EUROSMART
The Voice of the Digital Security Industry

[TR-e-IoT-SCS-Part-8]

Metadata Certification Policy

Pilot – v1.2

RELEASE

Editor: Isaac Dangana – Red Alert Labs

Contributors & Reviewers: François Guerin – Thales, Alban Feraud – Idemia, Rachel Shabat – Winbond, Juergen Noller – Infineon, Sebastian Colle – Infineon, Steffen Heinkel – Infineon, Jonas Andersson – Fingerprint, Eric Vetillard – NXP, Sylvie Wuidart – STM, Jan Eichholz – G&D, Christine Crippa-Martinez – Thales, Ayman Khalil – Red Alert Labs, Sreedevi Beena – Red Alert Labs

Approved by: Martin Schaffer – SGS, Philippe Proust – Thales, Gisela Meister – G&D, John Boggie – NXP, Stefane Mouille – Cabinet Louis Reynaud

EXECUTIVE SUMMARY

The IoT devices ecosystem could be very dynamic. Vendors could be constantly updating their IoT applications and devices or replacing simply replacing them. Vulnerabilities could be also discovered in existing certified IoT devices, requiring that their use be limited to reduce the cybersecurity risks or sometimes to be revoked.

A responsible IoT Solution user or service provider must be able at anytime to monitor the certification status of all certified IoT devices in order to manage efficiently the risks.

For this reason, Eurosmart defined the metadata certification concept allowing e-IoT-S certificates consumers (e.g. IoT Service Providers, Integrators, End-Users) to run efficient security policies (e.g. Access Controls, Vulnerability Management, Assurance Continuity, etc.) on IoT Devices that are certified under this scheme.

Date	Version	Description of changes
07/01/19	V0.1	Initial version created
07/04/19	V0.2	Updates related to terms and definitions
31/05/19	V1.0	BETA RELEASE
06/08/19	V1.0.1	Addition of BASIC level
21/10/19	V1.2	PILOT RELEASE

1 Contents

1 INTRODUCTION

This document describes the fields that constitutes the metadata certification statement (MCST) and how the metadata certification service (MCSE) operates.

1.1 Disclaimer

EUROSMART and all related entities, provide all materials, work products and, information ("TECHNICAL REPORTS") AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workman like effort, of lack of viruses, and of lack of negligence, all with regard to the TECHNICAL REPORTS, and the provision of or failure to provide support or other services, information, software, and related content through the TECHNICAL REPORTS or otherwise arising out of the use of the TECHNICAL REPORTS.

ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE TECHNICAL REPORTS.

WITHOUT LIMITING THE FOREGOING, EUROSMART DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THESE TECHNICAL REPORTS ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE TECHNICAL REPORTS AVAILABLE, EUROSMART IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS EUROSMART UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE.

ANYONE USING THIS TECHNIAL REPORT SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EUROSMART OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE TECHNICAL REPORTS, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE TECHNICAL REPORTS OR OTHERWISE ARISING OUT OF THE USE OF THE TECHNICAL REPORTS, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THESE TECHNICAL REPORTS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF EUROSMART OR ANY SUPPLIER, AND EVEN IF EUROSMART OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1.2.1 General References

Reference	*Name/Description*
[ISO/IEC 15489]	Information and documentation -- Records management 2016

1.2.2 Requirements & Evaluation

Reference	*Name/Description*
[TR-e-IoT-SCS-Part-1]	E-IoT-SCS Certification Scheme Process & Policy - This document defines the policies and processes that govern the IoT device certification scheme.
[TR-e-IoT-SCS-Part-2]	E-IoT-SCS Generic Protection Profile - This document is a generic representation of common security requirements on IoT devices. It is based on a security risk analysis approach of an IoT Device operating in a typical infrastructure without considering a specific type of data or a context for risk calculation. The main output of this document is a list of security goals and requirements qualifying the need to counter security threats identified on a typical IoT device.
[TR-e-IoT-SCS-Part-3]	E-IoT-SCS Evaluation Methodology - Document defining the evaluation activities to be performed by an evaluator and links between them in order to conduct properly an evaluation. It lists evaluation evidences required to perform actions as defined in the security assurance requirements. It defines way to report evaluation results in Evaluation technical report and observation report. It also provides rules to define verdict and criteria of failure.

