



**FASTR**

Future of Automotive Security Technology Research

# Evaluation of Secure Over-the-Air Software Update Systems for the Automobile Industry

FASTR Connectivity and Cloud Work Group

Helena Handschuh, Syed Zaeem Hosain, Dan Klinedinst, Mark Marson, Adam Mistick

October 24, 2017

**TABLE OF CONTENTS**

1. Introduction ..... 1

2. Details on the Evaluation of the Uptane System. .... 1

    2.1 Background: ..... 1

    2.2 Uptane Details..... 1

    2.3 Guidelines Checklist from Uptane Evaluation..... 2

3. Details on the Evaluation of the OneM2M System. .... 7

    3.1 Background ..... 7

    3.2 One M2M Details ..... 7

    3.3 Guidelines checklist from OneM2M Evaluation..... 8

4. Summary of Evaluations ..... 13

    4.1 Platform # 1: Uptane ..... 13

    4.2 Platform #2: OneM2M..... 13

    4.3 Other Platforms Considered..... 13

5. Conclusions..... 13

6. References..... 14

Copyright and Other Legal Information ..... 14

**TABLE OF FIGURES**

Figure 1: Uptane SOTA Software Update Evaluation Checklist \_\_\_\_\_ 6

Figure 2: OneM2M SOTA Software Update Evaluation Checklist \_\_\_\_\_ 12

## I. INTRODUCTION

What is FASTR? FASTR (Future of Automotive Security Technology Research) is a non-profit consortium focused on accelerating automotive security innovation to *enable* trust in the autonomous vehicle of the future by *catalyzing* the creation and deployment of key technologies. FASTR views the automotive security landscape holistically, including everything from the physical supply chain, to consumer electronics used to unlock your car door, to the technical stack responsible for perception and motion planning, and beyond.

During the first half of 2017, the FASTR Connectivity and Cloud Work Group developed guidelines for analyzing secure over-the-air (SOTA) software update systems for the automotive industry [1]. These guidelines were then used by FASTR to evaluate 2 SOTA systems, Uptane and OneM2M, with the end goal of providing the industry with a means to assess different solutions, a superset of requirements/capabilities that could be considered best in class, and an analysis of areas requiring additional features or capabilities to ensure robust security. In this case, guidelines were weighted equally, however particular use cases may indicate the need to adjust the weighting.

## 2. DETAILS ON THE EVALUATION OF THE UPTANE SYSTEM.

### 2.1 BACKGROUND:

We used documentation from Uptane [3], [4] as our source and evaluated it against FASTR's guidelines for secure over-the-air software updates [1]. Reference [2] contains the full evaluation results.

### 2.2 UPTANE DETAILS

On the positive side, Uptane has clearly put a lot of thought and effort into designing their software repository and distribution system. The Design Overview [3] does a good job scoping their system. The beginning of that document clearly defines the goals, use cases, failure modes, and constraints of the system. It also does a thorough job discussing the threat model and analyzes a generic system against it. Finally, Uptane describes design principles of its system, which are intended to address the requirements of the system, as well as the weaknesses in the generic system they analyzed.

The Implementation Specification [4] documents the metadata formats required in order to be compliant with the Update system. While this document is sufficient for implementers to get started, we would have preferred an "Examples" section, in which the metadata files are filled in with actual values to support different scenarios. Overall, the Uptane documentation is clear and contains enough information for developers to implement software update systems compliant with Uptane's requirements.



Our main concern is that the Uptane design addresses almost none of the issues which arise when considering secure key management. Keys are simply assumed to be where they need to be. The protection of fielded keys and using them in a secure manner is not addressed. Revocation is briefly mentioned as being handled implicitly, with keys either expiring, or new keys overwriting old keys. Overall there are almost no requirements for managing the cryptographic keys. In particular, the generation, storage, backup, and distribution of keys within the system is not discussed.

It is understandable that Uptane has not addressed key management in their system. There are many different suppliers and devices in an automobile, as well as many different automobile makers, and each has their own security and key management processes. This makes it incredibly difficult to develop a comprehensive plan for managing all the different keys.

