EUROSMART
The Voice of the Digital Security Industry

Technical Report

[TR-e-IoT-SCS-Part-6]

Vulnerability Management, Maintenance & Continuous Assurance

Pilot – v1.2

RELEASE

Editor: Roland Atoui – 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

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

Pilot

Date	Version	Description of changes
05/12/18	V0.1	Initial version created
10/12/18	V0.2	Completed Chapters 2 and 3
17/12/18	V0.3	Completed Chapters 4, 5 and 6
18/12/18	V0.4	Including comments from Certif Scheme TF members conference-call
05/02/19	V0.5	Updates on Roles & Responsibilities + Taking into account comments from the last call
27/05/19	V0.6	Updates on Roles & Responsibilities + update vulnerability management process + preparation for final delivery
30/05/19	V1.0	BETA RELEASE
06/08/19	V1.0.1	Addition of BASIC level
26/09/19	V1.1	Including comments from NXP
21/10/19	V1.2	PILOT RELEASE

pilot

1 Contents

Pilot

1 Introduction

In this document we introduce a risk-based vulnerability management which is the process in which vulnerabilities in the ToE are identified and their related risk is evaluated. This evaluation leads to correcting the vulnerability thus reducing, removing or accepting the risk.

The vulnerability management workflow is defined as follows:

