3GPP, OMA, etc)
CM10	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M specifying security associations from existing specifications (3GPP, OMA, etc)
CM11	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M specifying security associations from existing specifications (3GPP, OMA, etc)
CM12	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M but importing requirements from existing specifications, e.g. OMTP, ETSI SCP, where possible
CM13	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M
CM14	secured communications use only those cryptographic algorithms which are assessed as being fit for purpose, e.g. the length and randomness of keys is sufficient to resist a brute-force attack	ETSI M2M
CM15	industry-accepted recommendations for the use of cryptographic algorithms in secured communications are followed	ETSI M2M

8.9 Threat 9: Modification of Data Stored in the M2M Service Capabilities

8.9.1 Description

In this attack, stored Sensitive Data (but not cryptographic keys, attacks against which are treated elsewhere in the present document) is modified in an unauthorized manner. In one example, registration data in the M2M Core is modified, so that unauthorized D-type M2M Devices or M2M Gateways may be connected to the M2M Core, or the data is corrupted so that normal operation of the M2M Core may be prevented. Likewise, registration data stored in M2M Gateways relating to D'-type M2M Devices may be modified or corrupted. In another example, stored data in the SCs of D-type M2M Devices or in M2M Gateways may be modified or corrupted in order to cause false information to be reported to the M2M Core.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, M2M Service Provider, M2M Device/Gateway Manager, System Administrator.

8.9.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents (if the attack is against the M2M Core): Hacker, Disaffected employee (with admin access), commercial competitor, organised crime syndicate, extremist/hacktivist, nation state therefore score 4.
  - Their motivation: high motivation due to desire to disable a complete eco-system, therefore 4.

  - Their opportunity: may have physical access and/or electronic proximity and can attack the whole eco-system. Therefore score 4.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 4.

- Maximum score above is 4 therefore the likelihood of a successful attack: 4 (severe likelihood if no countermeasures are in place).
- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: without suitable counter-measures, it would be difficult or impossible to detect the attack.
  - Recoverability: difficult. It may be necessary to re-provision the whole eco-system with new keys.
- Seriousness of Threat at M2M Service Layer: . 4 "National" National Infrastructure - Severe damage to systems/processes that support important infrastructure requirements.
- Risk (i.e. priority) = seriousness x likelihood = 16 (high-point of "critical risk").
- Is mitigation required?: yes. Counter measures are required to minimize this risk, with a high priority.

8.9.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.9.3.1 Potential Counter-Measures

CM8 as above.

CM16: stored Sensitive data is integrity-protected, such that unauthorised modification can be detected.

Advantages:

- Resists the attack.

Disadvantages:

- Crypto overheads.

CM17: if the integrity-verification of stored data uses cryptographic keys (other than public keys), those keys are stored and used in a Secured Environment or Trusted Environment, according to where the measurement and verification processes take place.

Advantages:

- Resists the attack.

Disadvantages:

- Increases the cost and complexity of the Secured Environment or Trusted Environment, which may or may not be significant.

CM18: the integrity-verification of stored Sensitive Data takes place in a Secured Environment or a Trusted Environment.

Advantages:

- Resists the attack.

Disadvantages:

- Increases the cost and complexity of the Secured Environment or Trusted Environment, which may or may not be significant.
- Difficult to test.
- May require product certification.

8.9.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	M2M Service Provider's Domain, Gateway, D-type Devices	ETSI M2M, specifying existing techniques
CM16	M2M Service Provider's Domain, Gateway, D-type Devices	ETSI M2M, specifying existing techniques
CM17	M2M Service Provider's Domain, Gateway, D-type Devices	ETSI M2M but importing requirements from existing specifications, e.g. OMTP where possible
CM18	M2M Service Provider's Domain, Gateway, D-type Devices	ETSI M2M but importing requirements from existing specifications, e.g. OMTP where possible

8.10 Threat 10: Provisioning of non-Legitimate Keys

8.10.1 Description

A provisioning server is impersonated, thereby generating and provisioning usable but non-legitimate root keys and service keys to M2M Devices, and (where applicable) M2M Gateways and the M2M Core.

NOTE: These keys are defined in [i.6]. This attack could also be used to provision non-usable keys in order to deny service to a wide population of Devices and Gateways and Cores.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined, depending on how D'-type Devices use keys).

Stakeholders affected: Consumer of M2M Services, M2M Service Provider, M2M Device/Gateway Manager.

8.10.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: organised crime syndicate, hacktivist, nation state, therefore 4.
  - Their motivation: important objective for attacker but limited due to high possibility of detection, therefore "substantial" = 3.
  - Their opportunity: Devices/Gateways addressable over IP networks. Cores will be behind properly configured firewalls. Therefore "substantial" = 3.
  - Their capability: assume knowledge of protocols, therefore "high" = 4 for an unprotected system.

- Maximum score above is 4, i.e. "severe likelihood". Threat Agent with High motivation, high opportunity and capability.
- Impact assumptions:
  - Effect on stakeholders(s): major, if viruses are introduced to the Core via unprotected Devices/Gateways, as described at the ETSI workshop in January 2011. Applications are unable to rely on the SCL software and therefore cannot deliver their payloads.
  - Detect-ability: difficult if there are no counter-measures for detecting unauthorised software.
  - Recoverability: increased by segregation containment, mechanisms for proof of system integrity. Decreased by lack of audit of software configuration, damaging effects of loss of confidentiality or privacy of customer data.
- Seriousness of Threat at M2M Service Layer: 4 (National Infrastructure).

NOTE 1: This could be 3 "Enterprise" depending on the use case.

- Risk (i.e. priority) = seriousness x likelihood = 16 (high end of critical risk).

NOTE 2: This could be 12, mid-point of "critical risk", depending on the use case.

- Is mitigation required? Yes, counter measures are required to minimize this risk, with a high priority.

8.10.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.10.3.1 Potential Counter-Measures

CM9,10, 11, as above.

8.10.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM9, 10, 11	M2M Service Provider's Domain, M2M D-type Devices, M2M Gateways	ETSI M2M, specifying existing solutions

8.11 Threat 11: Unauthorised or Corrupted Application and Service-Layer Software in M2M Devices/Gateways

8.11.1 Description

An attacker installs unauthorised M2M service-layer software or modifies authorised software functions in M2M Devices or M2M Gateways. This attack may be used to:

- commit fraud, e.g. by the incorrect reporting of energy consumption;
- cause a breach of privacy by obtaining and reporting confidential information to the attacker;

- cause the disclosure of sensitive data such as cryptographic keys or other credentials which are stored or managed by the SC software;
- prevent operation of the affected M2M Devices/Gateways.

The attack may be perpetrated locally or by illicit use of remote management functions.