### 2.3 GUIDELINES CHECKLIST FROM UPTANE EVALUATION

We used the guidelines checklist from [1] to help us evaluate the Uptane system. Figure 1 below the filled in checklist from our analysis.

| Uptane SOTA Software Update Evaluation |                                                                                                                                                                               |       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                                                                                   | Score |
| [GDL 1]                                | Defines in-scope threats at high level                                                                                                                                        | 5/5   |
| Evaluation Comments                    | Uptane does good job scoping threats in [2].                                                                                                                                  |       |
| [GDL 2]                                | Side channel attacks and attacks requiring physical modification of the vehicle are out of scope                                                                              | 4/5   |
| Evaluation Comments                    | Uptane identifies physical attacks as out of scope in [2]. They should consider specifically rule out side-channel attacks which may not require physical modification of the |       |
| [GDL 3]                                | Defines which tampering attacks are in scope                                                                                                                                  | 5/5   |
| Evaluation Comments                    | Uptane does good job defining goals of the system in [2].                                                                                                                     |       |
| [GDL 4]                                | High-level digital certificate recommendation for software updates                                                                                                            | 5/5   |
| Evaluation Comments                    | Uptane system uses public key digital certificates.                                                                                                                           |       |
| [GDL 5]                                | Recommends software updates be encrypted                                                                                                                                      | 5/5   |
| Evaluation Comments                    | Uptane system supports encryption of software updates                                                                                                                         |       |
| [GDL 6]                                | Recommendation to sign after encryption                                                                                                                                       | 4/5   |
| Evaluation Comments                    | Does not explicitly state this, but it is implicit based on their design principles.                                                                                          |       |
| [GDL 7]                                | Software with invalid signature is never installed                                                                                                                            | 5/5   |
| Evaluation Comments                    | Uptane system only installs updates with valid signatures.                                                                                                                    |       |
| [GDL 8]                                | Only allowing authorized entities can update software                                                                                                                         | 5/5   |



| Uptane SOTA Software Update Evaluation |                                                                                                                    |       |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                        | Score |
| Evaluation Comments                    | Uptane system uses metadata which ensures update is authorized.                                                    |       |
| [GDL 9]                                | Recommendation for software updates to include versioning information to prevent rollbacks                         | 5/5   |
| Evaluation Comments                    | The Uptane system supports a release counter to prevent rollback.                                                  |       |
| [GDL 10]                               | Recommendation to use TLS for all network connections                                                              | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed                                                                            |       |
| [GDL 11]                               | Recommendation discouraging use of SSL                                                                             | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed                                                                            |       |
| [GDL 12]                               | Recommendation to perform host name verification of server                                                         | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed                                                                            |       |
| [GDL 13]                               | Recommendation to determine what information needs to be retained                                                  | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed                                                                            |       |
| [GDL 14]                               | Recommendation to retain important information                                                                     | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed                                                                            |       |
| [GDL 15]                               | Only deliver software to authorized devices                                                                        | 5/5   |
| Evaluation Comments                    | The Uptane system supports strong binding between software updates and the target vehicle.                         |       |
| [GDL 16]                               | Recommendation to perform threat modelling of the system                                                           | 5/5   |
| Evaluation Comments                    | Uptane has done a very good job of threat modeling in [2].                                                         |       |
| [GDL 17]                               | Recommendation to fail gracefully during DoS attacks                                                               | 5/5   |
| Evaluation Comments                    | Uptane has documented different flavors of DoS attacks [2] and their system includes mitigations against them [3]. |       |
| [GDL 18]                               | Recommendation to use secure boot wherever possible                                                                | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                           |       |
| [GDL 19]                               | Recommendation to utilize anti-malware protection wherever possible                                                | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                           |       |
| [GDL 20]                               | Update process never runs concurrently with other processes                                                        | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                           |       |



| Uptane SOTA Software Update Evaluation |                                                                                                                                                                    |       |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                                                                        | Score |
| [GDL 21]                               | Sensitive data and keys must be cleared after use                                                                                                                  | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 22]                               | TRNG guideline                                                                                                                                                     | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 23]                               | TRNG guideline                                                                                                                                                     | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 24]                               | TRNG guideline                                                                                                                                                     | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 25]                               | Encryption algorithm guideline                                                                                                                                     | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 26]                               | Cryptographic hash algorithm guideline                                                                                                                             | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 27]                               | Digital signature algorithm guideline                                                                                                                              | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 28]                               | Key agreement guideline                                                                                                                                            | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 29]                               | Key agreement guideline                                                                                                                                            | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |
| [GDL 30]                               | Recommended fields for digital certificate                                                                                                                         | 5/5   |
| Evaluation Comments                    | Uptane specification [3] includes digital certificate format.                                                                                                      |       |
| [GDL 31]                               | Digital certificate verification guideline                                                                                                                         | 5/5   |
| Evaluation Comments                    | Uptane specification [3] requires verifying all signatures. Implicit in that chains are verified all the way to the root.                                          |       |
| [GDL 32]                               | Recommendation to verify the before/after dates on each certificate                                                                                                | 4/5   |
| Evaluation Comments                    | Uptane system recommends expiration date associated with all signed metadata. No "Not Before" field in documentation reviewed, but easily supported by the system. |       |
| [GDL 33]                               | Digital certificate revocation guideline                                                                                                                           | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                           |       |