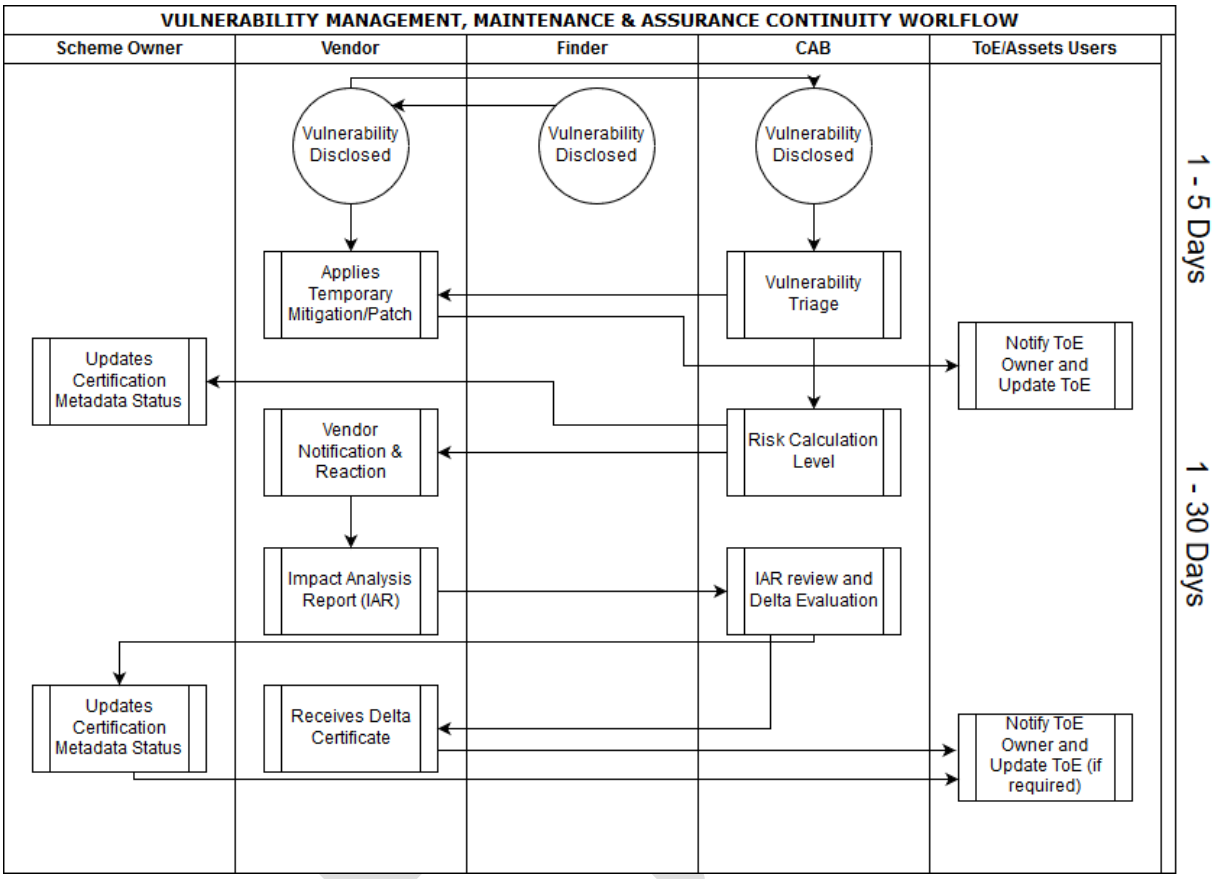

Figure 1: Vulnerability Management, Maintenance and Assurance Continuity Workflow

FAQ 1.1

Q1.1: which actions of the "CAB column" of the Figure 1 ***shall be executed by CAB-E and CAB-R?***

R1.1: *The role of each CAB in the vulnerability management process is detailed in this document in each concerned section.*

Example: Section 2.1.3-Active Monitoring*:*

- *This responsibility is agreed on by CAB-R and CAB-E upon each certification*

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 17000:2004]	Conformity assessment — Vocabulary and general principles
[ISO/IEC 17065:2012]	Conformity assessment — Requirements for bodies certifying products, processes and services
[ISO/IEC 17067:2013]	Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
[EU Cybersecurity Act]	European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

[ISO/IEC 15408]	Common Criteria for Information Technology Security Evaluation (Part 1-3)
[ISO/IEC 18045]	Information technology -- Security techniques -- Methodology for IT security evaluation
[ISO/IEC 17025]	General requirements for the competence of testing and calibration laboratories
[ISO/IEC 30111:2013]	Information technology -- Security techniques -- Vulnerability handling processes
[ISO/IEC 29147:2014]	Information technology -- Security techniques -- Vulnerability disclosure
[IoTSF-Vulnerability]	IoT Security Foundation - Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies
[IoTSF-Patch]	IoT Security Foundation - Patching Constrained Devices

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

1.5 Audience of this Document

The primary audience of this Vulnerability Management, Maintenance and Continuous Assurance are vendors[1] developing IoT devices and CABs (both evaluators and reviewers) undergoing the E-IoT-SCS Certification process.

It is intended to help them understand the process from vulnerability disclosure to patching to updating the certificate accordingly.

[1] A vendor could be an integrator[1] of different components purchased from other vendors.

1.6 Support

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

1.7 Roles & Responsibilities

Scheme Owner	This could be embodied by Eurosmart or ENISA for instance.
ToE/Asset User	Users of IoT devices, and may refer to individuals, organisations or governments.
Vendor	Vendors that comprise the developers, manufacturers and suppliers of IoT Devices. This may also include so-called "intermediate vendors/OEMs" that make up the supply chain of a specific product or service.
Finders	Finders who make up the community of individuals that identify and report vulnerabilities. Finders are sometimes also referred to as discoverers, reporters or researchers.
Government	play a complex role in the vulnerability disclosure process. They can act as finders, vendors and coordinators, as well as acquire or maintain vulnerabilities for national security purposes. Governments also develop legislation and regulations that may influence vulnerability disclosure. NCAs, NABs, National Certification Bodies
Coordinators	Coordinators are trusted organisations that act as intermediaries between finders and vendors to ensure that vulnerabilities are disclosed and mitigated responsibly. Well-known coordinators include CSIRTs, CERTS
CAB Reviewer (CAB-R)	1. Inspects product samples taken either from the point of production, or from the market, or from both for conformity with the certified type. 2. Verifies the validity of the 3rd party compliance certificate covering the production process and auditing of the management system, including examination of the vendor's quality records relating to the production process. 3. Monitors actively the latest reported security vulnerabilities impacting the ToE, following the EU CSIRT sources for security alerts. (This responsibility is agreed on by CAB-R and CAB-E upon each certification)
CAB Evaluator (CAB-E)	1. Tests product samples taken either from the point of production, or from the market, or from both to check that they fulfil the specified requirements; 2. Monitors actively the latest reported security vulnerabilities impacting the ToE, following the EU CSIRT2 sources for security alerts. (This responsibility is agreed on by CAB-R and CAB-E upon each certification)

[2] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

2 Vulnerability Identification/Disclosure

2.1.1 Definition of a Security Vulnerability

For the purposes of this document a security vulnerability is a flaw within the ToE related to software and/or hardware that can cause it to work contrary to its documented design and could be exploited to cause the ToE to violate the security requirements defined the Security Profile.

