|  |
| --- |
| Input Contribution |
| Meeting ID\* | REQ 26 |
| Title:\* | TR-0026-Vehicular\_Domain\_Enablement\_Clause\_9\_2\_Security |
| Source:\* | Jairo Lopez, Hitachi, jairo.lopez.uh@hitachi.comJiaxin Yin, Huawei, yinjiaxin@huawei.comDongjoo Kim, LG Electronics, dongjoo7.kim@lge.comNick Yamasaki, KDDI CORPORATION, nr-yamasaki@kddi.comKenichi Yamamoto, KDDI CORPORATION, kc-yamamoto@kddi.com |
| Uploaded Date:\* | 2016-11-29 |
| Document(s) Impacted\* | WI 0046oneM2M-TR-0026-Vehicular-Domain-Enablement-V0-4-0.DOC |
| Intended purpose ofdocument:\* | [x]  Decision[x]  Discussion[ ]  Information[ ]  Other <specify> |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0026. |
| Template Version:23 February 2015 (Dot not modify) |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

This document is the description of Clause 9.2 “Security” in TR-0026

# 9 Key Issues for Enablement for Vehicular Domain

9.2.x Key Issues x: Security

Due to the dynamic nature of vehicles, any service that intends to run in the vehicle domain will have to contend with security within the physical constraints of the vehicle as well as security when attempting communication with other vehicles and with external services. As has been shown throughout the use cases, there is a lot of sensitive data within vehicles that must be secured. There are also a great number of use cases that require using this sensitive data for decision making that must be transmitted in a secure manner. Furthermore, many decisions (or late decisions) by the vehicle components may impact human safety, so security and reactivity of the entire data acquisition, processing and decision chain is especially critical.

In oneM2M Release 2, Security CSF (SEC CSF) comprises the following functionalities:

* Sensitive data handling;
* Security administration;
* Security association establishment;
* Access control including identification, authentication and authorization;
* Identity management.

Within security, we believe that there has been one particular area that has not been clearly defined, which we label secure communication.

### 9.2.x.1 Secure communication

The vehicular domain has been traditionally the most rapidly networked domain. With the introduction of more powerful Electronic Control Units (ECUs) and a number of high bandwidth networking technologies, such as MOST, Automotive Ethernet and LTE-A, it has become imperative that vehicle domain communications be as secure as possible. Security for the vehicle domain must also be realized without impacting vehicle functionality or imposing taxing resource acquisition and allocation.

In the M2M System functional architecture, there exists the scopes of Intra-M2M Service Provider (SP) and Inter-M2M SP communication. We propose creating a similar classification in order to define secure communication in the vehicle domain. The classifications we recommend are described in Table 1.

Table 1 Communication classifications

|  |  |
| --- | --- |
| **Classification name** | **Description** |
| **External communication (EC)** | Communication between a vehicle and broader network operator related services. This includes, but is not limited to Internet based services. These services may or may not be included as a part of M2M systems. |
| **Inter-vehicle communication (InterVC)** | Communication between two or many vehicles. These vehicles may or may not be included in a M2M system. |
| **Intra-vehicle communication (IntraVC)** | Communication within the physical boundaries of one vehicle in the M2M system. This classification extends to wireless based communication that has a source and destination within the same vehicle. |

It is quickly apparent that the three classifications we have described have different requirements. We also propose that there are two major categories within these classifications. These are detailed in Table 2.

Table 2 Classification categories

|  |  |
| --- | --- |
| **Classification category** | **Description** |
| **Software based secure communication (SBSC)** | Secure communication created by using software running on any type of general purpose CPU in the system |
| **Hardware based secure communication (HBSC)** | Secure communication created by using specialized hardware based functions available to the system |

There is a need to consider SBSC from a standards point of view, as there are stricter resource requirements in the InterVC and IntraVC classifications. We assume that that EC will be using much more flexible and powerful vehicle gateway-like devices which will lean towards the use of HBSC, meaning that already standardized algorithms can be used. Since in InterVC and IntraVC, the devices used vary greatly in available resources and functionalities, we propose to include SBSC that can be further classified by the criteria seen in Table 3.

Table 3 SBSC recommended criteria

|  |  |
| --- | --- |
| **Criteria** | **Description** |
| **Cryptographic method type** | Symmetric or asymmetric cryptographic method |
| **Program size** | The non-volatile memory size of the program securing the communication (typically encrypting / decrypting messages) |
| **Average CPU time per byte** | The amount of time a general purpose CPU would need to successfully encrypt/decrypta byte of a message |
| **Memory use** | The size of the volatile memory footprint for the method to successfully encrypt/decrypt a message |

Whenever possible, the selection of a particular encryption algorithm, be it SBSC or HBSC based, for communication must be realized by the security mechanisms defined in the oneM2M release. When dealing with systems that are not part of the M2M system, the algorithm to use must be selected using other standardized security mechanisms available to both parties.

### 9.2.x.1.1 Lightweight Encryption

This type of encryption, discussed in ITU-T [i.19], significantly reduces the time consumed by a general purpose CPU for encryption, while permitting the system to pick a suitable level of protection for data confidentiality and integrity. Particularly for SBSC communications, these type of light-weight encryption algorithms shall be considered for resource constrained devices.

[i.19] Draft Recommendation ITU-T X.iotsec-1: "Simple encryption procedure for Internet of Things (IoT) environments".