| Uptane SOTA Software Update Evaluation |                                                                                                                                                                                                                                    |       |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                                                                                                                                        | Score |
| [GDL 34]                               | Certificate Authority revocation guideline                                                                                                                                                                                         | 0/5   |
| Evaluation Comments                    | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 35]                               | Recommendation for network security between backend servers and the Gateway                                                                                                                                                        | 1/5   |
| Evaluation Comments                    | Uptane Design Overview [3] mentions need for networks security and using TLS. Uptane specification [4] explicitly declares network security out of scope.                                                                          |       |
| [GDL 36]                               | Recommendation to use point-to-point encryption whenever feasible                                                                                                                                                                  | 3/5   |
| Evaluation Comment                     | Uptane Design Overview [3] recognizes the importance of encrypting software updates. However, point-to-point encryption may not always be possible and Uptane specification [4] supports download of unencrypted software updates. |       |
| [GDL 37]                               | Recommendation discouraging use of passwords                                                                                                                                                                                       | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 38]                               | Recommendation for compliant systems to use multifactor authentication                                                                                                                                                             | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 39]                               | Recommendation for compliant systems to have a detailed KMP                                                                                                                                                                        | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 40]                               | Recommendation for KMP to contain complete list of keys in the system                                                                                                                                                              | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 41]                               | Recommendation to generate all keys using ahigh-quality random number generators                                                                                                                                                   | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 42]                               | Recommendation for KMP to describe generation of all the keys in the system                                                                                                                                                        | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 43]                               | Recommendation to store and back up all keys in an appropriate manner                                                                                                                                                              | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 44]                               | Recommendation for KMP to describe how all the keys in the system are stored and backed up                                                                                                                                         | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 45]                               | Recommendation to distribute all keys in a secure, authenticated manner                                                                                                                                                            | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                           |       |
| [GDL 46]                               | Recommendation for KMP to describe how all the keys in the system are distributed                                                                                                                                                  | 0/5   |



| Uptane SOTA Software Update Evaluation |                                                                                                                                                                                                                                                              |       |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                                                                                                                                                                  | Score |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                                                     |       |
| [GDL 47]                               | Recommendation for KMP to describe how all the keys in the system are used                                                                                                                                                                                   | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                                                     |       |
| [GDL 48]                               | Recommendation to have established procedures for updating keys                                                                                                                                                                                              | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                                                     |       |
| [GDL 49]                               | Recommendation to have established procedures if an expired key or certificate is encountered                                                                                                                                                                | 5/5   |
| Evaluation Comment                     | Uptane specification [4] requires verifying all signatures and expiration dates on keys, so will not install software signed with expired keys.                                                                                                              |       |
| [GDL 50]                               | Recommendation for KMP to describe which keys and certificates expire and will need to be updated, and the procedures for doing so                                                                                                                           | 3/5   |
| Evaluation Comment                     | Uptane specification [4] requires expiration dates be present and verified in certificates/metadata. Procedures for updating expired keys not addressed in documentation reviewed.                                                                           |       |
| [GDL 51]                               | Recommendation for KMP to describe the behavior of the system if an expired key or certificate is encountered                                                                                                                                                | 3/5   |
| Evaluation Comment                     | Uptane specification [4] requires that the system return an error code and not install software updates if expired keys or certificates are encountered. Additional actions (logging locally or informing back end) not addressed in documentation reviewed. |       |
| [GDL 52]                               | Recommendation to have established procedures for revoking and replacing keys and certificates                                                                                                                                                               | 3/5   |
| Evaluation Comment                     | Uptane Design Overview [3] describes implicit revocation of keys by signing metadata containing new key to replace old key, or allowing key to expire. Other mechanisms such as revocation lists not addressed in documentation reviewed.                    |       |
| [GDL 53]                               | Recommendation to have established procedures if a revoked key or certificate is encountered                                                                                                                                                                 | 3/5   |
| Evaluation Comment                     | If a key is revoked by allowing it to expire [2], then the system will reject software updates signed with that key [3].                                                                                                                                     |       |
| [GDL 54]                               | Recommendation for KMP to describe procedures for revoking and replacing keys and certificates                                                                                                                                                               | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                                                     |       |
| [GDL 55]                               | Recommendation for KMP to describe the behavior of the system if a revoked key or certificate is encountered                                                                                                                                                 | 0/5   |
| Evaluation Comment                     | Not addressed in documentation reviewed.                                                                                                                                                                                                                     |       |

