TTC技術レポート
Technical Report

TR-M2M-0008v1.0.0

Analysis of security solutions for the oneM2M system

2014 年 11 月 10 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

TR-M2M-0008v1.0.0

Analysis of security solutions for the oneM2M system

＜参考＞ [Remarks]

１．国際勧告等の関連 [Relationship with international recommendations and standards]

本技術レポートは、oneM2M で作成された Technical Report 0008v1.0.0 に準拠している。

[This Technical Report is transposed based on the Technical Report 0008v1.0.0 developed by oneM2M.]

２．作成専門委員会 [Working Group]

oneM2M 専門委員会 [oneM2M Working Group]

ONEM2M TECHNICAL REPORT

Document Number	TR 0008
Document Name:	oneM2M-TR-0008-Security-V1.0.0
Date:	2014-April-10
Abstract:	The TR analyses security issues which may arise from use cases, captures relevant threats, maps them to the security requirements and derives possible security mechanisms to realize the security features for oneM2M Release1

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

Contents

1 Scope

The scope of the present document is to create a common understanding on security within oneM2M systems. To achieve that, security services are explained, threats analysed and security requirements within oneM2M identified and derived from use cases. In addition the present document discusses how security mechanisms relate to the oneM2M architecture. Suitable security procedures and mechanisms are defined within [i.14].

2 References

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

2.1 Normative references

None.

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] oneM2M drafting rules (draft)

[i.2] TR-0004 Definitions and Acronyms

[i.3] TS-0002 Requirements

[i.4] TS-0001 Functional Architecture (draft)

[i.5] TR-0001 Use Cases (draft)

[i.6] ISO/IEC 29115 Information technology- Security Techniques – Entity authentication assurance framework

[i.7] ETSI TS 102 221 V11.0.0 Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 11)

[i.8] ETSI TS 102 671 V9.1.0 Smart Cards; Machine to Machine UICC; Physical and logical characteristics (Release 9)

[i.9] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

[i.10] ETSI TS 133 220 "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[i.11] ANSI INCITS 359-2004 American National Standard for Information Technology–Role Based Access Control.

[i.12] NIST Interagency Report 7316 Assessment of Access Control Systems.

[i.13] DRAFT NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

[i.14] TS-0003 Security Solutions (draft)

[i.15] IETF RFC6749: The OAuth 2.0 Authorization Framework, October 2012

3 Definitions, symbols, abbreviations and acronyms

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [i.2] and the following apply:

End to End Security: Service provided by the M2M System to M2M Applications that establishes trusted security credentials to secure connections between applicative entities, independently of other parties involved.

Hardware Security Module (HSM): a separate and tamper resistant physical computing device, e.g. as defined in [i.7] and [i.8], able to perform security procedures related to oneM2M Service functions. The HSM is used within the M2M Device or M2M Gateway and is different from a Server-HSM used within a network infrastructure node / component.

Long-term service-layer key: key used for service-layer relevant security operations. The key is valid permanently or for a significant period of time, i.e. no temporarily derived key material.

Pseudonym: alias identity within the context of the Pseudonymity service defined in ISO/IEC 15408 [i.9]

Security Mechanism: process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system

Security Policy: set of rules and practices that specify or regulate how a system or organization provides security services to protect resources

Security Service: processing or communication capability that is provided by a system to give a specific kind of protection to resources where these resources may reside within the system or any other system

Sensitive Function: function which requires protection from unauthorized monitoring, tampering or execution that is operating on sensitive data / credentials or key material, e.g. derivation of keys from M2M long-term service-layer keys and cryptographic algorithms.

Server-HSM: dedicated computing device, able to perform security procedures related to oneM2M service functions and integrated within M2M network infrastructure servers.

Security Association: Logical relationship between 2 nodes that are associated with a communication link. Security Associations are not communications links. Security Associations can take a number of forms but in each case they identify the nature of the security service (confidentiality, integrity, authentication or authorisation), the required algorithm and key. Security Associations can be established for single transactions (and thus their establishment can form part of the transaction itself) or for session based associations (in such instances the association is generally established independently of the individual transactions that are to be secured).

3.2 Symbols

None.

3.3 Abbreviations

None.

3.4 Acronyms

For the purposes of the present document, the abbreviations given in [i.2] and the following apply:

API	Application Programming Interface

CSE	Common Service Entity
CSF	Common Service Function
DoS	Denial of Service
ETSI SCP	ETSI Technical Committee Smart Card Platform
FFS	For Further Study
HTML	Hyper Text Markup Language
HSM	Hardware Security Module
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NA	Network Application
OS	Operating System
SA	Security Association
SQL	Structured Query Language
WAN	Wide Area Network

4 Conventions

The key words “Shall”, ”Shall not”, “May”, ”Need not”, “Should”, ”Should not” in this document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 Overview

5.1 oneM2M Security Context and Domains

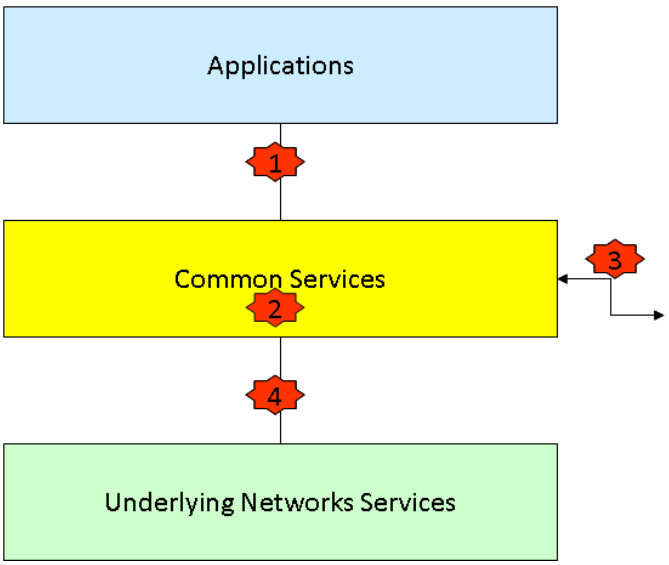

Figure 1 : Overview of the oneM2M Security context

The oneM2M security context described in Figure 1 is based on the high level functional view given in [i.4]. Four security domains are identified. Each of these domains provides security features to meet certain threats and in particular protect against attacks, in associated trust scenarios.

- **(1) Application domain security:** the set of security features that enable Applications and Common Services to securely exchange messages and protect against attacks on the Mca Reference Points.

- **(2) Intra Common Services domain security:** the set of security features that enable Common Service Functions in the Common Service Entity to securely exchange messages and which in particular protect against attacks on the CSE.
- **(3) Inter Common Services domain security:** the set of security features that enable secure exchange of messages between CSEs and protect against attacks on the Mcc Reference Points.
- **(4) Underlying Network security:** the set of security features that enable Underlying Network Services and Common Services to securely exchange messages and protect against attacks on the Mcn Reference Points.

5.2 Applications

An M2M Application Service Provider can rely on independent credentials to secure its End-to-End communications, so that application related information isexposed to either the M2M Service Provider or the underlying network operator. The M2M System provides an interoperable interface for provisioning and administration of security credentials in M2M nodes which can be used by the M2M Application or any trusted third party that is involved in application security.

5.3 Common Services

In cases where the M2M Service provider is trusted to provide security to the M2M Application, the ability to secure communication between nodes for the purpose of the M2M Service Layer can be made directly available by M2M Service Providers to the M2M Applications through an API.

5.4 Underlying Network

In cases where the underlying network provides secure communication for M2M Equipments that is trusted by the M2M Application Service Provider, the key derivation and secure connection establishment capabilities exposed by the underlying network can be used by the M2M System in the infrastructure domain, base on long term keys provided by the underlying network. There is a need for the M2M System to extend the provisioning of such security to edge nodes that are not directly connected to the underlying network (e.g. because they are behind a gateway).

6 Generic Security Mechanisms

Implementing security features and countermeasures to threats requires mechanisms that provide security related operations with an appropriate level of confidence. Those generic mechanisms are described within this clause. They include:

- secure storage of sensitive data
- sensitive functions executing operations on sensitive data
- secure connection allowing the secure transmission of sensitive data

6.1 Secure Storage

Sensitive data comprises key material / credentials, privacy related data such as identifiers and other data as identified by the M2M Solution Provider for the purpose of its use case. In order to prevent misuse of sensitive data, it requires protected and secure storage within the termination points of the M2M System. Secure storage capability can be implemented by several means within the network infrastructure nodes and network applications by the M2M Service Provider. In addition it needs to be ensured that secure storage capabilities are present in the termination node residing at the consumer, i.e. in the M2M Device and/or the M2M Gateway, depending on the requirements of the use case. It is highly recommended that M2M Devices/Gateways support a secure and tamper resistant storage capability for sensitive data, in particular when they are physically exposed to potential attackers.

The sensitivity level of data is associated to the minimum protection level indicating desired quality of protection against attacks as in Table 1.

Protection Level	Sensitivity Level of Data	Description
0	None	No protection. The data are exposed even without active attacks.
1	Low	Low protection, data are protected from passive observers but could be exposed by active attacks, be they local or remote. E.g. software solutions exist that rely on general purpose processing hardware of the supporting equipment.
2	Medium	Medium protection, protection of the data from remote attacks is addressed, but local attacks, especially physical attacks, remain possible, ie. Medium protection provides countermeasures against software attacks only E.g. Software solutions to protect data and sensitive functions rely on specific processing providing enforced isolation and enables sensitive code and data to be kept away from an unprotected operating environment, software and memory. The code running in the protected environment is cryptographically verified for integrity assurance.
3	High	High protection, addressing both remote and local attacks to access the data, including attacks involving physical access. This includes strong counter measures against software and hardware attacks, such as detection of abnormal operating conditions and scrambling plus hardware masking of the memory and side channel analysis of operations involving sensitive data.