References of M2M use cases for which the analysis applies: All except Connected Consumer.

References of M2M use cases for which the analysis does not apply: Connected Consumer.

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Applications Developer, Consumer of M2M Services, Manufacturer of M2M Devices and/or M2M Gateways, M2M Device/Gateway Manager.

8.11.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Criminal, Hacker, Disaffected employee, extremist/hacktivist, (e.g. to disable the energy usage of a major public facility), therefore = 3.
  - Their motivation: mischief, financial (extortion) or political therefore "substantial" = 3.
  - Their opportunity: requires known architecture and protocols and can sustain the attack but on only one Device/Gateway at a time. Therefore limited opportunity = 2.
  - Their capability: disaffected employee may have knowledge/ expertise, access to training manuals and procedures. May have significant technical and financial backing, therefore substantial capability = 3.
- Maximum score above is 3 "substantial likelihood".
- Impact assumptions:
  - Effect on stakeholders(s): major, if viruses are introduced to the Core via unprotected Devices/Gateways, as described at the ETSI workshop in January 2011. Applications are unable to rely on the SCL software and therefore cannot deliver their payloads.
  - Detect-ability: difficult if there are no counter-measures for detecting unauthorised software.
- Recoverability: increased by segregation containment, mechanisms for proof of system integrity. Decreased by lack of audit of software configuration, damaging effects of loss of confidentiality or privacy of customer data.
- Seriousness of Threat at M2M Service Layer: 4 "national infrastructure" could be damaged if widely-deployed Devices or Gateways are vulnerable to viruses.
- Risk (i.e. priority) = seriousness x likelihood = 12 at the mid-point of "critical risk".
- Is mitigation required? yes, counter measures are required to minimize this risk, with a high priority.

8.11.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.11.3.1 Potential Counter-Measures

CM19: The integrity of executable functions in M2M Devices/Gateways can be verified.

Advantages:

- Detects the attack.

Disadvantages:

- Increases the cost and complexity of the M2M Device/Gateway, which may or may not be significant.

CM20: Policy-based action can be taken to prevent the use of functions or of M2M Devices/Gateways which fail the integrity verification test.

Advantages:

- Prevents corrupted or unauthorised functions from being used.
- Resists the attack, without necessarily having to disable the whole M2M Device/Gateway.
- Allows the possibility of remote remediation of faults by download of new or patched functionality.

Disadvantages:

- Increases the cost and complexity of the M2M Device/Gateway, and possibly the M2M Core, which may or may not be significant.
- Policy decisions made in the M2M Core may require a standardised abstraction of Device/Gateway functionality.

8.11.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM19	M2M D-type Devices, M2M Gateways	ETSI M2M
CM20	M2M D-type Devices, M2M Gateways	ETSI M2M

8.12 Threat 12: Subverting the M2M Device/Gateway Integrity-Checking Procedures

8.12.1 Description

This threat is a consequence of the optional integrity validation described in [i.5], [i.6] and [i.7] which is itself a counter-measure arising from threat 10, above. In fact, this attack may be perpetrated as a facilitator for the attack described in Threat 10. The attacker subverts the (optional) integrity-checking procedure, to:

- produce a good integrity result in an M2M Device/Gateway containing tampered or unauthorized M2M service-layer functionality;
- put an M2M Device/Gateway out of action by causing non-existent faults to be picked up by the integrity check of M2M service-layer functionality.

This attack may be perpetrated by modification of any RIVs stored in the M2M Device/Gateway, or by causing unauthorised new RIVs to be installed, or by corrupting the integrity-checking processes in the M2M Device/Gateway.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Consumer of M2M Services, Manufacturer of M2M Devices and/or M2M Gateways, M2M Device/Gateway Manager.

8.12.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Criminal, Hacker, Disaffected employee, extremist/hacktivist, therefore = 3.
  - Their motivation: mainly financial or political therefore "substantial" = 3.
  - Their opportunity: requires known architecture and protocols and can sustain the attack but only one Device/Gateway at a time. Therefore limited opportunity = 2.
  - Their capability: disaffected employee may have knowledge/ expertise, access to training manuals and procedures. Terrorists may have considerable expertise and financial backing, therefore limited capability = 3.
- Maximum score above is 3, "substantial likelihood".
- Impact assumptions:
  - Effect on stakeholders(s): minor localised inconvenience.
  - Detect-ability: without suitable counter-measures, it would be difficult or impossible to detect the attack before it has its effect.
  - Recoverability: decreased by: without counter-measures, faults in RIVs cannot be detected; the Integrity Validation process cannot detect faults in itself; RIVs could be replaced but the attack could re-occur.
- Seriousness of Threat at M2M Service Layer: : 4 "national infrastructure", i.e. same as threat 10, since a successful attack in the present threat enables an attack in threat 10 to be successful.
- Risk (i.e. priority) = seriousness x likelihood = 12 (mid-point of "critical risk").
- Is mitigation required? yes, counter measures are required to minimize this risk, with a high priority.

8.12.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.12.4 Potential Counter-Measures

CM16 above, applied to RIVs.

CM21: the measurement part of the Integrity Validation of executables takes place in a Trusted Environment [i.7] and the comparison with the RIVs takes place in a Secured Environment [i.7].

Advantages:

- Resists the attack.

- Many chipsets may already have this functionality built in.

Disadvantages:

- May increase the cost and complexity of the M2M Device/Gateway, but this may or may not be significant.

CM23: if the integrity-verification of executables uses cryptographic keys (other than public keys), those keys are stored and used in a Trusted or Secured Environment ,according to whether the keys are used in the measurement part or the comparison part of the Integrity Validation [i.7]. Advantages and disadvantages are the same as for CM17 above.

8.12.4.1 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM21, 23	M2M Gateway, M2M D-type Device	ETSI M2M, but existing specifications of other SDOs may be useful

8.13 Threat 13: Unauthorised or Corrupted Software in M2M Core

8.13.1 Description

An attacker installs unauthorised software or tampers with the software in the M2M Core. This attack may be used to :

- commit fraud;
- cause a breach of privacy;
- cause the disclosure of sensitive data such as cryptographic keys or other credentials;
- prevent operation of the affected functions.

The attack may be perpetrated locally or by illicit use of remote management functions.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, Manufacturer of M2M Core, M2M Service Provider, System Administrator.

8.13.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Hacker, Disaffected employee (with admin access), commercial competitor, organised crime syndicate, extremist/hacktivist, nation state therefore score 4.
  - Their motivation: high motivation due to desire to attack a complete eco-system, therefore 4.
  - Their opportunity: may have physical access and/or electronic proximity and can attack the whole eco-system. Therefore score 4.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 4.
- Maximum score above is 4 therefore the likelihood of a successful attack: 4 (severe likelihood if no countermeasures are in place).

- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: without suitable counter-measures, it would be difficult or impossible to detect the attack before it has its effect.
- Recoverability: not difficult but the attack may re-occur.
- Seriousness of Threat at M2M Service Layer: 4 National Infrastructure (an M2M core could be part of that NI).
- Risk (i.e. priority) = seriousness x likelihood = 16, high-point of "critical risk".
- Is mitigation required? yes, Counter measures are required to minimize this risk, with a high priority.

8.13.3 Mitigation of Risk

This risk should be:

- mitigated by ETSI M2M specifications: yes;
- transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no;
- avoided (e.g. by changes to specified functionality): no;
- accepted (where risk is small, or if it is out of scope for standardisation): no.

8.13.3.1 Potential Counter-Measures

CM19, CM20, as above but applied to the M2M Core.

8.13.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM19, CM20	M2M Service Provider's Domain	ETSI M2M

8.14 Threat 14: Subverting the Integrity-Checking Procedures in the M2M Core

8.14.1 Description

This threat is a consequence of the integrity-checking of executables in an M2M core, which is itself a counter-measure arising from threat 13, above. In fact, this attack may be perpetrated alongside the attack described in Threat 13. The attacker subverts the integrity-checking procedure, to:

- produce a good integrity result in an M2M Core containing tampered or unauthorized M2M service-layer functionality;
- put an M2M Core out of action by causing non-existent faults to be picked up by the integrity check of M2M service-layer functionality.

This attack may be perpetrated by modification of any RIVs stored in the M2M Core, or by causing unauthorised new RIVs to be installed, or by corrupting the integrity-checking processes in the M2M Core.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (no), D-type Device (no), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, Manufacturer of M2M Core, M2M Service Provider, System Administrator.

8.14.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: Hacker, Disaffected employee (with admin access), commercial competitor, organised crime syndicate, extremist/hacktivist, nation state therefore score 4.
  - Their motivation: high motivation due to desire to attack a complete eco-system, therefore 4.
  - Their opportunity: may have physical access and/or electronic proximity and can attack the whole eco-system. Therefore score 4.
  - Their capability: threat agents would have knowledge/ expertise, access to training manuals and procedures. reverse engineering ability and financial resources, therefore score 4.
  - Maximum score above is 4 therefore the likelihood of a successful attack: 4 (severe likelihood if no countermeasures are in place).
- Maximum score above is 4 "severe likelihood".
- Impact assumptions:
  - Effect on stakeholders(s): major inconvenience and loss of confidence.
  - Detect-ability: without suitable counter-measures, it would be difficult or impossible to detect the attack before it has its effect.
  - Recoverability: decreased by: without counter-measures, faults in RIVs cannot be detected; the Integrity Validation process cannot detect faults in itself; RIVs could be replaced but the attack could re-occur.
- Seriousness of Threat at M2M Service Layer: 4 National Infrastructure (an M2M core could be part of that NI).
- Risk (i.e. priority) = seriousness x likelihood = 16 (high-point of "critical risk").
- Is mitigation required? yes, counter measures are required, with a high priority.

8.14.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.14.3.1 Potential Counter-Measures

CM16 above, applied to RIVs.

CM22: The process of integrity-verification of executables in an M2M Core is protected against tampering.

Advantages:

- Resists the attack.

- Many chipsets may already have this functionality built in.

Disadvantages:

- May increase the cost and complexity of the M2M Core, but this may or may not be significant.

CM24: if the integrity-verification of executables in an M2M core uses cryptographic keys (other than public keys), those keys are protected against discovery and against modification by an unauthorised entity.

The advantages and disadvantages are the same as for CM22.

8.14.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM16, 22, 24	M2M Core	ETSI M2M, but existing specifications of other SDOs may be useful

8.15 Threat 15: General Eavesdropping on M2M Service-Layer Messaging Between Entities

8.15.1 Description

By eavesdropping on M2M service layer messages between components in the M2M Service Provider's Domain, M2M Devices and M2M Gateways, confidential or private information may be discovered. This excludes the use of eavesdropping to discover or infer the value of keys, which is covered elsewhere in the present document. The eavesdropping may physically occur in:

- a LAN which connects M2M Devices to an M2M Gateway;
- a WAN which connects M2M Gateways and M2M Devices to the M2M Core;
- a WAN which connects provisioning servers to M2M Devices, M2M Gateways and an M2M Core.

The attack may exploit lack of protection in communications, or vulnerabilities in protected communications, at any layer including the M2M service layer.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Consumer of M2M Services, M2M Device/Gateway Manager, M2M Service Provider, M2M (W)LAN Operator, Public Communications Network Operator.

8.15.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: individual criminal, hacker, commercial competitor, therefore 2.
  - Their motivation: mainly financial, therefore 2 (moderate motivation).
  - Their opportunity: can occur at concentration points e.g. Gateway or an M2M Core, and monitoring could be carried out over long periods of time. Monitoring would not be difficult. Therefore 4 (high opportunity).
  - Their capability: commercial competitor could be well equipped and knowledgeable, therefore 3 (substantial capability).

- Maximum score above is 4, i.e. severe likelihood.
- Impact assumptions:
  - Effect on stakeholders(s): significant effect upon the M2M Service Provider if the users find out about the loss of privacy and if it can be blamed on this attack.
  - Detect-ability: difficult or impossible to detect.
  - Recoverability: once confidentiality is lost, it's difficult to re-establish.
- Seriousness of Threat at M2M Service Layer: 2 "serious impact".
- Risk (i.e. priority) = seriousness x likelihood = 8 (high-point of "major risk").
- Is mitigation required? yes, counter measures are required to minimize this risk, with a high priority.

8.15.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.15.3.1 Required Counter-Measures

CM13

CM25: Communications between entities in the M2M system are protected by end-to-end security associations which provide end-to-end confidentiality.

8.15.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM13, CM25	M2M Service Provider's Domain, M2M D-type Devices, M2M Gateways	ETSI M2M but re-using existing specifications for secure communications

8.16 Threat 16: Alteration of M2M Service-Layer Messaging Between Entities

8.16.1 Description

By altering M2M service layer messages between components in the M2M Service Provider's Domain, M2M Devices and M2M Gateways, the attacker may deceive or defraud the M2M Service Provider or other stakeholders. The alteration of messages may physically occur in:

- a LAN which connects M2M Devices to an M2M Gateway;
- a WAN which connects M2M Gateways and M2M Devices to the M2M Core;
- a WAN which connects provisioning servers to M2M Devices, M2M Gateways and an M2M Core;
- communications between the M2M Core and M2M Applications in the Network and Applications Domain.