**Figure 1: Uptane SOTA Software Update Evaluation Checklist**



## 3. DETAILS ON THE EVALUATION OF THE ONEM2M SYSTEM.

### 3.1 BACKGROUND

This document contains an evaluation of OneM2M's secure over-the-air (SOTA) software update system. The review is based on OneM2M documentation [6], [7], [8] and [9], using the FASTR SOTA software update system guidelines [1].

Additional information on the OneM2M Architecture is available at the OneM2M web site:

<http://www.onem2m.org>.

### 3.2 ONE M2M DETAILS

We evaluated the OneM2M Security Architecture. This is a general security architecture that covers Machine-to-Machine (M2M) and Internet of Things (IoT) applications and devices. It is not specific to automobiles. However, applications for data communications to and from automobiles are fully within its scope.

We reviewed four OneM2M documents ([6], [7], [8] and [9]) describing the OneM2M Security Architecture, and evaluated them against the FASTR guidelines for secure over-the-air (SOTA) software updates.

The OneM2M Security Architecture is a thorough specification of the specific needs of such automotive M2M and IoT applications, although they do not explicitly cover a SOTA implementation.

The requirements for a good SOTA system *could* be fulfilled by the information presented in the OneM2M Security Architecture documents, with the exception of the detailed design that may be required for software version management and the controls necessary to deal with software updates. These were beyond the scope of the four documents, although information in the complete OneM2M Release 2 Specification (see <http://www.onem2m.org> for more information) may be more illuminating.

The OneM2M Security Architecture does not address secure key management. It instead relies on the presence of external systems for this purpose, although [5] does describe the requirements for secure key transfer between elements in the system and architecture.

Detailed procedures for generating, storing and distributing keys is assumed to be provided in other *non-OneM2M* specifications.



### 3.3 GUIDELINES CHECKLIST FROM ONEM2M EVALUATION

Figure [2]

| OneM2M SOTA Software Update Evaluation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |       |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Guideline                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Score |
| [GDL 1]                                | Defines in-scope threats at high level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5/5   |
| Evaluation Comments                    | OneM2M has a thorough description of security threats in [2]. Chapter 7 is dedicated to describing the scope of the threats to the various security domains.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |
| [GDL 2]                                | Side channel attacks and attacks requiring physical modification of the vehicle are out of scope                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 4/5   |
| Evaluation Comments                    | In [5], section 5.1.0, OneM2M refers to physical access to the Secure Environments as out of scope, but also states that this is expected to be considered in “future releases”.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |
| [GDL 3]                                | Defines which tampering attacks are in scope                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 5/5   |
| Evaluation Comments                    | In [2], OneM2M recommends that Devices and Gateways support tamper resistant storage for sensitive data, in particular when they are physically exposed to potential attackers.<br>In [3], section 5.7.5, OneM2M recommends that gateways may verify that messages have not been tampered or modified by intermediate entities. It further requires that “end-to-end data credentials are protected for confidentiality, integrity and against tampering”.<br>In [5], OneM2M defines that protection level 4 sets a high level of confidence for user privacy and security and requires the use of tamper resistant hardware devices for storage of all sensitive data such as cryptographic keys. |       |
| [GDL 4]                                | High-level digital certificate recommendation for software updates                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5/5   |
| Evaluation Comments                    | OneM2M does not discuss a specific implementation for software updates, but in [3], section 8.3 and 8.4, require that all end-to-end messages/data communications use Security Certificate Keys and defines the process for use.<br>In [5], chapter 8 is dedicated to a description of Certificates, and their use in the OneM2M architecture.                                                                                                                                                                                                                                                                                                                                                     |       |
| [GDL 5]                                | Recommends software updates be encrypted                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 5/5   |
| Evaluation Comments                    | OneM2M does not specifically refer to software updates, but recommends encryption for all messages/data communication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |       |
| [GDL 6]                                | Recommendation to sign after encryption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5/5   |
| Evaluation Comments                    | The OneM2M architecture inherently requires this.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |
| [GDL 7]                                | Software with invalid signature is never installed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5/5   |
| Evaluation Comments                    | OneM2M does not specifically refer to software updates, but all messages/data communications must validate the required security and integrity checks to allow acceptance by the architecture elements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |       |
| [GDL 8]                                | Only allowing authorized entities can update software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5/5   |
| Evaluation Comments                    | OneM2M does not specifically refer to software updates, but in [4], various sections cover update processes and the requirements for authorization for updates to be allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |       |
| [GDL 9]                                | Recommendation for software updates to include versioning information to prevent rollbacks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 0/5   |