Table 1: Configuration of Protection level for Sensitive Data handling

6.2 Sensitive Functions

All security features as described within the remainder of this document rely on the secure execution of certain sensitive functions. Sensitive functions operate on sensitive data that is securely stored such that sensitive data will never leak to any unauthorized entity. Sensitive functions are typically performed in termination points within the M2M System.

Examples of sensitive functions include:

- cryptographic algorithms
- (session) key derivation functions
- hash functions

Access to sensitive functions is subject to security policies and access control. Sensitive functions are accessible via a well defined interface.

6.3 Secure Connection

As many M2M Applications generate and exchange sensitive data, and essential M2M Services deal with the routing and exploitation of such information, the M2M System needs to be able to support security services such as ensuring availability, mutual authentication between communicating parties, confidentiality (e.g. protection against eavesdropping by unauthorized parties), integrity (i.e. protection against manipulation) and access control.

Sensitive data has to be transmitted within the M2M Solution between various stakeholders, each represented by a respective termination point within the M2M System. In order to ensure a secure transmission of that sensitive data, sensitive functions on securely stored data will be executed to set up a secure connection.

Whether the support of security services is addressed at the M2M Service Layer level or at the M2M Application level, the ability to establish security associations between corresponding M2M nodes is required. Ideally, this ability could apply to nodes affiliated with different M2M Application Service Providers and M2M Service Providers, not excluding capabilities that may be provided by third parties such as data analytics.

7 Security Vulnerabilities and Threats

7.1 Introduction

This clause lists and describes threats relevant to the security domains. Threats are described using a pre-defined template including information on the issue caused by the threat, a description of the threat itself and an indication of use cases impacted or potentially impacted. In addition affected security domains (see clause 5) and M2M Stakeholders are listed. The description of each threat concludes with an analysis indicating which of the main M2M Architecture components are impacted by the threat.

NOTE: A detailed risk assessment / evaluation of the level of impact of the threat depends on the assets and their value. The value of the assets heavily depends on the individual use case implemented in the M2M Solution. Risk assessment / evaluation is therefore out of scope of this threat analysis and falls under the responsibility of the respective stakeholders responsible for providing the M2M Solution and/or solution component. The number given to each of the threats do not give any indication on their priority.

7.2 Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways

Threat ID	**1**
Overview	**Long-term service-layer keys are discovered while they are stored in M2M Devices or M2M Gateways and are copied.**
Issue	Copied long-term service-layer keys may be used to impersonate M2M Devices and/or M2M Gateways.
Description	Long-term service-layer keys are stored within the M2M Device or M2M Gateway. Those keys are discovered and copied by unauthorized entities and used for illegitimate purposes. Discovery of stored long term service-layer keys may be achieved e.g. by monitoring internal processes (e.g. by Differential Power Analysis) or by reading the contents of memory of the M2M Device or M2M Gateway (by hardware probing or by use of local management commands).
Impacted Use Cases	All
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer
Architecture impact	Device / constrained Device : impacts storage of long-term service-layer keys Middle Node / Gateway : impacts storage of long-term service-layer keys Common Services Entity / Function: impacts Security CSF

7.3 Deletion of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways

Threat ID	**2**
Overview	**Long-term service-layer keys are deleted or deprecated while they are stored in M2M Devices or M2M Gateways**
Issue	Denial of service attack, preventing operation of the M2M Solution.
Description	Long-term service-layer keys are deleted or deprecated. This may be achieved by use of management commands (including impersonation of a system Manager) or by removal of the HSM if present and if removable. This attack may be perpetrated against the key-storage functions of M2M Devices or M2M Gateways.
Impacted Use Cases	All
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	Device / constrained Device : impacts storage of long-term service-layer keys Middle Node / Gateway : impacts storage of long-term service-layer keys Common Services Entity / Function: impacts Security CSF, may impact data management & repository CSF

7.4 Replacement of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways

Threat ID	**3**
Overview	**Long-term service-layer keys are replaced while they are stored in M2M Devices or M2M Gateways**
Issue	Users/consumers cannot be made accountable for their activities within the M2M System. Allows illegitimate operation of the M2M Solution.
Description	Long-term service-layer keys are replaced while they are stored in M2M Devices or M2M Gateways, in order to modify its operation. The attack may be achieved by use of management commands (including impersonation of a system manager) or by removal of the HSM if present and if removable. This attack may be perpetrated against the key-storage functions of M2M Devices.
Impacted Use Cases	All
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network

	Operator, if network operator keys are shared; User/Consumer.
Architecture impact	Device / constrained Device : impacts access mechanism to storage and management of long-term service-layer keys Middle Node / Gateway : impacts access mechanism to storage and management of long-term service-layer keys Common Services Entity / Function: impacts Security CSF, may impact data management & repository CSF

7.5 Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure

Threat ID	**4**
Overview	**Long-term service-layer keys are discovered while they are stored in the M2M infrastructure equipment (e.g. equipment holding network CSE or security server) and are copied.**
Issue	Copied keys may be used to impersonate M2M infrastructure equipment.
Description	Discovery may be achieved e.g. by the monitoring of internal processes, or by reading the contents of memory locations. The methods of attack include remote hacking and illicit use of management or maintenance interfaces.
Impacted Use Cases	All
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M System and its components; M2M Service Provider; System Administrator; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	M2M Service infrastructure

7.6 Deletion of Long-Term Service-Layer Keys stored in M2M Infrastructure equipment

Threat ID	**5**
Overview	**Long-term service-layer keys are deleted or deprecated while they are stored in the M2M infrastructure equipment (e.g. equipment holding network CSE or security server).**
Issue	Deletion of keys in the infrastructure equipment prevents proper operation and may lead to denial of service.
Description	Long-term service-layer keys may be deleted or deprecated by use of management commands (including impersonation of a System Administrator).
Impacted Use	All

Cases	
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M System and its components; M2M Service Provider; System Administrator; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	M2M Service infrastructure

7.7 Discovery of sensitive Data in M2M Devices or M2M Gateways

Threat ID	**6**
Overview	**Sensitive data is discovered while used during the execution of sensitive functions in M2M Devices or M2M Gateways and are copied.**
Issue	Copied sensitive data such as key material may be used to compromise M2M System security.
Description	Sensitive data such as long-term service-layer keys are used during the execution of sensitive function within the M2M Device or M2M Gateway and exposed. Sensitive data is then copied by unauthorized entities and used for illegitimate purposes.
Impacted Use Cases	All
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	Device / constrained Device : impacts storage of sensitive data and execution of sensitive functions Middle Node / Gateway : impacts storage of sensitive data and execution of sensitive functions Common Services Entity / Function: impacts Security CSF

7.8 General Eavesdropping on M2M Service-Layer Messaging between Entities

Threat ID	**7**
Overview	**General Eavesdropping on M2M Service-Layer Messaging Between Entities**
Issue	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

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.
Impacted Use Cases	All
Affected Security domain	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. Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator; User/Consumer
Architecture impact	Device / constrained Device : impacts storage of long-term service-layer keys Middle Node / Gateway : impacts storage of long-term service-layer keys Common Services Entity / Function: impacts Security CSF, may impact data management & repository CSF

7.9 Alteration of M2M Service-Layer Messaging between Entities

Threat ID	**8**
Overview	**Alteration of M2M Service-Layer Messaging Between Entities**
Issue	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
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.
Impacted Use Cases	All
Affected Security domain	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. Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security; if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider,Manufacturer of M2M Devices and/or M2M Gateways, M2M Device/Gateway Management entities, M2M Service Provider, Network Operator, User/Consumer
Architecture impact	Device / constrained Device : impacts storage of long-term service-layer keys Middle Node / Gateway : impacts storage of long-term service-layer keys Common Services Entity / Function: impacts Security CSF, may impact data management & repository CSF

7.10 Replay of M2M Service-Layer Messaging between Entities

Threat ID	**9**
Overview	**Replay of M2M Service-Layer Messaging Between Entities**
Issue	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.
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.
Impacted Use Cases	All
Affected Security domain	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. Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer
Architecture	Device / constrained Device : impacts storage of long-term service-layer keys

impact	Middle Node / Gateway : impacts storage of long-term service-layer keys Common Services Entity / Function: impacts Security CSF, may impact data management & repository CSF

7.11 Unauthorized or corrupted Applications or Software in M2M Devices/Gateways

Threat ID	**10**
Overview	**Unauthorised or Corrupted Application and Service-Layer Software in M2M Devices/Gateways**
Issue	An attacker installs unauthorised M2M Service-layer software or modifies authorised software functions in M2M Devices or M2M Gateways.
Description	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; • prevent operation of the affected M2M Devices/Gateways. The attack may be perpetrated locally or by illicit use of remote management functions.
Impacted Use Cases	All
Affected Security domain	Application domain security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; User/Consumer.
Architecture impact	M2M Service Provider's Domain; M2M Devices and M2M Gateways

7.12 M2M System Interdependencies Threats and cascading Impacts

Threat ID	**11**
Overview	**M2M System interdependencies threats and cascading impacts**
Issue	Underlying systems and resources may impose many forms of interdependency with the M2M Application, M2M Device / Gateway or M2M Infrastructure which is not apparent during period of normal operation.
Description	While M2M endpoints and M2M Gateways might be dedicated to specific M2M Services, M2M Systems as a whole will frequently share resources with a variety of other un-related systems and applications.
Impacted Use	All use cases.