1.2.3 CABs Accreditation

The following documents describe how to become an Accredited CAB

Reference	*Name/Description*
[TR-e-IoT-SCS-Part-4]	CABs Agreement - Guidelines listing the rules for setting up agreement between CABs and Certification Scheme stakeholders (e.g. other CABs – CAB reviewer, CAB evaluator, NABs, etc.)
[TR-e-IoT-SCS-Part-5]	CABs Accreditation Policy - Guidelines describing policy for CABs accreditation

1.2.4 Certification Secure Life-Cycle Management

Reference	*Name/Description*
[TR-e-IoT-SCS-Part-6]	Vulnerability Management, Maintenance & Continuous Assurance Policy: Document describing vulnerability management procedures and the life-cycle management of the Certificate after issuance

[TR-e-IoT-SCS-Part-7]	Mark & Certificate Usage Policy for e-IoT Certification Scheme: Document describing the procedure and conditions which govern the use of the e-IoT BASIC and SUBSTANTIAL mark and certificate by IoT device vendors, CABs and end-users
[TR-e-IoT-SCS-Part-8]	The Metadata Certification Policy for e-IoT Certification Scheme: Document describing the Metadata Certification Concept and Requirements guaranteeing the relevancy and Authenticity of the Certificates.

1.2.5 Supporting Documents

Reference	*Name/Description*
[TR-e-IoT-SCS-Part-9]	Templates (Vendor Questionnaire, Impact Analysis Report, Security Profile, Evaluation Report, Mapping Table Concept)
[Informative Annexes]	A set of informative annexes complementing the e-IoT Security Certification Scheme deliverables such as the "e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE", or "Risk Assessment Methodologies".

1.3 Terms and Definitions

Refer to **[TR-e-IoT-SCS-Part-1]**, Section 1.4

1.4 Abbreviations and Notations

Refer to **[TR-e-IoT-SCS-Part-1]**, Section 1.5

1.1 Audience of this Document

The intended audience of this document are mainly Vendors, CABs and IoT Service Providers.

1.5 Support

For help and support, contact e-IoT-SCS@eurosmart.com

1.6 Notes

- IOT Devices with no attestation/self-attestation root certificate can be included in the metadata. This is not recommended but in this case the verification could still be done onto the characteristics of the IoT device but with no crypto proof.
- This version of the document is setting up the principles, it is expected to be completed once the service is ready to be published. Nevertheless, the metadata certification statements must be provided by all vendors going through the certification process and validated by CABs.

1.7 Metadata Definition

Metadata has been defined as "data describing the context, content and structure of records and their management through time" in the **[ISO/IEC 15489]**. It is an inextricable part of managing records in

any format. The use of metadata supports methods to identify, authenticate, describe, locate and manage resources in a precise and consistence way that meets business, accountability, and archival requirements.[1]

2 IoT Metadata Certification Statement (MCST)

A metadata statement is a document containing information about a device's characteristics, features and capabilities arranged in a structured manner that can be read and understood by service providers. The reporting format of the metadata statement is generic and therefore can be used to describe any device from any vendor.

The information can include details starting from the layers of the ToE(x) to the outer description of the device including its name and specification. The different layers are:

- IoT HW (hardware),
- IoT ROE (Restricted Operating Environment),
- IoT Core,
- IoT Application and Mobile Application.

Thus, the following metadata statement fields are defined in different categories: "General", "IoT Core", "IoT ROE", "IoT Hardware", "Sensor", "Extended ToE", "Certification", "CAB-Determination/Evaluation", "CAB-Review/Decision". Each category can have several fields.

2.1 Metadata Statement Fields

Category	Field	Description
General	**GEN.Description**	A human-readable short description of the IoT device.
	GEN.Device.version	Metadata service must also change this Device Version if the update fixes severe security issues, e.g. the ones reported by preceding Certification Status.
	GEN.ToE.Type	This field must be filled with the information that whether the ToE includes or excludes extended ToE. ("ToE"/" ToEx").
	GEN.device.ID	This field must be filled with the identification number of the device.
	GEN.Product.CommercialName	(Optional) If the device possesses a commercial name, given by the vendor, the