|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |     |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Evaluation Comments | OneM2M does not address the concept of rollbacks for software updates.                                                                                                                                                                                                                                                                                                                                                                                                 |     |
| [GDL 10]            | Recommendation to use TLS for all network connections                                                                                                                                                                                                                                                                                                                                                                                                                  | 5/5 |
| Evaluation Comments | In [2], section 9.4, TLS is recommended for provisioning of credentials / tokens, particularly if TCP/IP is used. For distribution of tokens, DTLS is recommended.<br>In [3], section 5.8.4, the description of data flow from devices to gateways and other architecture elements includes the required use of TLS and DTLS for security purposes.<br>In [5], section 6, the use of TLS and DTLS is expected for all messages / data communications that are secured. |     |
| [GDL 11]            | Recommendation discouraging use of SSL                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0/5 |
| Evaluation Comments | There is no specific mention of SSL (positive or negative) in the OneM2M documents.                                                                                                                                                                                                                                                                                                                                                                                    |     |
| [GDL 12]            | Recommendation to perform host name verification of server                                                                                                                                                                                                                                                                                                                                                                                                             | 5/5 |
| Evaluation Comments | In [5], section 10.1.1.5, “the certificate used to sign ... shall include nameConstraints satisfied by the hostname part of the full URI specification ...” essentially requires verification.                                                                                                                                                                                                                                                                         |     |
| [GDL 13]            | Recommendation to determine what information needs to be retained                                                                                                                                                                                                                                                                                                                                                                                                      | 0/5 |
| Evaluation Comments | OneM2M does not define specific information that needs to be retained, particularly in the context of software updates.                                                                                                                                                                                                                                                                                                                                                |     |
| [GDL 14]            | Recommendation to retain important information                                                                                                                                                                                                                                                                                                                                                                                                                         | 0/5 |
| Evaluation Comments | OneM2M does not define specific information that needs to be retained, particularly in the context of software updates.                                                                                                                                                                                                                                                                                                                                                |     |
| [GDL 15]            | Only deliver software to authorized devices                                                                                                                                                                                                                                                                                                                                                                                                                            | 4/5 |
| Evaluation Comments | OneM2M does not specifically refer to software updates, but all message / data communications are expected to be between authorized devices.                                                                                                                                                                                                                                                                                                                           |     |
| [GDL 16]            | Recommendation to perform threat modelling of the system                                                                                                                                                                                                                                                                                                                                                                                                               | 5/5 |
| Evaluation Comments | OneM2M has a thorough description of security threats in [2]. Chapter 7 is dedicated to describing the scope of the threats to the various security domains.                                                                                                                                                                                                                                                                                                           |     |
| [GDL 17]            | Recommendation to fail gracefully during DoS attacks                                                                                                                                                                                                                                                                                                                                                                                                                   | 0/5 |
| Evaluation Comments | OneM2M does not cover DoS in its documents.                                                                                                                                                                                                                                                                                                                                                                                                                            |     |
| [GDL 18]            | Recommendation to use secure boot wherever possible                                                                                                                                                                                                                                                                                                                                                                                                                    | 0/5 |
| Evaluation Comments | OneM2M does not cover secure boot in its documents.                                                                                                                                                                                                                                                                                                                                                                                                                    |     |
| [GDL 19]            | Recommendation to utilize anti-malware protection wherever possible                                                                                                                                                                                                                                                                                                                                                                                                    | 0/5 |
| Evaluation Comments | OneM2M does not cover anti-malware protection in its documents.                                                                                                                                                                                                                                                                                                                                                                                                        |     |
| [GDL 20]            | Update process never runs concurrently with other processes                                                                                                                                                                                                                                                                                                                                                                                                            | 0/5 |
| Evaluation Comments | OneM2M does not specifically refer to software updates.                                                                                                                                                                                                                                                                                                                                                                                                                |     |
| [GDL 21]            | Sensitive data and keys must be cleared after use                                                                                                                                                                                                                                                                                                                                                                                                                      | 0/5 |