Cases	
Affected Security domain	Application domain security, Intra Common Services domain security, Inter Common Services domain security, Underlying Network security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	M2M Service Provider's Domain, M2M Devices and M2M Gateways

7.13 M2M Security Context Awareness

Threat ID	**12**
Overview	**Context-awareness**
Issue	A lack of context awareness for M2M endpoints, gateways and applications may increase the risks associated with resource exhaustion and under provisioning, triggering service impacts or outages.
Description	If the provided Security Level is sufficient and appropriate depends on the use case and the context of the operation. Keeping the security level static for all use cases may lead to inefficient usage of resources (in terms or processor, memory, network, operationally and financially).
Impacted Use Cases	All use cases.
Affected Security domain	Application domain security, Intra Common Services domain security, Inter Common Services domain security, Underlying Network security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	M2M Service Provider's Domain, M2M Devices and M2M Gateways

7.14 Eaves Dropping/Man in the Middle Attack

Threat ID	**13**
Overview	**Eaves Dropping/Man In the Middle Attack**
Issue	Keys and other sensitive Information can be discovered by eavesdropping on messages at the transport layer
Description	The primary difficulty lies in monitoring the proper network's traffic while users are accessing the vulnerable site. Detecting basic flaws is easy. Just observe the site's network traffic. More subtle flaws require inspecting the design of the application and the server configuration. The attack exploits lack of security protection while data is in transit, or vulnerabilities in the protocol that was chosen to protect the communication pipe
Impacted Use	All

Cases	
Affected Security domain	Inter Common Services domain security; Underlying Network security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	Mca-Reference Point, Mcc-Reference Point, Mcn-Reference Point

7.15 Transfer of keys via independent security element

Threat ID	**15**
Overview	**Transfer of keys via independent security element**
Issue	The attack is carried out by an attacker who gains unauthorized possession of a set of viable keys and credentials by removing them from a legitimate M2M Device.
Description	The attack is carried out by an attacker who gains unauthorized possession of a set of viable keys and credentials by removing them from a legitimate M2M Device. The attacker will then use the removed keys and credentials in different, possibly unauthorized M2M Devices. The M2M Devices may attach to a network and consume non M2M network services, in which the charge will be passed to a legitimate M2M User. Additionally, a denial of service to the legitimate user may occur when the unauthorized M2M Device is online, the unauthorized M2M Device may use legitimate M2M Services, though the cost is passed on to the legitimate user.
Impacted Use Cases	All use cases.
Affected Security domain	Intra Common Services domain security; Inter Common Services domain security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; User/Consumer.
Architecture impact	Mca-Reference Point, Mcc-Reference Point

7.16 Buffer Overflow

Threat ID	**16**
Overview	**Buffer Overflows**
Issue	This type of attack is present when the use of non-type safe API's are exposed.
Description	Buffers of data + 'N' are passed through an API where it is known that the API is designed to have length constraints. The N bytes overflow into an area that was being utilized by other storage (heap overflow) or precipitates the return address to be corrupt (stack overflow). Stack overflows are indicated by the return code jumping to a random location, and as a consequence, incorrect code is executed and may change local data (rights of code or a file)

Impacted Use Cases	All.
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security
Affected Stakeholders	M2M Application Service Provider; M2M Service Provider; User/Consumer.
Architecture impact	Mca-Reference Point, Mcc-Reference Point

7.17 Injection

Threat ID	**17**
Overview	**Injection**
Issue	Send inappropriate queries to the application-level server that will exploit vulnerabilities of the query interpreter in order to gain un-authorized access.
Description	Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources. Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code, often found in SQL queries, LDAP queries, XPath queries, OS commands, program arguments, etc. Injection flaws are easy to discover when examining code, but more difficult via testing.
Impacted Use Cases	All.
Affected Security domain	Application domain security; Inter Common Services domain security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Service Provider; User/Consumer.
Architecture impact	CSE; Mca-Reference Point, Mcc-Reference Point

7.18 Session Management and Broken Authentication

Threat ID	**18**
Overview	**Session Management and Broken Authentication**
Issue	Custom session and authentication schemes frequently have flaws in areas such as logout, password management, timeouts, remember me, secret question and account update.
Description	Consider anonymous external attackers, as well as users with their own accounts, who may attempt to steal accounts from others. Also consider insiders wanting to disguise their actions. Exploitation spoof this type is of average difficulty, Attacker uses leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to impersonate users.
Impacted Use Cases	All

Affected Security domain	Application domain security; Inter Common Services domain security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; User/Consumer.
Architecture impact	CSE; Mca-Reference Point, Mcc-Reference Point

7.19 Security Misconfiguration

Threat ID	**19**
Overview	**Security Misconfiguration**
Issue	Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the M2M System.
Description	Consider anonymous external attackers as well as users with their own accounts that may attempt to compromise the M2M System. Also consider insiders wanting to disguise their actions. Easy to exploit, attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the M2M System.
Impacted Use Cases	All.
Affected Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security
Affected Stakeholders	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M Gateways; M2M Device/Gateway Management entities; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	CSE; Mca-Reference Point, Mcc-Reference Point, Mcn-Reference Point

7.20 Insecure Cryptographic Storage

Threat ID	**20**
Overview	**Insecure Cryptographic Storage**
Issue	The most common flaw in this area is simply not encrypting data that deserves encryption.
Description	Attackers typically don't break the cryptography. They break something else, such as find keys, get cleartext copies of data, or access data via channels that automatically decrypt. The most common flaw in this area is simply not encrypting data that deserves encryption. When encryption is employed, unsafe key generation and storage, not rotating keys, and weak algorithm usage is common. Use of weak or unsalted hashes to protect passwords is also common. External attackers have difficulty detecting such flaws due to limited access. They usually must exploit something else first to gain the needed access.
Impacted Use Cases	All.

Affected Security domain	Intra Common Services domain security; Inter Common Services domain security
Affected Stakeholders	M2M Application Service Provider; M2M Service Provider; Network Operator, if network operator keys are shared; User/Consumer.
Architecture impact	CSE

7.21 Invalid Input Data

Threat ID	**21**
Overview	**Invalid Input Data**
Issue	Input data validation is used to ensure that the content provided to an application does not grant an attacker access to unintended functionality or privilege escalation
Description	Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, and cross site scripting code to gain control over vulnerable machines. An attacker may be able to impose a Denial of Service, bypass authentication, access unintended functionality, execute remote code, steal data and escalate privileges. While some input validation vulnerabilities may not allow exploitation for remote access, they might still be exploited to cause a crash or a DoS attack.
Impacted Use Cases	All
Affected Security domain	Application domain security
Affected Stakeholders	M2M Application Service Provider; User/Consumer.
Architecture impact	Mca-Reference Point, Mcc-Reference Point

7.22 Cross Scripting

Threat ID	**22**
Overview	**Cross Scripting**
Issue	Cross Scripting allows attackers to inject code into the Web pages generated by the vulnerable Web application.
Description	Cross-site scripting takes advantage of Web servers that return dynamically generated Web pages or allow users to post viewable content to execute arbitrary HTML and active content such as JavaScript, ActiveX, and VBScript on a remote machine that is browsing the site within the context of a client-server session
Impacted Use Cases	All
Affected Security domain	Application domain security
Affected	M2M Application Service Provider; Manufacturer of M2M Devices and/or M2M

Stakeholders	Gateways; M2M Service Provider; User/Consumer.
Architecture impact	Mca-Reference Point, Mcc-Reference Point

8 Countermeasures

8.1 Introduction

Within this section, countermeasures and solutions are described preventing threats described in clause 7. A combination of countermeasures may need to be implemented to comprehensively mitigate the risk and to overcome the threat, i.e. a set of appropriate countermeasures has to be selected depending on the requirements of the specific M2M Solution.

8.2 Countermeasures

8.2.1 Tamper resistant Storage of long-term Service-Layer Keys within M2M Devices / Gateways

Related threats	**Threat 1:** Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways **Threat 2:** Deletion of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways **Threat 3:** Replacement of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways
Countermeasure 1	M2M long-term service-layer keys are stored in a HSM (whose tamper-resistance may be certified) residing within the M2M Device / Gateway which renders it infeasible for the attacker to discover the value of keys by logical or physical means.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack. A lot of prior art exists in the form of specifications of e.g. ETSI SCP. Other sensitive data / credentials in addition to long-term service-layer keys can be protected
Disadvantages	Additional per-item cost for HSM Need to specify and demonstrate the level of security assurance across the range of manufacturers and their products.

8.2.2 Secure Storage of long-term Service-Layer Keys within M2M Infrastructure Equipment

Related threats	**Threat 4:** Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure **Threat 5:** Deletion of Long-Term Service-Layer Keys stored in M2M Infrastructure equipment

Countermeasure 2	M2M long-term service-layer keys (other than public keys) are securely stored in a server-HSM residing in infrastructure equipment which renders it infeasible for the attacker to discover the value of keys by logical or physical means.
Applicable Security domain	Application domain security, Intra Common Services domain security, Inter Common Services domain security or Underlying Network security
Advantages	Resists the attack. A lot of prior art exists.
Disadvantages	Additional cost. Need to specify and demonstrate the level of security assurance across the range of manufacturers and their products.

8.2.3 Non-access to Service-Layer Keys stored within HSM / server-HSM

Related threats	**Threat 4:** Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure
Countermeasure 3	HSM / server-HSM do not reveal the value of the stored secret keys (other than public keys), even to a management system or to an authorised representative of the M2M System Operator, such as a System Administrator.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	See Countermeasure 1
Disadvantages	None.

8.2.4 Secure Execution of sensitive Functions in M2M Devices / M2M Gateways

Related threats	**Threat 6:** Discovery of sensitive Data in M2M Devices or M2M Gateways
Countermeasure 4	The execution of Sensitive Functions never causes long-term service-layer keys to be exposed outside of the HSM in which they are stored. Sensitive functions may be exectured within the HSM.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	See Countermeasure 1
Disadvantages	May increase the complexity of the HSM.

8.2.5 Physical / logical Binding of HSM to M2M Device / Gateway

Related threats	**Threat 2:** Deletion of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways **Threat 15:** Transfer of keys via independent security element
Countermeasure 5	The HSM containing the M2M long-term service keys is bound to the M2M Device or M2M Gateway, using physical and/or logical means.

Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack. Keys cannot be stolen (and M2M Device/Gateway rendered inoperable) by removal of HSM.
Disadvantages	Logical binding of HSM to Device/Gateway are of limited effectiveness.