[1]https://committee.iso.org/files/live/sites/tc46sc11/files/documents/N800R1%20Where%20to%20start-advice%20on%20creating%20a%20metadata%20schema.pdf

		vendor can document it in this field.
	GEN.device.operationalenvironment	This field must define the operational environment where this device is going to be used.
	GEN.device.VendorName	This field must be described with the vendor's name.
	GEN.device.userInterface	If the device possesses a user interface, this field must be filled with all the types of interfaces it has. The interface can be a screen(touchscreen/normal), keypad, button, etc.
	GEN.device.authentication	If the device is enabled with self-authentication. E.g.: two factor authentications. (Yes/No)
	GEN.e-IoT-Certification.ID	If this field is empty, it is presumed that the device is not certified.
	GEN.e-IoT-Certification.startdate	This field must be completed with the start date of e-IoT certification, if the device already possesses it.
	GEN.e-IoT-Certification.enddate	This field must be completed with the end date of e-IoT certification, if the device already possesses it.
IoT Core	**CORE.ConnectivityProtocol**	The protocol which the device will be using for getting connected. E.g.: Wi-Fi, ZigBee, Bluetooth, Z-wave, LoRAWAN etc.
	CORE.Cloud	If the device supports cloud connectivity. (Yes/No)
	CORE.driverVersion	For all the drivers used inside the device, complete this field with the names and corresponding version of the drivers.
IoT ROE	**IoTROE**	If the device possesses a ROE? The ROE can consist of a

		secure storage, secure boot, access control policy, isolation of applications, resistance to physical/local attacks, resistance to all types of attacks, etc.
IoT Hardware	**IoTHardware**	This field must define the elements constituting the Hardware of the device/type of hardware. This can include SE, SoC, TEE, etc. The type can be Embedded devices, Linux based devices, Resource constraint devices, microcontroller devices with flash/firmware, etc.
Sensor	**Sensor.type**	This field must describe all the types of sensors used in the device. This can include biometric sensors, IR sensors, temperature sensor, etc.
ExtendedTOE	**ToEx.MobileApplication**	If the device supports mobile application, please complete this field with an "Yes" or "No"
	ToEx.MobileApplication.protection	Is the communication channel encrypted by default? (Yes/No)
Certification	**Certification.status**	This field must be filled with the current certification status of the device. The five status a device certification can possess are "Active", "Confidential", "Suspended", "Certified", "Withdrawn".
	Certification.startdate	This field must be filled with the certification start date, if the device is certified.
	Certification.enddate	This field must be filled with the certification end date, if the device is certified.
CAB-Determination/Evaluation	**CABE.name**	This must be filled with the name of the CAB-R who carried out the evaluation activities.
	CABE.contact	This must be filled with the contact details of the CAB-R who carried out the

		evaluation/determination activities.
CAB-Review/Decision	**CABR.name**	This must be filled with the name of the CAB-E who carried out the review activities.
	CABR.contact	This must be filled with the contact details of the CAB-E who carried out the review/decision activities.

Note: This table is expected to include more fields in the future to allow a more efficient communication on the value of the certificate and the scope of coverage. For instance, it will show the list of requirements that were not applicable on a specific product allowing risk-owners to set up adequate security policies.

3 IoT Metadata Certification Service (MCSE)

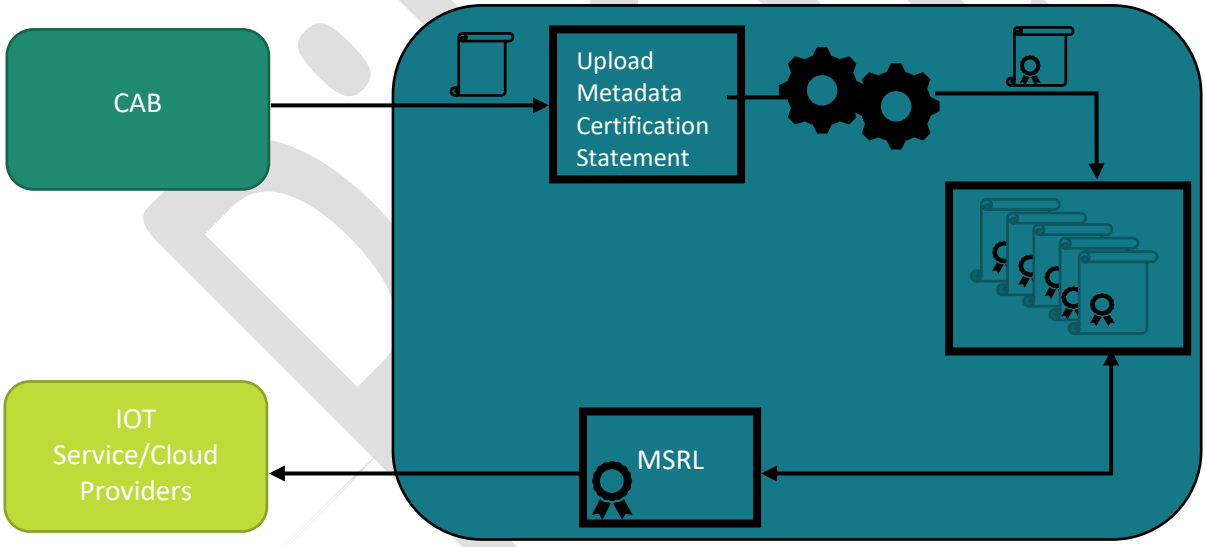

Figure 1: Metadata Certification Service Model

Service Providers for IoT Devices will naturally want to be able to trust a device that attempts to make use of their services this makes the deployment of "device metadata service" very useful, secure and scalable in quickly determining if a specific device model is trustworthy to access a resource.