The attack may exploit lack of protection in communications, or vulnerabilities in protected communications, at any layer including the M2M service layer.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: consumer of M2M services, M2M Device/Gateway manager, M2M service provider, (W)LAN operator, Public Communications Network Operator, Systems Administrator.

8.16.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: individual criminals, commercial competitor, organised crime syndicates. Therefore = 3.
  - Their motivation: primarily financial = 2, moderate.
  - Their opportunity: real-time alteration could be difficult, due to infrequent data transfers, unless they communicate at regular, predictable intervals. Therefore = 2, limited.
  - Their capability: we can assume knowledge of communications protocols, if there are no counter-measures. Therefore = 3 substantial capability.

  Maximum score above is 3, substantial likelihood.

- Impact assumptions:
  - Effect on stakeholders(s): could be significant loss of revenue if it occurs between the Core and NAs or as a wide-scale attack against Devices or Gateway communications.
  - Detect-ability: not easy to detect before it occurs, or to prevent, if there are no counter-measures.
  - Recoverability: difficult or impossible to recover the original, authentic massages.
- Seriousness of Threat at M2M Service Layer: : 2 "serious impact". Possible effect upon revenue and customer confidence.

NOTE: The seriousness depends somewhat on the application. Perhaps it could be a "3" for some applications.

- Risk (i.e. priority) = seriousness x likelihood = 6 (mid-point of "major risk"). Note: perhaps it could be a "9" for some applications.
- Is mitigation required? yes) Counter measures are required to minimize this risk as soon as possible.

8.16.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes, since the M2M service layer cannot assume any level of protection provided by the access network or transport network.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): yes.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.16.3.1 Required Counter-Measures

CM9, CM10, CM13, CM25

8.16.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM9, 10	M2M Service Provider's Domain, Gateway, D-type Device. D'-type device is FFS	ETSI M2M specifying security associations from existing specifications (3GPP, OMA, etc)
CM13	M2M Service Provider's Domain, Gateway, D-type Device. D'-type device is FFS	ETSI M2M
CM25	M2M Service Provider's Domain, Gateway, D-type Device. D'-type device is FFS	ETSI M2M, but re-using existing specifications for secure communications

8.17 Threat 17: Replay of M2M Service-Layer Messaging Between Entities

8.17.1 Description

By repeating all or portions of previous M2M service layer messages between components in the M2M Service Provider's Domain, M2M Devices and M2M Gateways, the attacker may deceive or defraud the M2M Service Provider or other stakeholders. The repetition of messages may physically occur in:

- a LAN which connects M2M Devices to an M2M Gateway;
- a WAN which connects M2M Gateways and M2M Devices to the M2M Core;
- a WAN which connects provisioning servers to M2M Devices, M2M Gateways and an M2M Core;
- communications between the M2M Core and M2M Applications in the Network and Applications Domain.

The attack may exploit lack of protection in communications, or vulnerabilities in protected communications, at any layer including the M2M service layer.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (no).

Stakeholders affected: consumer of M2M services, M2M Device/Gateway manager, M2M service provider, (W)LAN operator, Public Communications Network Operator.

8.17.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: individual criminals, commercial competitor, organised crime syndicates. Therefore = 3.
  - Their motivation: primarily financial = 2, moderate.
  - Their opportunity: real-time replay could be difficult, due to infrequent data transfers, unless they communicate at regular, predictable intervals. Therefore = 2, limited.
  - Their capability: we can assume knowledge of communications protocols, if there are no counter-measures. Therefore = 3 substantial capability.

Maximum score above is 3, substantial likelihood.

- Impact assumptions:
  - Effect on stakeholders(s): could be significant loss of revenue (especially for smart metering) if it occurs between the Core and NAs or as a wide-scale attack against Devices or Gateway communications.
  - Detect-ability: not easy to detect before it occurs, or to prevent, if there are no counter-measures.
- Recoverability: difficult or impossible to recover the original, authentic massages.
- Seriousness of Threat at M2M Service Layer: 3 "Enterprise".
- Risk (i.e. priority) = seriousness x likelihood = 9: low-point of "critical risk".
- Is mitigation required? yes Counter measures are required to minimize this risk, with a high priority.

8.17.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred: no.
- Avoided: no.
- Accepted: no.

8.17.3.1 Potential Counter-Measures

CM26: The protocol includes functionality to detect if all or part of a message is an unauthorised repeat of an earlier message or part of a message.

Advantages:

- Provides mitigation of threat e.g. repetition of an earlier meter reading.
- A well-established counter-measure.

Disadvantages:

- Communications and processing overhead.

8.17.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM26	M2M Service Provider's Domain, Gateway, D-type Device	ETSI M2M

8.18 Threat 18: Breach of Privacy due to Inter-Application Communications

8.18.1 Description

An M2M application in an M2M Device, in an M2M Gateway, or in the NAD, obtains sensitive information (other than key material) from another M2M application, by inter-application communications via the Service Capabilities, in a way which breaches privacy policies or regulations. This threat covers a number of possible cases, as follows:

- The applications are operated by different M2M Service Providers. The Service Provider of the donor application would not knowingly permit release of the information to the Service Provider of the receiving application.

- The applications are operated by the same M2M Service Provider, who is not permitted to share information between applications. In a vulnerable system, leakage of information may be due to inappropriate safeguards or malicious intent.
- The applications may reside in the same entity or they may be in any two entities (e.g. M2M Devices) which can communicate with each other at the application layer via SCs in the M2M Devices or in an M2M Core or in an M2M Gateway.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Applications Developer, Consumer of M2M Services, M2M Service Provider, Manufacturer of M2M Devices and/or M2M Gateways, Manufacturer of M2M Core.

8.18.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: hacker, commercial competitor, hacktivist, therefore 3.
  - Their motivation: to get information about competitors' customers or applications; moderate motivation = 2.
  - Their opportunity: the receiving application can be loaded using official software download processes, hence = 4, high opportunity.
  - Their capability: their knowledge of competitors' applications may be limited, hence = 2.

  Maximum score above is 4, severe likelihood.
- Impact assumptions:
  - Effect on stakeholders(s): could have a legal/regulatory impact on an M2M service provider.
  - Detect-ability: low if there are no counter-measures, since the system will not recognise it as an attack.
  - Recoverability: difficult to re-establish the trust of users and regulators.
- Seriousness of Threat at M2M Service Layer: 2: "serious impact". Impact (if successful) would have possible repercussions for revenue, penalty payments, market share and customer confidence.
- Risk (i.e. priority) = seriousness x likelihood = 8: at the high end of "major risk".
- Is mitigation required? yes Counter measures are required to minimize this risk as soon as possible.