8.2.6 Strong Authentication for Access to long-term Service-Layer Keys

Related threats	**Threat 2:** Deletion of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways **Threat 3:** Replacement of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways **Threat 5:** Deletion of Long-Term Service-Layer Keys stored in M2M Infrastructure equipment
Countermeasure 6	Access to and/or modification of stored Sensitive Data and in particular of the long-term service-layer keys requires strong (i.e. cryptographic) authentication of the accessing/modifying entity, followed by authorisation.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack.
Disadvantages	Involves cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms. Communication impact for remote management

8.2.7 Use of Security Associations, mutual Authentication and Confidentiality

Related threats	**Threat 8:** Alteration of M2M Service-Layer Messaging between Entities
Countermeasure 7	A security association is established between the communicating entities, which provides mutual authentication, integrity and confidentiality
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack. Well established counter-measure. High degree of assurance in the M2M application, supporting critical infrastructure functions and mitigating both logical and cascading kinetic impacts.
Disadvantages	Involves cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms. Communication impact for remote management may create unacceptable network loads during certain periods, such as key expiry, or system-wide re-starts. May place unsustainable loads on the endpoint device, for instance during cryptographic

	operations for authentication or for encryption. May place inappropriate demands on the device for memory protection to protect credentials – or protections are insufficient to support assurance requirements

8.2.8 Proven Resistance to Man-in-the-Middle Attacks

Related threats	**Threat 8:** Alteration of M2M Service-Layer Messaging between Entities
Countermeasure 8	The security association between communicating entities uses protocols which are proven to resist man-in-the-middle attacks
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack.
Disadvantages	Involves cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms. Communication impact for remote management

8.2.9 Limited Life Session Keys bound to Service Layer

Related threats	**Threat 8:** Alteration of M2M Service-Layer Messaging between Entities
Countermeasure 9	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
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security, if keys are shared with underlying network.
Advantages	Resists the attack. Limits exposure window if a session key is exposed or discovered. A well-established counter-measure. Allows shorter key lengths reduces cryptographic overheads
Disadvantages	Involves cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms. Communication impact for remote management May place unsustainable loads on the endpoint device, for instance during cryptographic operations for authentication and re-key. May create unacceptable network and M2M Service backhaul loads during certain periods, such as re-key, or system-wide re-starts.

8.2.10 Replay Protection

Related threats	**Threat 9:** Replay of M2M Service-Layer Messaging between Entities
Countermeasure 10	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
Applicable Security	Application domain security; Intra Common Services domain security; Inter Common Services

domain	domain security; Underlying Network security
Advantages	Resists the attack.
Disadvantages	Involves cost, e.g. of providing crypto authentication means to System Administrators, and access-control mechanisms. Communication impact for remote management

8.2.11 Keys can be derived from M2M Service-layer keys

Related threats	**Threat 1**: Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways **Threat 4**: Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure **Threat 9**: Replay of M2M Service-Layer Messaging between Entities
Countermeasure 11	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.
Applicable Security domain	Application domain security, Underlying Network security.
Advantages	Resists the attack. Limits exposure window if a session key is exposed or discovered. A well-established counter-measure. Allows shorter key lengths reduces cryptographic overheads.
Disadvantages	May place unsustainable loads on the endpoint device, for instance during cryptographic operations for authentication and re-key. May create unacceptable network and M2M Service backhaul loads during certain periods, such as re-key, or system-wide re-starts.

8.2.12 Integrity Verification

Related threats	**Threat 10**: Unauthorized or corrupted Applications or Software in M2M Devices/Gateways
Countermeasure 12	The integrity of executable functions and files in M2M Devices/Gateways can be verified.
Applicable Security domain	Application domain security.
Advantages	Detects the attack. High degree of assurance in the M2M application, supporting critical infrastructure functions and mitigating both logical and cascading kinetic impacts.
Disadvantages	Increases the cost and complexity of the M2M Device/Gateway, which may or may not be significant. May place unsustainable loads on the endpoint device, for instance during cryptographic operations for authentication or for encryption. May place inappropriate demands on the device for memory protection to protect credentials – or protections are insufficient to support assurance requirements. May create unacceptable network loads during certain periods, such as key expiry, or

	system-wide re-starts.

8.2.13 Policy based Actions

Related threats	**Threat 10**: Unauthorized or corrupted Applications or Software in M2M Devices/Gateways
Countermeasure 13	Policy-based action can be taken to prevent the use of functions or of M2M Devices/Gateways which fail the integrity verification test.
Applicable Security domain	Application domain security
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. May place unsustainable loads on the endpoint device and reduce performance, for instance during integrity checking (hashing) operations of system files.

8.2.14 Shared Asset Inventory

Related threats	**Threat 11:** M2M System Interdependencies Threats and cascading Impacts
Countermeasure 14	All M2M assets should be inventoried and shared assets identified, and interdependencies identified related to people, processes, technology and facilities.
Applicable Security domain	Application domain security, Underlying Network security.
Advantages	Exposes unknown interdependencies for management assessment.
Disadvantages	Adds cost to the design stage. Requires scheduled repetition: on-going costs.

8.2.15 Sensitivity Assessment

Related threats	**Threat 11:** M2M System Interdependencies Threats and cascading Impacts
Countermeasure 15	Conduct sensitivity assessment of various shared assets, for management review.
Applicable Security domain	Application domain security, Underlying Network security.
Advantages	Exposes independent system sensitivities for management assessment.
Disadvantages	Adds cost to the design. Requires scheduled repetition: on-going costs.

8.2.16 Risk Assessment

Related threats	**Threat 11:** M2M System Interdependencies Threats and cascading Impacts
Countermeasure 16	Based asset inventory and sensitivity assets, conduct or expand an planned risk assessment to most sensitive assets documenting interdependencies under normal and abnormal conditions for both M2M Service and other systems sharing sensitive assets. Make recommendations for management to treat, transfer or accept interdependency risks.
Applicable Security domain	Application domain security; Underlying Network security.
Advantages	Exposes interdependencies risks at are frequently overlooked in complex systems Avoids expense security retro-fits post-deployment Reduces service impacts and outages associated with system interdependencies.
Disadvantages	Adds cost to the deployment. Requires scheduled repetition: on-going costs.

8.2.17 Context Inventory and Assessment on Sensitivity

Related threats	**Threat 12:** M2M Security Context Awareness
Countermeasure 17	The different operational contexts of the M2M Systems assets should be inventoried and assessed for sensitivity to confidentiality, integrity and availability requirements.
Applicable Security domain	Application domain security; Underlying Network security.
Advantages	Exposes any different security contexts for engineering and management assessment.
Disadvantages	Adds cost to the design. Requires scheduled repetition: on-going costs.

8.2.18 Risk Assessment

Related threats	**Threat 12:** M2M Security Context Awareness
Countermeasure 18	Based context inventory and sensitivity assets, **conduct or expand an planned risk assessment** to determine is risks differ across operational contexts.
Applicable Security domain	Application domain security, Underlying Network security.
Advantages	Increases system performance, reduces costs. Avoids expense security retro-fits post-deployment
Disadvantages	Adds cost to the design stage. Requires repetition every time system is upgraded or changed.

8.2.19 Secure Communication Link

Related threats	**Threat 9**: Replay of M2M Service-Layer Messaging between Entities **Threat 13:** Eaves Dropping/Man in the Middle Attack
Countermeasure 19	Establish Secure Communications Link/ security association between relevant entities / nodes using modern cryptographic algorithms.
Applicable Security domain	Application domain security, Inter Common Services domain security; Underlying Network security
Advantages	Resists the attacks
Disadvantages	Requires additional implementation effort.

8.2.20 Secure Coding Practices

Related threats	**Threat 16:** Buffer Overflow
Countermeasure 20	Implement secure coding practices that enforce rigorous input data validation in system and services, database applications, and web services.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security
Advantages	Reduces or eliminates vulnerabilities in software before deployment.
Disadvantages	None.

8.2.21 Prevent Injection of un-trusted Data

Related threats	**Threat 17:** Injection
Countermeasure 21	Preventing injection requires keeping un-trusted data separate from commands and queries. If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter.
Applicable Security domain	Application domain security; Inter Common Services domain security
Advantages	Reduces or eliminates vulnerabilities in software before deployment.
Disadvantages	None.

8.2.22 Security Controls

Related threats	**Threat 18:** Session Management and Broken Authentication
Countermeasure 22	Put in place encryption and/or strong session management security controls. Implement secure coding practices that enforce rigorous input data validation in system and services, database applications, and web services.
Applicable	Application domain security; Inter Common Services domain security

Security domain	
Advantages	Resists the attack and additionally reduces or eliminates vulnerabilities in software before deployment.
Disadvantages	May add cost during the design phase.

8.2.23 Clean Application Architecture

Related threats	**Threat 19:** Security Misconfiguration
Countermeasure 23	Implement a strong application architecture that provides good separation and security between components.
Applicable Security domain	Application domain security; Intra Common Services domain security; Inter Common Services domain security; Underlying Network security
Advantages	Reduces or eliminates vulnerabilities in software before deployment.
Disadvantages	May add cost during the design phase. Difficult to evaluate strength of architecture.

8.2.24 Standard Algorithms

Related threats	**Threat 20:** Insecure Cryptographic Storage
Countermeasure 24	Ensure appropriate strong standard algorithms and strong keys are used, and key management is in place.
Applicable Security domain	Intra Common Services domain security; Inter Common Services domain security
Advantages	Resists the attack. Reduces cost and effort as well as increases security by using standard algorithms.
Disadvantages	None.

8.2.25 Protection of Storage by Privileges

Related threats	**Threat 21:** Invalid Input Data
Countermeasure 25	Processes must be put in place to protect the storage. Therefore it is recommended that least-privileges are implemented so that service privileges are minimized as much as possible to reduce risk.
Applicable Security domain	Application domain security
Advantages	Reduces or eliminates vulnerabilities in software before deployment.
Disadvantages	May add cost during the design phase.