The following proposed process is based on the international standard for disclosing a vulnerability as outlined in **[ISO/IEC 29147:2014]**.

2.1.2 Means for Contact

Vendors must provide means for contacts allowing researchers or other entities who discovered a new vulnerability to notify them.

A typical webpage text could be as follow:

> *"[Company Name] takes security issues extremely seriously and welcomes feedback from security researchers in order to improve the security of its products and services. We operate a policy of coordinated disclosure for dealing with reports of security vulnerabilities and issues. To privately report a suspected security issue to us, please send an email to security-alert@<companydomain>, giving as much detail as you can. We will respond to you as soon as possible. If the suspected security issue is confirmed, we will then come back to you with an estimate of how long the issue will take to fix. Once the fix is available, we will notify you and recognize your efforts on this page.*
>
> *Thank You*
>
> *Thanks to the following people who have helped make our products and services more secure by making a coordinated disclosure with us: [Name/alias, Twitter handle]"*

The communication means provided must allow a secure exchange of information which could be a part of the "flaw remediation" evaluation procedure.

It is strongly recommended that CABs Reviewers are notified as soon as the vulnerability has been submitted. Transferring automatically the security-alert email or submitted form to the CAB-R is encouraged to reduce the time spent on this process.

2.1.3 Active Monitoring

CABs[3] should monitor, at a minimum, CSIRTs websites for security alerts such as the one listed by ENISA:

https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

2.1.4 Bulletins and Alerts

Based on the analysis of identified vulnerability, Vendors may issue security bulletins or alerts thus notifying consumers and ToE owners.

[3] This responsibility is agreed on by CAB-R and CAB-E upon each certification

Pilot

2.2 Confidentiality

The information on a new vulnerability will be handled with the highest confidentiality until it has been assessed and its severity determined according to the traffic light resulted from the vulnerability triage process.

3 Vulnerability Triage & Risk Calculation

Should the CAB-R be notified of or identify a vulnerability it should triage the severity of the vulnerability and send notifications based on Traffic Light Protocol[4].

The Vulnerability Triage step is the first step of the Vulnerability Assessment process and is used as a quick pre-selection process to help determine which groups should be notified, and how quickly the vulnerability needs to be assessed by the CAB-E including its impact on the certificate status.

A temporary mitigation/patching shall be applied by the vendor no matter what according to the value of Table 2.

The Vulnerability Triage Protocol is defined in Table 2. It follows the steps listed below:

1. A Vulnerability is identified,
2. CAB-R will kick off the Triage Action according to the "Triage Reasoning" described in Table 2. A vulnerability level (Red, Amber, Green or White) is assigned in order to determine how the vulnerability should be managed.
3. Vendor to apply temporary mitigation/patching after being notified by CAB-R according to the assigned triage level and the information in Table 2. CAB-R notifies CAB-E in order to assess the impact of the vulnerability within the expected time specified in "Risk calculation" column of Table 2 following the risk assessment model adopted for this framework. The outcome of this assessment, will be used to determine the next course(s) of action which includes the following:
    a. The vulnerability does not impact the ToE at all (or not in any significant way), the next action is to inform the vendors & customers of this conclusion.
    b. The vulnerability impacts the target and based on the risk assessment model adopted for the scheme, a risk level.

    The risk is calculated according to the methodology defined in the **GENERAL PROTECTION PROFILE [TR-E-IOT-SCS-PART-2]**. CAB-E shall try to map the vulnerability to an existing threat of the security profile as a first step before imagining new scenarios.
4. CAB-E notifies CAB-R about the results of the risk calculation and qualification.
5. CAB-R to decide whether the vulnerability affects the basic/substantial certificate or not. CAB-R to notify Vendors in order to patch according to the information in the Table 1 below.
6. [Optional] In case of a full attack identification, CAB-R could ask CAB-E for a full attack quotation.