|                     |                                                                                                                                                                               |     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Evaluation Comments | OneM2M does not specifically refer to software updates that would require clearing keys after use.                                                                            |     |
| [GDL 22]            | TRNG guideline                                                                                                                                                                | 0/5 |
| Evaluation Comments | OneM2M does not refer to TRNG.                                                                                                                                                |     |
| [GDL 23]            | TRNG guideline                                                                                                                                                                | 0/5 |
| Evaluation Comments | OneM2M does not refer to TRNG.                                                                                                                                                |     |
| [GDL 24]            | TRNG guideline                                                                                                                                                                | 0/5 |
| Evaluation Comments | OneM2M does not refer to TRNG.                                                                                                                                                |     |
| [GDL 25]            | Encryption algorithm guideline                                                                                                                                                | 5/5 |
| Evaluation Comments | OneM2M does not specifically refer to software updates, but in [5], section 8, OneM2M recommends various encryption algorithms for all messages/data communications payloads. |     |
| [GDL 26]            | Cryptographic hash algorithm guideline                                                                                                                                        | 5/5 |
| Evaluation Comments | In [5], section 10.1.1.1, OneM2M requires that the hash algorithm shall be SHA-256 for certificates.                                                                          |     |
| [GDL 27]            | Digital signature algorithm guideline                                                                                                                                         | 3/5 |
| Evaluation Comments | OneM2M discusses digital signature algorithm classes in [3], section 6.2.2.2.3, but does not provide specific guidelines.                                                     |     |
| [GDL 28]            | Key agreement guideline                                                                                                                                                       | 3/5 |
| Evaluation Comments | OneM2M discusses digital signature algorithm classes in [3], section 6.2.2.2.3, but does not provide specific guidelines.                                                     |     |
| [GDL 29]            | Key agreement guideline                                                                                                                                                       | 3/5 |
| Evaluation Comments | OneM2M discusses digital signature algorithm classes in [3], section 6.2.2.2.3, but does not provide specific guidelines.                                                     |     |
| [GDL 30]            | Recommended fields for digital certificate                                                                                                                                    | 5/5 |
| Evaluation Comments | In [5], section 10, OneM2M specifies the requirements for fields in the digital certificates.                                                                                 |     |
| [GDL 31]            | Digital certificate verification guideline                                                                                                                                    | 5/5 |
| Evaluation Comments | OneM2M requires that all digital certificates be validated.                                                                                                                   |     |
| [GDL 32]            | Recommendation to verify the before/after dates on each certificate                                                                                                           | 4/5 |
| Evaluation Comments | OneM2M discuss use of creationTime and expirationTime fields in authorization resources in [3] and [4].                                                                       |     |
| [GDL 33]            | Digital certificate revocation guideline                                                                                                                                      | 4/5 |
| Evaluation Comments | OneM2M discusses certification status verification and revocation in [5], section 8.1.2.2.                                                                                    |     |
| [GDL 34]            | Certificate Authority revocation guideline                                                                                                                                    | 0/5 |