8.2.26 Whitelist

Related threats	**Threat 22:** Cross Scripting

Countermeasure 26	Positive or “whitelist” input validation helps to protect against cross scripting. Such validation should decode any encoded input, and then validate the length, characters, and format on that data before accepting the input.
Applicable Security domain	Application domain security
Advantages	Straight forward implementation.
Disadvantages	Additional effort due to decoding and validation of input. Applications need to accept special characters.

9 Security Requirements

9.1 Authentication requirements

9.1.1 Levels of Assurance for Authentication

Four levels of assurance for entity authentication are defined in line with levels of assurance as defined in [i.6]. Each level describes the degree of confidence in the authentication processes and provides the described level of assurance that the entity using a particular identity actually is the entity to which that identity was assigned. Level 1 is the lowest level of assurance and Level 4 the highest. Each of these levels provides requirements for the implementation of the process.

- Level 1: lowest level with minimal confidence in the claimed or asserted identity of the entity but some confidence that the entity is the same over consecutive authentication events. This level is used when minimum risk is associated with erroneous authentication.
- Level 2: provides some level of confidence in the claimed or asserted identity of the entity. This level is used when moderate risk is associated with erroneous authentication. Single factor authentication is acceptable. Successful authentication depends on the entity proving, through a secure authentication protocol, that the entity has control of the sensitive data / credentials. Controls are in place to protect against attacks on stored sensitive data / credentials.
- Level 3: provides high confidence in the claimed or asserted identity of the entity. This level is used when substantial risk is associated with erroneous authentication. Multi-factor authentication is required. Any sensitive data or information exchanged in authentication protocols is cryptographically protected in transit and at rest.
- Level 4: provides very high confidence in the claimed or asserted identity of the entity. This level is used when high risk is associated with erroneous authentication. This level provides the highest level of entity authentication assurance. In addition to Level 3 this level requires the usage of tamper resistant hardware devices for the storage of all sensitive data such as cryptographic keys,

Some authentication factors may not apply to M2M communication.

9.2 Authorization requirements

In many traditional client-server authorization models, clients can access protected resources on the server by using the resource owner's credentials directly. This is typically done either by directly authenticating as the resource owner, or by using authorization credentials of the resource owner.

This approach, however, has the inherent limitation that the resource owner may want to grant restricted access to their resources (such as read-only, or limited in time), while they themselves retain the full access to the same resources.

When the owner of a resource wants to give such restricted permissions for using the resource to some third-party without sharing their full owner's credentials which allows full access to said resource, there are several issues to be solved:

- have a mechanism to allow a resource owner to configure the access authorization rules for restricted access by third-parties
- have a capability to handle the access by third-parties which will use the resource on behalf of User.
- allow the third-party to access the User's resource even when the User is offline.

9.3 Privacy related requirements

Although a user of a M2M System is generally considered to be an application or functional agent that represents a human, there are links between a device and its user that can be either directly derived or indirectly deduced. Consequently, identifiers used for communication in the M2M System must not be directly related to the real identity of either the device or its user, except where this is a requirement for operation of a specific M2M Application. The use of pseudonyms is a means to support this requirement.

9.4 RBAC Token Based Feature Requirements

Role Based Access Control (RBAC) in can be implemented using a token based framework (e.g. OAuth). The credential or token distribution can be implemented using an online scheme and an offline scheme. The requirements below are applicable to the offline scheme.

Requirement ID	Classification	Requirement Text
R-0001	RBAC-Token based	The CSE/node is capable of validating the AE that made the access request with the token presented to determine the role and the resource use/control.
R-0002	RBAC-Token based	The Token provisioning is recommended to be secure, (eg: protected from eavesdropping and manipulation avoid replay and service denial attacks), i.e. Tokens are Confidentiality and Integrity protected.
R-0003	RBAC-Token based	For offline credential/token provisioning, a secure platform (eg: Device Management server) is recommended to be used.
R-0004	RBAC-Token based	For offline provisioning of credentials/tokens, if IP/TCP is used, the TLS is recommended to be used to distribute the Token securely.
R-0005	RBAC-Token based	For offline provisioning of credentials/tokens, If IP/UDP is used for Token distribution, DTLS is recommended to be used to distribute the Token securely.

10 Authorization and Access Control

10.1 Authorization

10.1.1 Solutions for token based authorization

10.1.1.1 Solution 1: OAuth

The user can use the OAuth framework to give permission for restricted access to a third party entity in a token based access controlled system. The OAuth system issues 'access tokens', which represents authorized use of the system as the proof of the user's authorization. Note that the 'access token' is managed by server system associating with the 'authorized use', which consists of specific scopes and duration of access.

The third party entity can access necessary data and/or information without sharing credentials (such as user-id and password) which allows full access to the system.

In the oneM2M architecture, resource owners could be subscribers of the M2M Service, and third-party applications could be Web applications used by resource owner or by another user which is allowed to access the resource. This is of particular interest in Internet of Things scenarios, where the data streams produced by source devices owned by individual users could be made available to data consumer applications deployed by other parties.

10.1.1.1.1 Status of Specification

As described in [i.15], OAuth is an "authorization framework [that] enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf".

OAuth was standardized by the IETF, and there are two versions which are not compatible with each other. OAuth 1.0 is published as RFC5849, and OAuth 2.0 is published as RFC6749 to solve identified issued in OAuth 1.0.

10.1.1.1.2 Usage Scenario

The following clause illustrates interactions to give an authorization for resource access by third-party application following OAuth 2.0.
Note that once the access-token has been issued and passed to the M2M Application, the M2M Application can get access to restricted resource providing access-token without requiring further interaction with resource owner.

Description for Use Case:

The subscriber user wants to authorize a M2M Application for accessing data

Pre-conditions:

- M2M Platform is ready to provide some data resource to be referred as URI
- The M2M Application is assigned an application-id for the M2M platform
- The condition of authorized access to the resource is pre-defined as system-wide Role.

Procedures:

1) The user accesses the web page to enable new service provided by M2M application using a web browser.
2) The web page redirect to the authorization request page along with application-id and URI of the data. This web page can be dedicatedly prepared for allowing access from the M2M application.
3) The authorization request page requests the user to enter username and password to authenticate the user as owner of the resource.
4) The user inputs username and password to be authenticated.
5) The authorization request page shows the web form page to confirm the user allowing access to the data from M2M Application which is identified by application-id.
6) When user posts the form to confirm, it redirects again to the page in step2.
7) The page shows the message that authorization for the data access is granted, then redirects to the web page of the application portal along with 'access token' data.
8) When the user opens the page, the 'access token' data will be sent to the Application portal.
9) The Application portal page forwards the 'access token' to the M2M Application to be used for future access to the data belonging to the user.
10) M2M Application acknowledges and necessary authorization is given by user.
11) When the M2M Application is triggered as scheduled task, the M2M Application requests access to the user's data on the M2M Platform along with access token for the user.
12) M2M Platform checks the validity of the 'access token' given by the M2M Application
13) If the access token is determined as 'valid' the requested user data is provided to the M2M Application

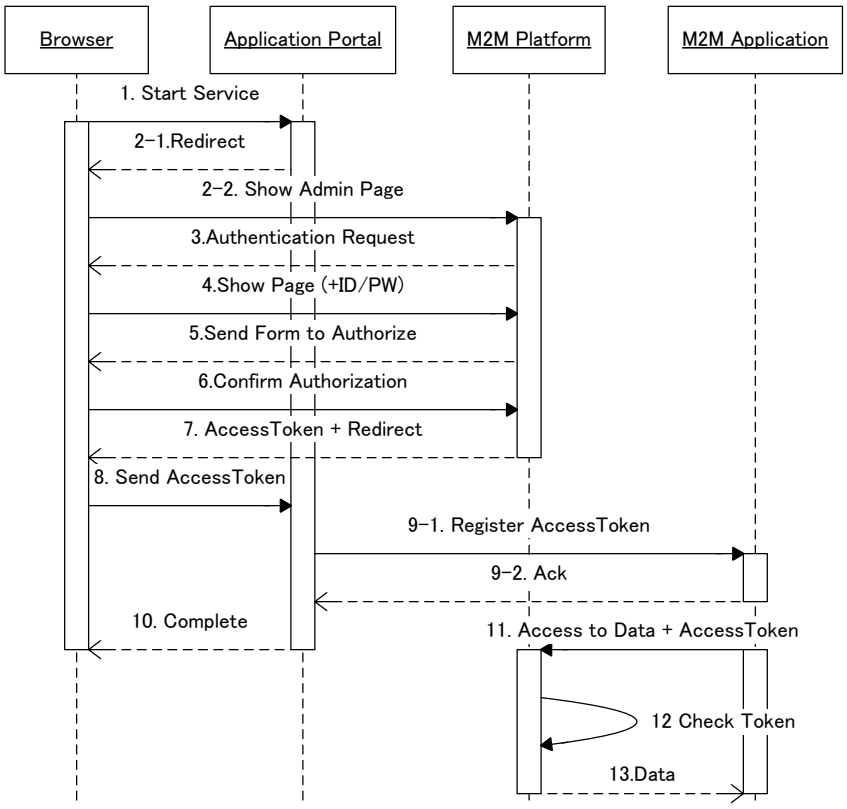

Figure 2: OAUTH flow

Post-conditions:

- M2M Application gets access-token to access the data
- M2M Platform can determine M2M Application can access the data

10.2 Access Control Management

Access Control is a set of Security components that control which entity (or who) can access specified services/resources and under what condition.

There are three important components of access control: identification, authentication, and authorization.

- Identification is a first part of the credential set by which an entity requesting access to the service/resource information, identifies itself to an Authentication service. Some examples of identification mechanisms are: role name or identification number, etc.
- Authentication is the second part of a credential set to verify the identity of the entity requesting the access. These mechanisms could be: passwords, certificates, cryptographic keys, tokens, etc.
- Authorization is the process of determining what the identified entity can actually access by evaluating applicable policies. Authorization is based on some type of predefined criteria which is enforced through: access control lists, roles capabilities, and any set of attributes (e.g. role, environement, etc.) relevant to an authorization decision. Such example of environement attributes can be time of day or IP address.