8.18.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: yes.
- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no.
- Avoided (e.g. by changes to specified functionality): no.
- Accepted (where risk is small, or if it is out of scope for standardisation): no.

8.18.4 Potential Counter-Measures

CM27: a framework is used by the SCL which provides methods for securely:

- assigning attributes to the resource container regarding an M2M Application's access rights;
- managing those attributes;
- enforcing the access rights.

Advantages:

- Provides mitigation of the threat.
- Increases confidence in the ability of stakeholders to maintain the privacy of customer or competitor information.
- Allows inter-application communications under controlled conditions.

Disadvantages:

- Adds cost and complexity to entities in which it is implemented.

8.18.5 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM27	M2M Service Provider's Domain, Gateway, D-type Device. D'-type Devices are FFS	ETSI M2M. Global Platform specifications may be a useful source of normative material which can be referenced

8.19 Threat 19: Breach of Privacy due to Attacks on M2M Device/Gateway Service Capabilities

8.19.1 Description

An M2M Device or a M2M Gateway may store or may have access to Sensitive Data relating to a stakeholder (e.g. a consumer or an M2M Service Provider), which it obtains from one or more M2M Applications. An attacker subsequently obtains the data by unauthorised access to that data via the Service Capability. This attack does not include the discovery of cryptographic keys, which is covered elsewhere in the present document.

No inter-application communication is assumed or required in this attack, although the attacker may communicate the obtained Sensitive Data to another application that uses the same Service Capability.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets of the attack: M2M Service Provider's Domain: (no), Gateway (yes), D-type Device (yes), D'-type Device (no).

Stakeholders affected: Consumer of M2M Services, Manufacturer of M2M Devices and Gateways, M2M Service Provider, System Administrator.

8.19.2 Assessment of Risk

- Likelihood assumptions:
  - Threat agents: hacker, disaffected employee, commercial competitor, therefore = 2.
  - Their motivation: to get information about competitors' customers or applications; moderate motivation = 2.

- Their opportunity: remote interrogation or local presence, hence = 4, high opportunity.
- Their capability: their knowledge of competitors will have good knowledge of protocols and sustained presence is not necessary, hence = 4.

Maximum score above is 4, severe likelihood.

- Impact assumptions
  - Effect on stakeholders(s): could have a legal/regulatory impact on an M2M service provider.
  - Detect-ability: low if there are no counter-measures, since the system will not recognise it as an attack.
- Recoverability: difficult to re-establish the trust of users and regulators.
- Seriousness of Threat at M2M Service Layer: 2: "serious impact". Impact would be noticeable to parties other than the stakeholder. Possible repercussions for revenue, penalty payments, market share and customer confidence.
- Risk (i.e. priority) = seriousness x likelihood = 8: high end of "major risk".
- Is mitigation required? yes. Counter measures are required to minimize this risk as soon as possible.

8.19.3 Mitigation of Risk

This risk should be:

- mitigated by ETSI M2M specifications: yes;
- transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): no;
- avoided (e.g. by changes to specified functionality): no;
- accepted (where risk is small, or if it is out of scope for standardisation): no.

8.19.3.1 Potential Counter-Measures

CM8.

8.19.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM8	Gateway, D-type Device	ETSI M2M, specifying existing techniques

9 Type 2 Threats Affecting the M2M Functional Requirements

9.1 Threat 20: Discovery of M2M long-term service-layer keys from knowledge of access-network keys

9.1.1 Description

This threat pertains to the case in which M2M long-term service-layer keys are derived from or bootstrapped from Access Network keys. An attacker gains unauthorised knowledge of the AN keys and is able to generate from them a viable set of M2M service-layer keys. The M2M keys thereby produced may be used to make a significant quantity of cloned Devices/Gateways.

There are several ways in which this attack may affect M2M stakeholders:

1) The cloned Devices/Gateways may be used to consume non-M2M network services which may be charged to an M2M stakeholder.

2) The cloned Devices/Gateways may consume M2M services which may be charged to an M2M stakeholder.

3) The cloned Devices/Gateways may operate fraudulent processes and may be used to replace legitimate Devices/Gateways.

NOTE: It is assumed that an attacker cannot be prevented from gaining knowledge of the processes used to derive the M2M keys from the AN keys.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets affected: M2M Service Provider's domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (no).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, ISE manufacturer, M2M Device/Gateway Manufacturer, M2M Device/Gateway Manager, Public Communications Network Operator.

9.1.2 Assessment of Risk

- Likelihood assumptions:

  1) Threat agents: Criminal, Hacker, Disaffected employee, Commercial Competitor, therefore 2.

  2) Their motivation: Commercial competitor may be inhibited by risk of detection and damage to reputation. Other threat agents may be motivated by the ability to clone large numbers of Devices/Gateways. therefore = 3.

  3) Their opportunity: requires physical access and electronic proximity, known architecture and protocols but can produce a widespread attack. Therefore limited opportunity = 2.

  4) Their capability: some threat agents may have knowledge/ expertise, access to training manuals and procedures. Financial resources do not need to be great. Therefore substantial capability = 3.

Maximum score in 1) to 4) above is 3 therefore the likelihood of a successful attack: 3 (substantial on an unprotected Device/Gateway - depends on level of protection in Device/Gateway implementation).

- Impact assumptions:

  - Effect on stakeholders(s): minor financial loss may be significant if the cloned Devices/Gateways are used to consume the resources of a third party who has to be paid. Loss of reputation could be high, since this type of attack is likely to attract the attention of the mass media and industry critics.

- Detect-ability: increased by need for physical proximity to mount attack but decreased as sustained presence by attacker not required. Cloning can make it difficult for fraud management systems to be effective.
- Recoverability: increased as all cloned Devices/Gateways can be blocked at the network. Increased as only one legitimate Device/Gateway has to be permanently blocked. Decreased as the attack may be repeated, which may require large numbers of Devices/Gateways to be replaced with ones which support counter-measures.

- Seriousness of Threat: 2 = serious impact.
- Risk (i.e. priority) = seriousness x skill/likelihood = 6, mid-point of "major risk". Counter measures are required to minimize this risk as soon as possible. Is mitigation required?: yes.

9.1.3 Mitigation of Risk

This risk should be:

- mitigated by ETSI M2M specifications: no;
- transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): yes;
- avoided (e.g. by changes to specified functionality): no;
- accepted (where risk is small, or if it is out of scope for standardisation): no.

9.1.3.1 Potential Counter-Measures

CM2: Access Network credentials from which M2M long-term service keys are derived or bootstrapped are stored in a Secured Environment which renders it infeasible for the attacker to discover the value of the credentials.