3.1 CABs responsibilities

The metadata service is a web-based tool where CAB-R [2]can, on behalf of device vendors, upload signed metadata statements for service providers to access and use as a source of trusted information about a specific device model. CAB-Rs are preferred as the entity responsible for uploading the Metadata statement because they are expected to have verified the existence and correctness of the

[2] Note that this service could be provided by a CAB-E if during accreditation it was explicitly included in the scope of accreditation.

device functionality during the certification process and therefore will be better placed to sign & upload the metadata statement.

3.2 Process description

The metadata service maintains a signed, autogenerated list (Metadata Statement Reference List, **MSRL**), containing the URL of each "**approved**" metadata statement received from CABs. The MSRL serves as the starting point of a statement download process whereby service providers locate the URL of a target metadata statement and its corresponding hash. After the statement is accessed, the service provider re-computes the hash to verify the statement's integrity.

When a vendor's metadata statement is received, the metadata service verifies the statement's CAB certificate, and at this point, the statement becomes "**approved**". The statement's URL and hash is subsequently added to the MSRL which is published to the online metadata service, making it available to all users (service providers).

The MSRL is updated frequently to ensure that statements with expired/revoked certificates are deleted. The checks for MSRL signing certificates is based on Certificate Revocation List (CRL). The CRL also has a maximum lifetime which is published at a fixed frequency.

Vendors retain ownership of their product's metadata statements and can request to have the statement removed from the metadata service. The integrity (i.e signing) of the MSRL is done by the organisation charged with maintenance of the metadata service.

4 How to Publish a Metadata Statement

To publish a metadata statement, a vendor must first apply for an account with a CAB-R which potentially is the one who certified their product. Once an account has been set up, the vendor can then create and submit a metadata statement according to the requirements defined in this document.

4.1 Where is it hosted ?

The metadata statement can either be hosted by the vendor on their chosen web site or submitted directly to the CAB-R server for publishing. If the statement is self-hosted, the vendor submits the URL of its location to the CAB-R server.

Once a vendor submits a metadata statement, a series of actions are undertaken by the CAB-R before publishing. These actions are undertaken in two steps by two different individuals to maintain a segregation of duties.

Step 1

Each submission to the CAB-R server is verified for syntactic correctness and validity. The following are validated in the submitted metadata statement:

- The identity of the submitter and his affiliation with the IoT device vendor company.
- The certification status of the IoT device and the associated fields in the metadata statement.
- The IoT device ID for which the statement was submitted belongs to the submitter's company.

Once the submission has been verified, the metadata MSRL is prepared as follows:

- The hash value of the metadata statement is computed.
- The metadata MSRL sequence number is created.

- Any status updates on the authenticator are added (such as when the IoT device was certified).
- The nextUpdate date of the metadata file which also indicates the expiration date of the current submission is added.
- If the metadata statement is to be hosted by the MDS, a URL where it is hosted is also created. This updated MSRL data is then digitally signed using designated signing keys on behalf of CAB-R in a secure facility.

Step 2

The newly signed MSRL data is re-verified for the updated content and then it is published to the designated web location[3]. Finally, all the affected vendors of this publication are notified of the publication event.

4.2 Security Precautions for Signature Generation

For signature computation, several security processes and precautions could be implemented. The signature is not generated on the system where the CAB-R server is running. Rather, a stand-alone (not connected to internet) system is used for this step. The signature is performed using a private key that is kept in a secure hardware token. An HSM-like solution is used for key generation and signing of the MSRL.

The root and issuing CA's are managed in a secure facility by a third-party public CA. Any and all access to the token and the computing environment are logged and audited.

All access to the systems are authenticated. Segregation of duties is maintained between Step 1 (Signing) and Step 2 (Publishing) of the metadata SMRL and statement. Controls are in place to preserve data integrity of the submitted metadata at every step of the process and the metadata MSRL is verified again before the final publishing step.

[3] To be provided after Pilot phase

5 About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

6 Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Renaud**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.