10.2.1 Role Based Access Control (RBAC)

10.2.1.1 RBAC Overview

The essence of RBAC is that permissions are assigned to roles rather than to individual users. Roles are created for various job functions, and users are assigned to roles based on their qualifications and responsibilities. Users obtain the corresponding permissions through assigned appropriate roles. Users can be easily reassigned from one role to another without modifying the underlying access structure. RBAC is thus more scalable than user based security specifications and greatly reduces the cost and administrative overhead.

The following terms are used to describe ANSI RBAC reference model [i.11]:

- Component – component refers to one of the major blocks of RBAC features, core RBAC, hierarchical RBAC, SSD relations and DSD relations.
- Objects – an object can be any system resource subject to access control, such as a file, printer, terminal, database record, etc.
- Operations - An operation is an executable image of a program, which upon invocation executes some function for the user.
- Permissions - Permission is an approval to perform an operation on one or more RBAC protected objects.
- Role - A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.
- User - A user is defined as a human being. Although the concept of a user can be extended to include machines, networks, or intelligent autonomous agents.

The ANSI RBAC reference model is defined in terms of four model components Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations. The RBAC reference model that contains all the four model components is show in Figure A.

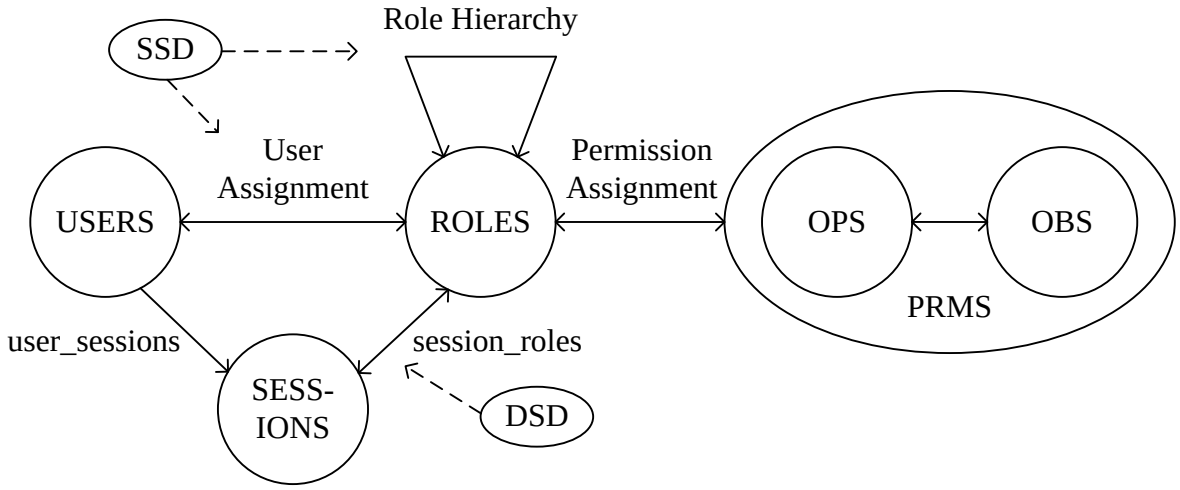

Figure 3: Role based access control model

Core RBAC

Core RBAC defines a minimum collection of RBAC elements, element sets and relations in order to completely achieve a Role-Based Access Control system. Core RBAC includes sets of five basic data elements called users (USERS), roles (ROLES), objects (OBS), operations (OPS) and permissions (PRMS). A user obtains roles through User Assignments, and a role obtains permissions through Permission Assignments. In addition, the core RBAC model includes a set of sessions (SESSIONS) where each session is a mapping between a user and an activated subset of roles that are assigned to the user. The permissions available to the user are the permissions assigned to the roles that are currently active across all the user's sessions. Core RBAC is required in any RBAC system, but the other components are independent of each other and may be implemented separately.

Hierarchical RBAC

The Hierarchical RBAC component adds relations for supporting role hierarchies. A role hierarchy is mathematically a partial order defining a seniority relation between roles, whereby senor roles acquire the permissions of their juniors and junior roles acquire users of their seniors. Role hierarchies can be established to reflect the natural structure of an enterprise. In a role hierarchy, one role may contain other roles, i.e. one role may implicitly include the permissions associated with roles.

Static Separation of Duty Relations

Separation of duty relations are used to enforce conflict of interest policies. Conflict of interest in a role-based system may arise as a result of a user gaining authorization for permissions associated with conflicting roles. Static Separation of Duty (SSD) Relations add exclusivity relations among roles with respect to user assignments. Because of the potential for inconsistencies with respect to static separation of duty relations and inheritance relations of a role hierarchy, the SSD relations model component defines relations in both the presence and absence of role hierarchies.

Dynamic Separation of Duty Relations

Dynamic Separation of Duty (DSD) Relations limits the permissions that are available to a user by placing constraints on the roles that can be activated within or across a user's sessions. Although this separation of duty requirement could be achieved through the establishment of a static separation of duty relationship, DSD relationships generally provide the enterprise with greater efficiency and operational flexibility.

10.2.1.2 Benefits of RBAC

The benefits of RBAC are:

- RBAC can reduce the complexity of security administration by placing roles between users and permissions.
- In RBAC it is easy to review who has been assigned to what permissions.
- RBAC is simpler than ABAC in privilege management. In RBAC bundles of permissions can be directly assigned to user through a role assignment, whereas in ABAC this may need to create a series of rules.
- From the view of audit, RBAC is easier than ABAC. In ABAC the consequence of rules may not be easy to fully grasp.

10.2.1.3 Limitations of RBAC

The limitations of RBAC are:

- Roles must be engineered before RBAC can be used. However, role engineering has turned out to be a difficult task. The challenge of RBAC is the contention between strong security and easier administration. [i.12]
- The least privileged condition is often difficult or costly to achieve because it is difficult to tailor access based on various attributes or constraints. In RBAC fine-grained access control may lead to "Role Explosion".
- In RBAC role assignments are based upon static job functions. Therefore it is difficult for RBAC to handle dynamically changing attributes, such time or IP address.
- It is difficult for RBAC to implement some security polices such as privacy and other regulatory mandates. [i.12]
- Web-based application adds more complexity to RBAC by weaving separate components together over the Internet to deliver application services, and the allocation of files and servers may not be compatible with organization structure. [i.12]
- RBAC cannot be used to ensure permissions on workflows in which sequences of operations need to be controlled.

10.2.2 Attribute Based Access Control (ABAC)

10.2.2.1 ABAC Overview

Although ABAC has no clear consensus model to date, the approach's central idea asserts that access can be determined based on various attributes presented by a subject. Rules specify conditions under which access is granted or denied.

In [i.13] Attribute Based Access Control (ABAC) is defined as: An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions. The major terms used to describe ABAC are described as follows:

- **Attributes** are defined characteristics of the subject, object, environment conditions that are predefined and preassigned by an authority. Attributes contain information given by a name-value pair.
- A **subject** is a human user or non-person entity, such as a device that issues access requests to perform operations on objects. Subjects are assigned one or more attributes.
- An **object** is a system resource for which access is managed by the ABAC system, such as devices, files, records, tables, processes, programs, networks, domains containing or receiving information. It can be the resource or requested entity, as well as anything upon which an operation may be performed by a subject including data, applications, services, devices, and networks.
- An **operation** is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, author, copy, execute, and modify.
- **Policy** is the representation of rules or relationships that makes it possible to determine if a requested access should be allowed, given the values of the attributes of the subject, object, and possibly environment conditions.
- **Environmental condition** is operational or situational context in which access request occur. Environmental conditions are detectable environmental characteristics. Environmental characteristics are independent of subject or object, and may include the current time, the current day of the week, location of a user, or the current threat level.

According to the description in [i.13], an ABAC model is shown in Figure B. An ABAC access control process could be described as:

1. A Subject sends an access request to ABAC system.
2. The ABAC evaluates Access Control Policies, Subject Attributes, Object Attributes, and Environment Conditions to compute an access control decision.
3. The ABAC permits this access to the object if the access is permitted; otherwise, it denies this access.

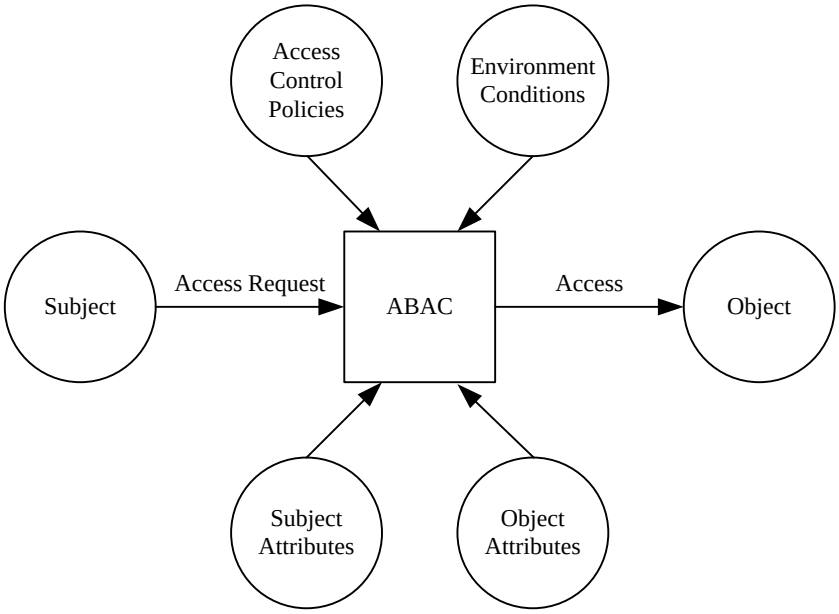

Figure 4: Attribute based access control model

10.2.2.2 Benefits of ABAC

Benefits of ABAC [i.13]:

- ABAC can provide fine-grained and contextual access control, which allows for a higher number of discrete inputs into an access control decision, providing a bigger set of possible combinations of those variables to reflect a larger and more definitive set of possible rules, policies, or restrictions on access.
- ABAC enables administrators to apply access control policy without prior knowledge of the specific subject. As long as the subject is assigned the attributes necessary for access to the required objects, rules or object attributes do not need to be modified.
- The access control policies that can be implemented in ABAC are limited only by the computational language and the richness of the available attributes.
- ABAC can provide more dynamic access control capability and limit long-term maintenance requirements of object protections, as access decisions can change between requests when attribute values change.