Advantages:

- Provides mitigation of the threat, e.g. protects the reputation of M2M stakeholders and avoids financial loss.

Disadvantages:

- Adds cost and complexity to Devices/Gateways. This does not apply to those Devices/Gateways which use the AN credentials for access to networks which mandate the use of UICC and secure channel, or which provide an equivalent level of protection for the AN credentials.

CM5: The derivation or bootstrapping of M2M long-term service keys from Access Network credentials never causes the former or the latter to be exposed outside of a Secured Environment.

Advantages:

- Provides mitigation of the threat, e.g. protects the reputation of M2M stakeholders and avoids financial loss.

Disadvantages:

- Adds cost and complexity to Devices/Gateways, which may or may not be significant.

CM29: Fraud management systems are deployed in the M2M Service Provider's Domain, which detect the use of duplicated M2M service keys and take appropriate action.

Advantages:

- Provides mitigation of the threat, e.g. protects the reputation of M2M stakeholders and avoids financial loss.

Disadvantages:

- Adds cost and complexity in the networks and Core. However, this CM should be regarded as an essential requirement for any large-scale commercial operation.

9.1.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM 2, 5	M2M Service Provider's domain, Gateway, D-type Device	Another SDO involved in the specification of Devices/Gateways. May require liaison with ETSI M2M
CM29	M2M Service Provider's domain, Gateway, D-type Device	May require liaison with other SDOs

9.2 Threat 21: Transfer of Module Containing Access-Network keys and/or M2M long-term keys to a different terminal/Device/Gateway

9.2.1 Description

An attacker gains unauthorised possession of a set of viable keys and credentials by removal, from a legitimate M2M Device/Gateway, of the ISE containing them. The attacker then use the ISE in a different and unauthorised telecoms terminal or M2M Device/Gateway, for fraudulent purposes.

There are several ways in which this attack may affect M2M stakeholders:

1) A telecoms terminal may use the ISE to attach to an AN and then consume non-M2M network services which may be charged to the legitimate M2M stakeholder.

2) The ISE may be used in an M2M Device/Gateway to consume M2M services which may be charged to the legitimate M2M stakeholder.

3) The M2M Devices/Gateway in which the ISE is used may operate fraudulent processes and may be used to replace a legitimate Devices/Gateways.

4) The original M2M Device/Gateway is rendered inoperable and it may be a costly exercise to re-instate it.

References of M2M use cases for which the analysis applies: All.

References of M2M use cases for which the analysis does not apply: None.

Targets affected: M2M Service Provider's domain: (yes), Gateway (yes), D-type Device (yes), D'-type Device (undetermined).

Stakeholders affected: Consumer of M2M services, M2M Service Provider, ISE manufacturer, M2M Device/Gateway Manufacturer, M2M Device/Gateway Manager, Public Communications Network Operator.

9.2.2 Assessment of Risk

NOTE: It is assumed that the AN keys are unique for every Device/Gateway.

- Likelihood assumptions:

  1) Threat agents: Criminal, Hacker, Disaffected employee, Organised crime syndicate, therefore 3.

  2) Their motivation: Organised criminals could attack many Devices/Gateway,, therefore = 3.

  3) Their opportunity: requires physical access and some product knowledge. Therefore limited opportunity = 2.

  4) Their capability: not much technical knowledge required, therefore substantial capability = 3.

Maximum score in 1 to 4 above is 3 therefore the likelihood of a successful attack: 3 (substantial on an unprotected Device/Gateway).

- Impact assumptions:

    1) Effect on stakeholders(s): significant amount of financial loss. Significant loss of reputation if attack is widely reported (as was a similar attack in South Africa).

    2) Detect-ability: decreased, as sustained presence by attacker not required and M2M Core may not know why the Device/Gateway is not working and fraud management systems may not be configured to detect the misuse of the keys/credentials.

    3) Recoverability: high cost if this is wide-spread.

- Seriousness of Threat: 2 = serious impact.

- Risk (i.e. priority) = seriousness x skill/likelihood = 6, mid-point of "major risk". Counter measures are required to minimize this risk as soon as possible.

9.2.3 Mitigation of Risk

This risk should be:

- Mitigated by ETSI M2M specifications: no.

- Transferred (e.g. for mitigation by another SDO - either in existing specs or by asking them to add new functionality): yes.

- Avoided (e.g. by changes to specified functionality): no.

- Accepted (where risk is small, or if it is out of scope for standardisation): no.

9.2.3.1 Potential Counter-Measures

CM6, CM29, as described previously.

C7: The Secured Environment containing the AN keys is physically and/or logically bound to the specific M2M Device or M2M Gateway for which it is intended.

Advantages:

- Provides mitigation of the threat, e.g. protects the reputation of M2M stakeholders and avoids financial loss.

Disadvantages:

- Adds cost and complexity to Devices/Gateways, unless this CM is already implemented because of specifications for the AN security.

CM28: Means exist in the Access Network and/or M2M Core to prevent AN credentials from being used for purposes other than for connection of a Device/Gateway to its intended M2M service layer.

Advantages:

- Provides mitigation of the threat, e.g. protects the reputation of M2M stakeholders and avoids financial loss.

Disadvantages:

- Adds cost and complexity in the networks and Core. However, this CM should be regarded as an essential requirement for any large-scale commercial operation.

9.2.3.2 Responsibility for Counter-Measures

Counter-Measure	Target	Responsibility
CM 6	M2M Service Provider's domain, Gateway, D-type Device	May require liaison with SDOs involved in the specification of Devices/Gateways
CM7	M2M Service Provider's domain, Gateway, D-type Device	May require liaison with SDOs involved in the specification of Devices/Gateways
CM28	M2M Service Provider's domain, Gateway, D-type Device	May require liaison with SDOs
CM29	M2M Service Provider's domain, Gateway, D-type Device	May require liaison with SDOs

10 Actions Recommended for ETSI TC M2M

10.1 Assurance of Counter-Measures

Table 1 provides the total list of counter-measures and the end-responsibility for each counter-measure.