|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Evaluation Comments | OneM2M does not discuss Certificate Authority revocation.                                                                                                                                                                                                                                                                                                                                                                                                                             |     |
| [GDL 35]            | Recommendation for network security between backend servers and the Gateway                                                                                                                                                                                                                                                                                                                                                                                                           | 5/5 |
| Evaluation Comments | <p>In [2], section 9.4, TLS is recommended for provisioning of credentials / tokens, particularly if TCP/IP is used. For distribution of tokens, DTLS is recommended.</p> <p>In [3], section 5.8.4, the description of data flow from devices to gateways and other architecture elements includes the required use of TLS and DTLS for security purposes.</p> <p>In [5], section 6, the use of TLS and DTLS is expected for all messages / data communications that are secured.</p> |     |
| [GDL 36]            | Recommendation to use point-to-point encryption whenever feasible                                                                                                                                                                                                                                                                                                                                                                                                                     | 4/5 |
| Evaluation Comment  | OneM2M recommends using encryption in [2], [3], [4] and [5] (i.e., all documents reviewed), however non-encrypted communication is also allowed.                                                                                                                                                                                                                                                                                                                                      |     |
| [GDL 37]            | Recommendation discouraging use of passwords                                                                                                                                                                                                                                                                                                                                                                                                                                          | 2/5 |
| Evaluation Comment  | OneM2M addresses use of username and passwords in [2] for access control functions, but does not explicitly discourage this use.                                                                                                                                                                                                                                                                                                                                                      |     |
| [GDL 38]            | Recommendation for compliant systems to use multifactor authentication                                                                                                                                                                                                                                                                                                                                                                                                                | 5/5 |
| Evaluation Comment  | In [5], Annex J, OneM2M describes the protection levels 3 and 4 that require the use of multi-factor authentication.                                                                                                                                                                                                                                                                                                                                                                  |     |
| [GDL 39]            | Recommendation for compliant systems to have a detailed KMP                                                                                                                                                                                                                                                                                                                                                                                                                           | 0/5 |
| Evaluation Comment  | OneM2M does not discuss KMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |
| [GDL 40]            | Recommendation for KMP to contain complete list of keys in the system                                                                                                                                                                                                                                                                                                                                                                                                                 | 0/5 |
| Evaluation Comment  | OneM2M does not discuss KMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |
| [GDL 41]            | Recommendation to generate all keys using a high-quality random number generators                                                                                                                                                                                                                                                                                                                                                                                                     | 0/5 |
| Evaluation Comment  | OneM2M does not discuss using high-quality random number generators for key generation.                                                                                                                                                                                                                                                                                                                                                                                               |     |
| [GDL 42]            | Recommendation for KMP to describe generation of all the keys in the system                                                                                                                                                                                                                                                                                                                                                                                                           | 0/5 |
| Evaluation Comment  | OneM2M does not discuss KMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |
| [GDL 43]            | Recommendation to store and back up all keys in an appropriate manner                                                                                                                                                                                                                                                                                                                                                                                                                 | 0/5 |
| Evaluation Comment  | OneM2M does not discuss storage and backup of keys.                                                                                                                                                                                                                                                                                                                                                                                                                                   |     |
| [GDL 44]            | Recommendation for KMP to describe how all the keys in the system are stored and backed up                                                                                                                                                                                                                                                                                                                                                                                            | 0/5 |
| Evaluation Comment  | OneM2M does not discuss KMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |     |
| [GDL 45]            | Recommendation to distribute all keys in a secure, authenticated manner                                                                                                                                                                                                                                                                                                                                                                                                               | 5/5 |
| Evaluation Comment  | OneM2M requires all keys to be distributed in a secure, authenticated manner, albeit not as part of a KMP.                                                                                                                                                                                                                                                                                                                                                                            |     |
| [GDL 46]            | Recommendation for KMP to describe how all the keys in the system are distributed                                                                                                                                                                                                                                                                                                                                                                                                     | 0/5 |



|                    |                                                                                                                                                                         |     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Evaluation Comment | OneM2M does not discuss KMP.                                                                                                                                            |     |
| [GDL 47]           | Recommendation for KMP to describe how all the keys in the system are used                                                                                              | 0/5 |
| Evaluation Comment | OneM2M does not discuss KMP.                                                                                                                                            |     |
| [GDL 48]           | Recommendation to have established procedures for updating keys                                                                                                         | 5/5 |
| Evaluation Comment | In [5], section 8.8.2.9, OneM2M documents the detailed procedure for updating expired keys.                                                                             |     |
| [GDL 49]           | Recommendation to have established procedures if an expired key or certificate is encountered                                                                           | 5/5 |
| Evaluation Comment | In [5], section 8.4.2, OneM2M describes procedures for dealing with expired keys, albeit not as part of a KMP. Other documents deal with handling expired certificates. |     |
| [GDL 50]           | Recommendation for KMP to describe which keys and certificates expire and will need to updated, and the procedures for doing so                                         | 3/5 |
| Evaluation Comment | OneM2M does not discuss KMP. It requires expirationTime in fields in the certificates, but does not discuss how to update them in a KMP.                                |     |
| [GDL 51]           | Recommendation for KMP to describe the behavior of the system if an expired key or certificate is encountered                                                           | 0/5 |
| Evaluation Comment | OneM2M does not discuss KMP, although there are procedures for dealing with expired keys and certificates.                                                              |     |
| [GDL 52]           | Recommendation to have established procedures for revoking and replacing keys and certificates                                                                          | 3/5 |
| Evaluation Comment | OneM2M has defined procedures for updating keys that have expired, albeit not in a KMP, and also does not mention any mechanism for revoking keys explicitly.           |     |
| [GDL 53]           | Recommendation to have established procedures if a revoked key or certificate is encountered                                                                            | 0/5 |
| Evaluation Comment | If an expired key is encountered, OneM2M will reject its use, although not in the context of a KMP.                                                                     |     |
| [GDL 54]           | Recommendation for KMP to describe procedures for revoking and replacing keys and certificates                                                                          | 0/5 |
| Evaluation Comment | OneM2M does not discuss KMP.                                                                                                                                            |     |
| [GDL 55]           | Recommendation for KMP to describe the behavior of the system if a revoked key or certificate is encountered                                                            | 0/5 |
| Evaluation Comment | OneM2M does not discuss KMP.                                                                                                                                            |     |