10.2.2.3 Limitations of ABAC

Limitations of ABAC:

- It is very difficult for ABAC to determine the permissions available to a particular user.
- ABAC may lead to a “Rule Explosion” when there too many attributes.
- ABAC system may be slow to answer authorization queries if the access control rules become complicated.
- It is difficult for ABAC to implement a static audit system, because it’s not practical to audit which users have been granted to a given permission or what permissions have been granted to a given user.

11 GBA (Generic Bootstrapping Architecture) framework

11.1 GBA overview

GBA framework relies on a BSF, HSS, SLF and NAF as specified in [i.10]. GBA has two modes (GBA_U and GBA_ME) and one variant (GBA_Digest).

- GBA_U and GBA_ME rely on AKA credentials stored in the UICC application.

  GBA_ME is a ME-based solution with all GBA-specific functions carried out in the ME. The Boostrapping Key "Ks" and the NAF key "Ks_NAF" are stored on the ME.

  GBA_U is a UICC-based GBA with UICC-based enhancement proposing higher level of security with the storage of GBA keys in the UICC. The Bootstrapping Key "Ks" and the NAF key "Ks_int_NAF" are stored in the UICC while the NAF Key "Ks_ext_NAF" is stored in the ME. All usage of the internal keys therefore need to reside on the UICC.

  The BSF decides which mode to run based on the UICC capabilities indicated in the GBA user security setting (GUSS).

- GBA_Digest is a GBA variant that extends the usage of GBA to environments where the UICC is not available. GBA_Digest relies on SIP Digest credentials.

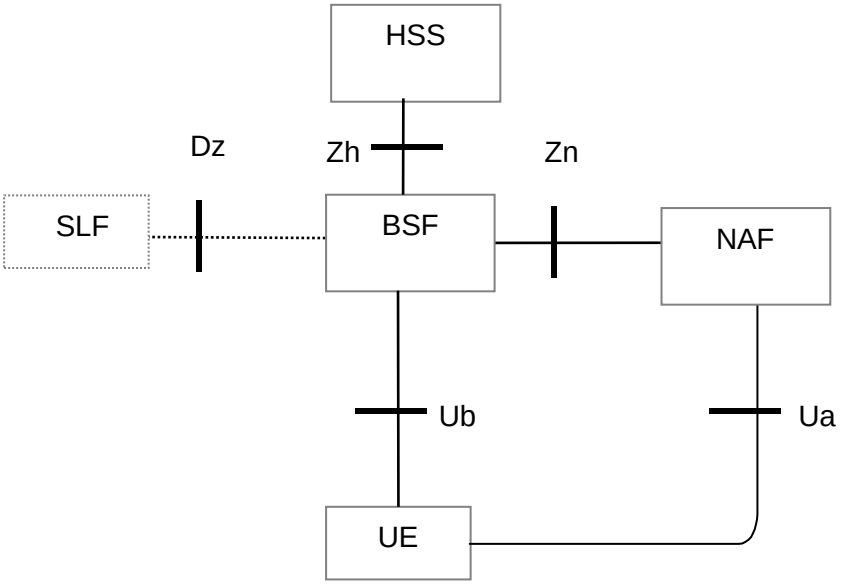

Figure 5-a: Simple Network Architecture for GBA in 3GPP [i.10]

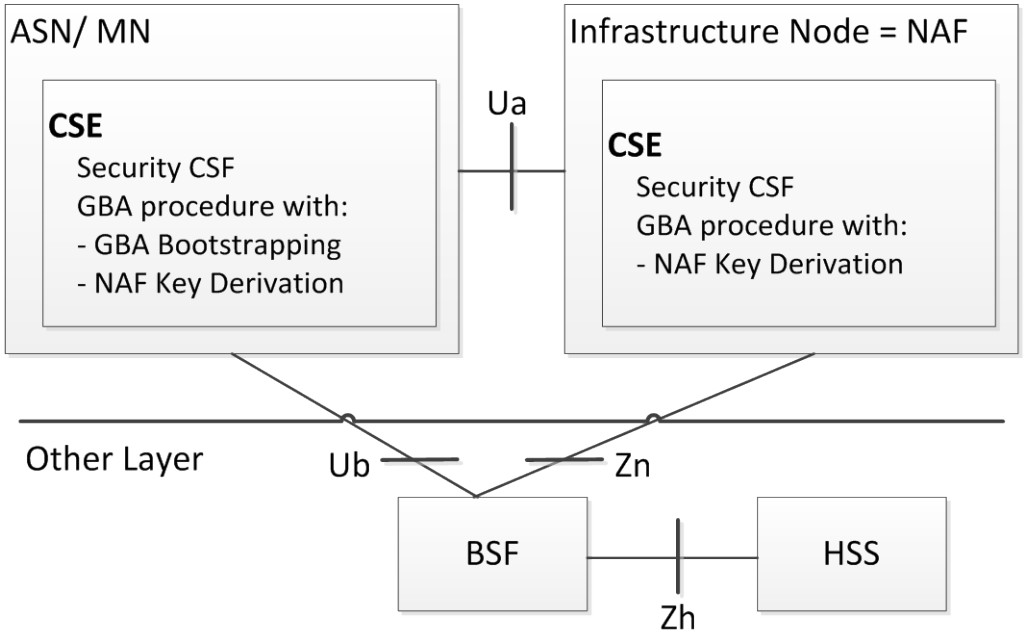

Figure 5-b: Use of GBA from underlying network in oneM2M

12 Suitable Security and Privacy Procedures and Processes

Based on the analysis, the following security procedures and functions are required within the Security CSF. The Security CSF architecture consists of following the layers as depicted below:

- Security Functions layer

  This layer contains a set of security functions that are exposed at reference point Mca and Mcc. These security functions can be classified into six categories; they are Identification, Authentication, Authorization, Security Association, Sensitive Data Handling and Security Administration.

- Secure Environment Abstraction Layer

  This layer implements various security capabilities such as key derivation, data encryption/decryption, signature generation/verification, security credential read/write from/to the Secure Environments, and so on. The security functions in the Security Functions Layer invoke these functions in order to do the operations related to the Secure Environments. In addition this layer also provides physical access to the Secure Environments. Implementation of this is out of scope of the present document.

- Secure Environments layer

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

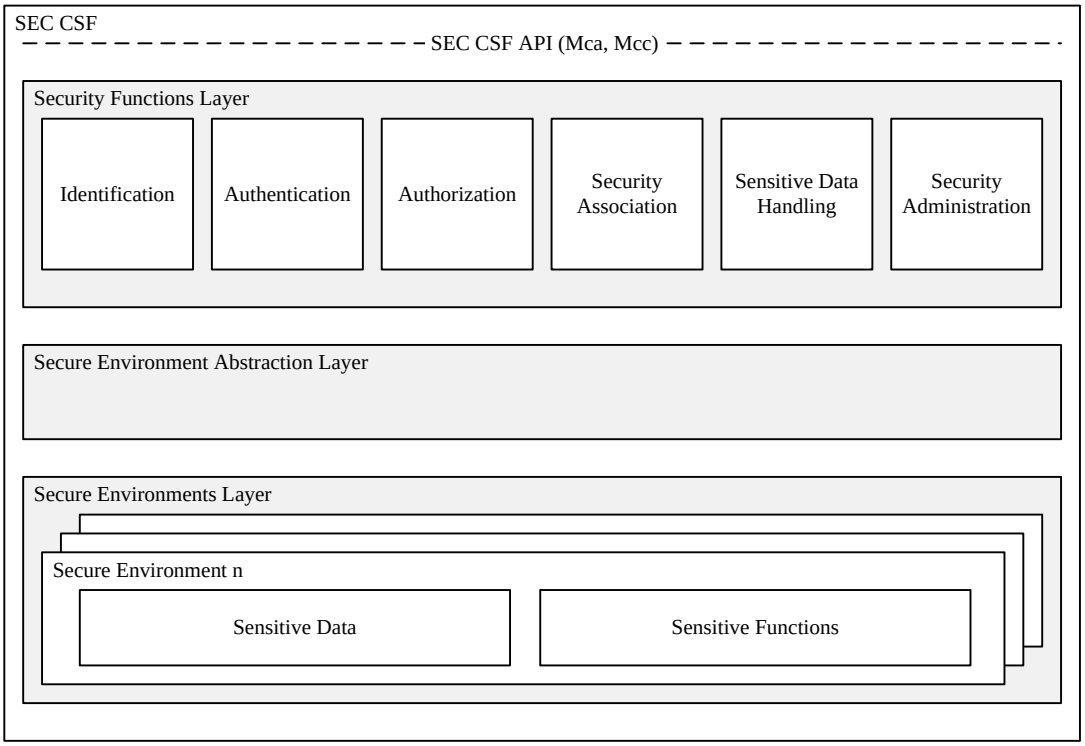

Figure 6: High level architecture of Security CSF

The interaction of the components between these layers creates a trust enabling architecture establishing security and trust between all parties involved in the M2M ecosystem as described below.

12.1 Trust Enabling Architecture

The Trust Enabling Architecture serves the purpose of establishing security and trust between all parties involved in the M2M ecosystem. It comprises the following infrastructure functions which may be external to the CSEs:

- M2M Enrolment functions, which manage the enrolment of M2M Nodes and M2M applications for access to M2M Services provided by an M2M Service Provider.
- M2M Authentication functions, in charge of identification and authentication of CSEs and AEs.
- M2M Authorization functions, which handles authorization requests to access resources.