Table 1

CM#	Associated Threats	Highest Associated Risk level	Description	End Responsibility for Mitigation
CM1	1, 4, 6	12 (in the middle of the "critical risk" category)	M2M long-term service keys (other than public keys) are stored in a Secured Environment [i.7] (whose tamper-resistance may be certified) which renders it infeasible for the attacker to discover the value of keys by logical or physical means	ETSI M2M. Material from OMTP specifications may be useful
CM2	20	6 (in the middle of the "major risk" category	Access Network credentials from which M2M long-term service keys are derived or bootstrapped are stored in a Secured Environment which renders it infeasible for the attacker to discover the value of the credentials	Another SDO involved in the specification of Devices/Gateways. May require liaison with ETSI M2M
CM3	1, 4, 6	12 (in the middle of the "critical risk" category)	The Secured Environment will not reveal the value of stored keys, even to a management system or to an authorised representative of the M2M Core Operator, such as a System Administrator	ETSI M2M. Material from OMTP, TCG, ETSI SCP specifications may be useful
CM4	1, 4, 6	12 (in the middle of the "critical risk" category)	the execution of Sensitive Functions (e.g. the derivation of further keys from long-term M2M service-layer keys) never causes long-term service keys to be exposed outside of the Secured Environments in which they are stored	ETSI M2M. Material from OMTP, TCG, ETSI SCP specifications may be useful
CM5	20	6 (in the middle of the "major risk") category	The derivation or bootstrapping of M2M long-term service keys from Access Network credentials never causes the former or the latter to be exposed outside of the Secured Environments in which they are stored, or in which the derivation or bootstrapping processes take place	Another SDO involved in the specification of Devices/Gateways. May require liaison with ETSI M2M
CM6	1, 4, 6, 21	12 (in the middle of the "critical risk" category)	The Secured Environment containing the M2M long-term service keys is bound to the M2M Device or M2M Gateway, using logical and/or physical means	If it is an ISE such as UICC, then the SDO which standardises the ISE (e.g. ETSI SCP for UICC and 3GPP for logical binding), otherwise ETSI M2M

CM#	Associated Threats	Highest Associated Risk level	Description	End Responsibility for Mitigation
CM7	21	6 (mid-point of Major Risk"	The Secured Environment containing the AN keys is bound to the specific M2M Device or M2M Gateway, using physical and/or logical means	If it is an ISE such as UICC, then the SDO which standardises the ISE (e.g. ETSI SCP for UICC and 3GPP for logical binding), Otherwise ETSI M2M
CM8	2, 3, 5, 7, 9, 19	16 (high-point of "critical risk").	Access to and/or the modification of stored Sensitive Data requires strong (i.e. cryptographic) authentication of the accessing/modifying party, followed by authorisation	ETSI M2M, specifying existing techniques
CM9	8, 10, 16	16 (at the high end of "critical risk"). It could be a 9 (low end of critical risk) for some use cases.	A security association is established between the communicating entities, which provides for mutual authentication and confidentiality	ETSI M2M specifying security associations from existing specifications (3GPP, OMA, etc)
CM10	8, 10	16 (at the high end of "critical risk")	The security association between communicating entities uses protocols which are proven to resist man-in-the-middle attacks	
CM11	8, 10	16 (at the high end of "critical risk"). It could be a 9 (low end of critical risk) for some use cases.	M2M service-layer keys in a provisioning message are encrypted for confidentiality, independently of any confidentiality provided by the messaging protocol	ETSI M2M but importing requirements from existing specifications (3GPP, OMA, etc)
CM12	8	16 (at the low end of "critical risk"). It could be a 9 (low end of critical risk) for some use cases.	during provisioning of M2M service-layer keys, the protocol end-points for the encryption/decryption of those M2M service keys are Secured Environments	ETSI M2M but importing requirements from existing specifications, e.g. OMTP, ETSI SCP, where possible
CM13	8, 15, 16	9 (at the low end of "critical risk")	communications whose security is anchored in M2M service-layer keys use session keys, i.e. keys with a limited lifetime which can be set by security policy. Session keys can be derived from M2M service-layer keys	ETSI M2M
CM14	8	9 (low end of critical risk	secured communications use only those cryptographic algorithms which are assessed as being fit for purpose, e.g. the length and randomness of cryptographic parameters is sufficient to resist a brute-force attack	ETSI M2M

CM#	Associated Threats	Highest Associated Risk level	Description	End Responsibility for Mitigation
CM15	8	9 (low end of critical risk)	industry-accepted recommendations for the use of cryptographic algorithms in secured communications are followed	ETSI M2M
CM16	9, 12, 14	16 (high-point of "critical risk").	stored Sensitive Data is integrity-protected, such that unauthorised modification can be detected	ETSI M2M, specifying existing techniques
CM17	9	16 (high-point of "critical risk").	if the integrity-verification of stored data uses cryptographic keys (other than public keys), those keys are stored and used in a Secured Environment or Trusted Environment, according to where the measurement and verification processes take place	ETSI M2M but importing requirements from existing specifications, e.g. OMTP where possible
CM18	9	16 (high-point of "critical risk").	the integrity-verification of stored Sensitive Data takes place in a Secured Environment or a Trusted Environment	ETSI M2M but importing requirements from existing specifications, e.g. OMTP where possible
CM19	11, 13	16 (high end of "critical risk")	The integrity of executable functions can be verified	ETSI M2M
CM20	11, 13	16 (high end of "critical risk")	Policy-based action can be taken to prevent the use of functions which fail the integrity verification test	ETSI M2M
CM21	12	12 (mid-point of "critical risk")	the measurement part of Integrity Validation of executables takes place in a Trusted Environment and the comparison with the RIVs takes place in a Secured Environment	ETSI M2M
CM22	12	16 (high end of critical risk)	The process of integrity-verification of executables in an M2M Core is protected against tampering	ETSI M2M, but existing specifications of other SDOs may be useful
CM23	12	12 (mid-point of "critical risk")	if the integrity-verification of executables uses cryptographic keys (other than public keys), those keys are stored and used in a Trusted Environment or Secured Environment, according to whether the keys are used in the measurement part or the comparison part of the Integrity Validation	ETSI M2M
CM24	14	16 (high end of "critical risk"	if the integrity-verification of executables uses cryptographic keys (other than public keys), those keys are protected against discovery and against modification by an unauthorised entity	

CM#	Associated Threats	Highest Associated Risk level	Description	End Responsibility for Mitigation
CM25	15, 16	8 (high-point of "major risk")	Communications between entities in the M2M system are protected by security associations which provide end-to-end confidentiality	ETSI M2M but re-using existing specifications for secure communications
CM26	17	9 (low-point of "critical risk")	The protocol includes functionality to detect if all or part of a message is an unauthorised repeat of an earlier message or part of a message	ETSI M2M but re-using existing specifications for secure communications
CM27	18	8 (high end of "major risk")	A framework is used by the SCL which provides methods for securely: assigning attributes to the resource container regarding an M2M Application's access rights; managing those attributes; enforcing the access rights	ETSI M2M. Global Platform specifications may be a useful source of normative material which can be referenced
CM28	21	6 (mid-point of "major risk"	Means exist in the Access Network and/or M2M Core to prevent AN credentials from being used for purposes other than for connection of a Device/Gateway to its intended M2M service layer	Another SDO
CM29	20, 21	6 (mid-point of "major risk"	Fraud management systems are deployed in the M2M Service Provider's Domain, which detect the use of duplicated M2M service keys and take appropriate action	Another SDO

10.2 Recommended Mapping of Counter-Measures onto Architectural Features

In this clause, the proposed counter-measures are mapped onto architectural features. The first table addresses features which were regarded as priorities for Release 1 at the time of writing. The other tables address other architectural features. It was not possible to define in the present document which CMs would be implemented in Release 1. Such decisions depend on contributions submitted to ETSI M2M meetings. However, the risk-assessment score for each CM gives a guide as to the priority for incorporating the CMs in the M2M Release 1 specifications (see notes on interpretation below). In some cases, it is stated explicitly that CMs are not a priority for Release 1. Also, some counter-measures are described as "must-do" items.