**Figure 2: OneM2M SOTA Software Update Evaluation Checklist**



## 4. SUMMARY OF EVALUATIONS

### 4.1 PLATFORM # 1: UPTANE

Uptane has specified an interesting software repository system. It could be a key component of an overall automobile security system if integrated with a robust key management framework. We believe strong cryptographic systems should start with a good key management framework, in which all the required keys and their management are specified. Security protocols for specific subsystems developed separately, without addressing key management, will be difficult to integrate into the entire system in a robust, flexible and resilient way.

### 4.2 PLATFORM #2: ONEM2M

OneM2M is a general security architecture rather than a specification for Secure Over-The-Air updates. A SOTA system could be designed based on the OneM2M Security Architecture, but functions specific to software updates would have to be added. Like Uptane, it leaves key management out of scope.

### 4.3 OTHER PLATFORMS CONSIDERED

FASTR examined specifications from the Open Mobile Alliance (OMA) to determine their applicability to secure over-the-air updates in vehicles. The OMA specifications are intended to define a framework for managing mobile devices, primarily phones. Although they define some authentication methods for the management protocols, they do not directly address the security of software updates. FASTR has determined that the security recommendations in the OMA specifications are not specific enough to software updates to be used as a standard by implementers. There is not enough detail to answer most of the guidelines FASTR considers critical [1]. Therefore, FASTR has not done a detailed cross-check between the OMA specification and the FASTR guidelines.

## 5. CONCLUSIONS

FASTR evaluated two SOTA software update systems from Uptane and OneM2M. The Uptane system was specific to managing software updates, while the OneM2M system was a more general security architecture. We believe either could be used as a basis for implementing secure software update systems for the automotive industry.

The main omission in both systems is robust key management. We would like to see more focus on developing good key management practices for the automobile industry as a whole. We also



recommend analyzing a third system in greater detail and will subsequently work on solutions and guidelines to address the common missing elements in those three systems, most notably a key management framework.

## 6. REFERENCES

- [1] *FASTR, Automotive Industry Guidelines for Secure Over-the-Air Software Updates, v1.0, October, 2017*
- [2] *FASTR, Uptane Secure Over-the-Air Software Update System Evaluation, v0.02, July, 2017*
- [3] *Uptane, Uptane Design Overview, v2017.01.13*
- [4] *Uptane, Uptane Implementation Specification, v2017.04.03*
- [5] *FASTR, OneM2M Secure Over-the-Air Software Update System Evaluation, <October, 2017>*
- [6] *OneM2M Security, TR-0008-V2.0.0, August 30 2016.*
- [7] *OneM2M End-to-End Security and Group Authentication, TR-0012-V2.0.0, August 30 2016.*
- [8] *OneM2M Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies, TR-0016-V-2.0.0, August 30 2016.*
- [9] *OneM2M Security Solutions, TS-0003-V2.4.1, August 30 2016.*

*We welcome suggestions for improvements to this document. Please contact us at [info@fastr.org](mailto:info@fastr.org)*

## COPYRIGHT AND OTHER LEGAL INFORMATION

This document is provided for informational purposes only, on an "AS IS" basis. FASTR Inc. and its members and agents disclaim all liability arising from use of the information in this document; readers use the information at their own risk.

Third party company, product and service names used in this document are for identification purposes only. Use of these names, logos, and brands does not imply endorsement. These names are the property of their respective owners.

FASTR and FASTR's chevron logo are service marks of FASTR Inc. and may only be used with FASTR's permission.

Copyright © 2017 FASTR, Inc. Contact FASTR at [info@fastr.org](mailto:info@fastr.org) for permission requests.