The above functionalities are assumed to be operated by trusted parties (generally M2M Service Providers but possibly trusted third parties).

12.2 Enroling M2M Nodes and M2M applications for oneM2M services

Though M2M nodes in the field domain are assumed to communicate without human involvement, individuals or organizations remain responsible for setting the access control policies used to authorize their M2M nodes to access M2M services. In the following text, M2M Nodes is used to refer to M2M field nodes.

In particular, individuals or organizations acquiring M2M nodes can subscribe to a contract with an M2M Service provider (M2M Service Subscription) under which they enrol their M2M nodes (e.g. using identifiers pre-provisioned on the nodes, such as Node-ID). This in turn may require an M2M Service provisioning step (including Security provisioning) that takes place on the target M2M nodes themselves, for which interoperable procedures are specified by oneM2M (see section A.1). Following M2M service provisioning, the nodes can be identified and authenticated by an M2M Authentication Function for association with an M2M Service Subscription, whose properties reflect the contractual agreement established between their owner and the M2M Service Provider.

Similarly, It shall be possible for an M2M Service Provider to mandate that application accessing M2M services be provisioned with security credentials used to authorize specific operations to instantiated applications (see section A.2). This step facilitates the deployment and management of applications that are instantiated in great numbers, as it enables all instances of an application to be managed through common security policies that are set once for all. It also enables to keep control over applications issued by untrusted sources.

The above steps may be delegated to an M2M trust enabler, when this role is not assumed by the M2M Service Provider.

12.3 M2M initial provisioning Procedures

12.3.1 M2M Node Enrolment and Service Provisioning

M2M service provisioning is the process by which M2M nodes are loaded with the specific information needed to seamlessly access the M2M Services offered by an M2M Service Provider. This is an initial step performed only when an M2M node is enroled for using the M2M services of an M2M Service Provider. Though this process can be performed during device manufacturing, there is a need to enable this process to take place during field deployment in an interoperable way. M2M service provisioning assumes the existence of an M2M service subscription contracted with the target M2M Service Provider for the target M2M node. Remote provisioning scenarios require the M2M node to be mutually authenticated using pre-existing credentials (e.g. Node-ID and associated credential) with an M2M enrolment function, to securely exchange the provisioning information with the contracted M2M Service Provider. The M2M Service Provisioning takes place between an M2M node (without provisioned CSE) and an M2M Service Provider via an M2M enrolment function. As a result of provisioning, M2M Nodes are provided with necessary credentials and possibly other M2M service related parameters (e.g. CSE-ID, M2M-Sub-ID).

The first step of M2M service provisionining is the security provisioning procedure, by which M2M service provider specific credentials are shared between the M2M node in the field domain and an M2M authentication function in the infrastructure. Authenticated M2M nodes can then be associated with an M2M Service Subscription used to determine their specific authorizations.

The following security provisioning scenarios are supported by the oneM2M architecture:

1) Pre-provisioning

   Pre-provisioning includes all forms of out-of band provisioning, e.g. provisioning M2M nodes with M2M subscription information during the manufacturing stage.

2) Remote provisioning:

   Remote provisioning relies on pre-existing credentials in M2M Nodes (e.g. digital certificates or network access credentials) to provision subscription related parameters through a secure session with an M2M Enrolment Function. This form of provisioning enables M2M nodes already in the field (e.g. operational M2M Nodes) to be provisioned with M2M Service subscription.

   Following M2M service provisioning, a CSE associated with the target M2M Service provider in ASN/MN securely stores credentials used for authentication in association with M2M Authentication Function, with an associated lifetime (e.g. corresponding to the duration of the contractual agreement embodied by the M2M service subscription).

12.2.2 M2M Application enrolment

This procedure is an optional step that enables the M2M SP and/or M2M application provider to control which applications are allowed to use the M2M services. It assumes that M2M applications obtains or registers credentials to be used for controlling authorization. Each application will then be provisioned with a security credential (M2M Application key) which can be used to grant specific authorization to access an approved list of M2M services. Such authorization takes place between a CSE and an AE.

12.3 M2M operational security procedures

This clause introduces high level procedures that shall be performed before any other procedure on Mcc and Mca can take place.

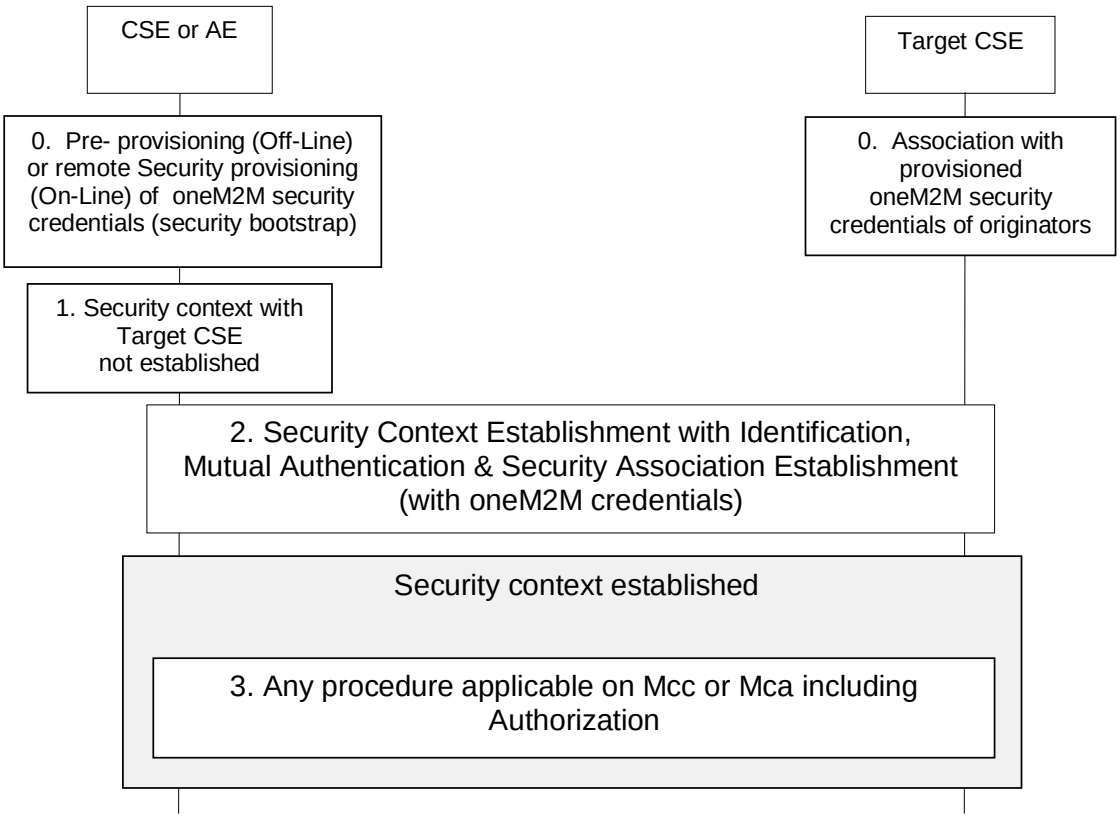

Figure 7: High Level Procedures on Mcc or Mca

12.3.1 Identification of CSE and AE

Identification is the process of identifying CSEs and AEs with the associated M2M service subscription to an M2M Authentication Function.

12.3.2 Authentication of CSE and AE

Prior to granting access to M2M services, the credentials resulting from the M2M node and M2M application enrolment procedures shall be used, together with the identities supplied in the identification step, to perform mutual authentication of the entities (AEs or CSEs) with an M2M Authentication Function. Upon mutual authentication, the corresponding entities receive authorization to access the M2M services defined in the M2M Service Subscription.

12.3.3 M2M Security Association Establishment

The M2M Security Association Establishment procedure is performed to generate a security credential (M2M Connection key) shared between communicating AEs/CSEs, when an AE/CSE on one node initiates communication with an AE/CSE on another node. This procedure is performed after successful identification and mutual authentication of the corresponding M2M entities and derives resulting keys that may be used to provide desired security services to the communicating entities, such as confidentiality and/or integrity of information exchange (these security services may be provided through establishment of a secure channel between the communicating entities or through object based security where only relevant information is encrypted prior to being shared). The lifetime of a security association shall be shorter than the lifetime of the credential used for authentication from which it is derived: It may be valid for the duration of a communication session, or be determined according to the validity period of the protected data. In case of a security association between two AEs, the lifetime of the security association can result from a contractual agreement between the subscribers of the communicating AEs.

12.3.4 M2M Authorization procedure

The M2M authorization procedure controls access to resources and services by CSEs and AEs. This procedure requires that the originator has been identified to an M2M Authentication Function and mutually authenticated and associated with an M2M Service Subscription. Authorization depends on:

- The privileges set by the M2M Service Subscription associated with the originator (e.g. service/role assigned to the originator),
- These privileges are set-up based on the Access Control Policies associated with the accessed resource or service.They condition the allowed operations (e.g. CREATE) based on the originator's privileges and other access control attributes (e.g. contextual attributes such as time or geographic location).

The authorization/access grant involves an Access Decision step to determine what the authenticated CSE or AE can actually access, by evaluating applicable Access Control Policies based on the CSE or AE privileges.

The following set of Access Control Policy attributes shall be available for an Access Decision.

- Access control attributes of Originator (e.g. Role, CSE_IDs, App-Inst-IDs, …)
- Access control attributes of Environment/Context (e.g. time , day, IP address,…)
- Access control attributes of Operations (e.g. create, execute, …)

The M2M Service Provider/administrator and owner of resources are responsible to establish access control policies that determine by whom, in what context and what operations may be performed upon those resources. If the requesting entity satisfies the owner's access control policy, then the access to the resource is granted.

The authorization procedure involves rerouting of access requests to an M2M authorization function and delivering access tokens valid for specific authorization.

History

Publication history		
V1.0.0	20140411	Approved at TP#10