Notes on interpretation:

1) How to interpret a CM: the format is CMx-y:

   - x = the reference number of the CM in the present document.
   - y = the risk-assessment score assigned to the CM in the appropriate context of each architectural feature. So, y gives an idea of the importance of taking account of the CM in ETSI M2M specifications:
     - Y = 9, 12, 16 "critical risk". Counter measures are required to minimize this risk, with a high priority.
     - Y = 4, 6, 8 "major risk". Counter measures are required to minimize this risk as soon as possible.
     - Y = 1, 2, 3 "minor risk". No primary need for counter measures.

- Y = 5, 7, 10, 11, 13, 14 are not possible in this scheme.

2) In the tables below, the r/h column, headed "Release" is empty. This is because it was not possible to define in the present document which CMs would be implemented in Release 1, as explained above.

3) Yellow highlights denote items where clarification of the requirement was still required at the time of writing.

4) Counter-measures 28 and 29 do not appear in the following tables. That is not an error.

Table 2

Functionality Numbering	Functionality	Description		Priority	Release
1) Threat Analysis, TR 103 167 Prioritization: Identify which threats are recommended to be addressed in Release 1					
	Sensitive data	Access and/or modification of stored sensitive data		CM08-16 CM18-16	
	Malware in the core	Preventing/detecting/handling of malware		CM16-16 CM19-16 CM20-16 CM22-16 CM24-16	
	Deletion of Keys	Deletion of keys in the core		CM8-16	
	Device/Gateway integrity checking	Device/Gateway Integrity Checking	NSCL can request verification of G/D integrity	-	
			NA can initiate a request of verification of G/D integrity through NSCL	-	
			Remediation procedures due to integrity checking	CM16-12 CM19-12 CM20-12 CM21-12 CM23-12	
	Integrity and replay Protection of messages			CM26-09	
	TBD	Other items not listed below			

Table 3

Functionality Numbering	Functionality	Description		Priority	Release
2) Bootstrapping/Provisioning: Provisioning of M2M service-layer security credentials relating to D' & D Devices, Gateways, and Applications (DA, D'A, GA, & NA)					
	Bootstrapping security credentials	Bootstrapping of M2M service-layer security credentials:	Relating to Devices (DSCL & GSCL) and Network (*we added the green highlighted text*)	CM02-06 CM05-06 CM08-16 CM09-16 CM10-16 CM11-16 CM12-12 CM13-12 CM14-12 CM15-12	
			relating to Applications (DA,, GA, & NA)	Out of scope for Release 1	
	Selection/Negotiation of Bootstrapping	Procedures on how to select/negotiate the bootstrapping method: Where options exist and where negotiation is applicable		See Provisioning security credentials	
	Protocols/Algorithms	Authentication protocols & algorithms For secure provisioning,		MUST DO CM14-9, CM15-9,	
	D' Device handling	Bootstrapping/provisioning (in scope or out of scope) Provisioning of security credentials Selection/Negotiation Protocols/Algorithms		Did not feature in our analysis. We feel that it is not a priority for Release 1	2

Table 4

Functionality Numbering	Functionality	Description			Priority	Release
3) Authentication & Authorization: Establishment of security association of communications between applications and SCLs (dla & mla interfaces) and between local and remote SCLs (mld interface) that allow authentication to be performed						
	Protocols	Authentication & Authorization protocols	For Device/Gateway (SCL) registration		Maximum	
			For application (D'A, DA, GA, & NA) registration	Threat 9 - Risk: 16	CM08-16 CM16-16 CM17-16 CM18-16	
				Threat 18 - Risk: 08	CM08-08	
	Algorithms	Authentication & Authorization Algorithms	Negotiation (from a suite of permissible algorithms) as part of the setup of security associations		MUST DO STAGE 3	
			Acceptable usage (e.g. key lengths, etc.)		MUST DO STAGE 3 CM14-09	
			Independent or shared algorithms (e.g. for secure provisioning, for Device registration, for application registration)		MUST DO STAGE 3	
	D' Device handling	D'A Authentication & Authorization (in scope or out of scope) Protocols Algorithms			May depend on architecture. Could be application layer - out of scope.	

Table 5

Functionality Numbering	Functionality	Description			Priority	Release
4) Privacy: Establishment of security association of communications between applications and SCLs (dIa & mIa interfaces) and between local and remote SCLs (mId interface) that allow data confidentiality to be preserved						
	Key Management & Hierarchy (mId only)	Device /Gateway key management			Maximum - Stage 2 is done	
		Relationship with application keys & session connection			Maximum - Stage 2 is done	
		Network Application key management			out of scope for Release 1	
		Relationship with session connection (always connected?)				
		Revoking keys			Maximum (to do). Ka/Ks done. Kr to do?	
		Key storage (root, session, & application)			Maximum. Stage 2 is done - may need clarification. CM01-12 CM02-06 CM03-12 CM04-12 CM05-06 CM06-12 CM07-06	
	Confidentiality	Anonymity of sender/requester identity. *Anecdotal evidence indicates that anonymity is very important to the community. It needs to be supported*			Not in threat analysis. Maximum importance.	
		Negotiation of a secure session Enabling and disabling			CM09-16 OR 9 CM10-16 CM13-09 CM25-08	
		Secure messaging (data privacy)	Interfaces	mIa	Out of scope for Rel 1 CM27-08	
				dIa	Suspect out of scope for Rel 1 Only countermeasure CM27-08	
				mId	MUST DO	
			Secure tunnel sessions procedures		MUST DO for mId	
	Protocols & Algorithms	Protocols & Algorithms for privacy (secure communication)	Negotiation (from a suite of permissible algorithms) as part of the setup of security associations.		MUST DO for mId	
	Protocols & Algorithms	Protocols & Algorithms for privacy (secure communication)	Negotiation (from a suite of permissible algorithms) as part of the setup of security associations.		MUST DO for mId	

History

Document history		
V1.1.1	August 2011	Publication