[4] https://en.wikipedia.org/wiki/Traffic_Light_Protocol

Total Risk	Vulnerability Triage Protocol (Permanent Patch Deadline)
HIGH	RED
SUBSTANTIAL	AMBER
BASIC	GREEN
Out of the Scope	WHITE

Table 1: RISK Level mapping to Vulnerability Triage Protocol in Order to Apply Permanent Patch

Below an example of a global scenario:

1. CAB-R is notified about a new identified vulnerability,
2. CAB-R kick-off the Triage Action and assign the vulnerability as **AMBER**:" *Vulnerability that is likely lead to a scalable attack. e.g. Software to exploit the vulnerability is available*."
3. CAB-R notifies the Vendors. Vendors starts implementing and applying the temporary mitigation/patching according to the **AMBER** "Temporary Mitigation/Patching Deadline" = 3 business days. CAB-R notifies CAB-E to start the risk calculation according to the deadline defined in Table 2= 5 business days and identifies the risk as **BASIC**,
4. CAB-E notifies CAB-R and Vendors about the results of the risk calculation that were linked to an existing threat of the security profile.
5. CAB-E qualify that the vulnerability affects the basic and substantial certificate. CAB-R notifies vendors to patch the product according to the **BASIC** "Permanent Mitigation/Patching deadline"= 30 Business days.
6. [Optional] As no full attack potential was identified, CAB-R didn't ask for a full attack quotation.

Triage Level	Triage Reasoning	Temporary Mitigation/Patching Deadline	Permanent Mitigation/Patching Deadline	Risk Calculation Deadline[5]
RED Not for disclosure, restricted to participants only	Attack in progress OR At-scale attacks exist that can be performed with	1 business day	10 business days	3 business days

[5] The CVSS (Common Vulnerability Scoring System) was not considered because it does not take into consideration the impacts related to the specific IoT operational environments.
Example: CVSS scoring doesn't consider the "safety, authenticity and scalability" impact categories.

	readily available tools and limited skill. e.g. Actual attacks against this ToE have been carried out			
AMBER Limited disclosure, restricted to participants' organizations	Vulnerability that is likely lead to a scalable attack. e.g. Software to exploit the vulnerability is available	3 business days	20 business days	5 business days
GREEN Limited disclosure, restricted to the community.	Vulnerability where attack unlikely, or not scalable. e.g. Researcher finds a theoretical flaw that requires special / new tools to carry out the attack.	10 business days	30 business days	14 business days
WHITE Disclosure is not limited.	Vulnerability that is outside the scope of the ToE.	n/a	n/a	n/a

Table 2: Vulnerability Triage Protocol

If the vendor decides not to issue a fix for a vulnerability, this triggers a count-down of 48h after the deadline is passed towards the certificate revocation of the targeted product version.

The CAB-R considers what action to take regarding the certificate validity according to the **SCHEME PROCESS AND POLICY [TR-E-IOT-SCS-PART-1].**

The Vendor keeps a record of any complaints relating to compliance with the certification requirements and documents the remedial actions taken. The client makes the records available to the CAB-R on request. If non-conforming products have been released onto the market, the Vendor informs the CAB-R so that it can agree on the action to be taken.

Pilot

3.1 Temporary Mitigation/Patching

The temporary mitigation/patching phase is mandatory in the process. It allows to secure a first level of security before evaluating the risk related to each vulnerability.

This scheme allows to patch the ToE first and evaluate later and the condition that the developer demonstrated a secure maintenance life-cycle process satisfying the flaw remediation requirements.

Since its very common to require a large amount of time to deploy a definitive update/patch for the vulnerability, temporary measures will be deployed by the vendor within the time as specified in the Vulnerability Triage Protocol.

3.1.1 Patching Securely

The delivery process of the temporary patch must be secure and signed by the Vendor accordingly. There are also organisational and management practices that need to be considered. These include the secure storage and management of cryptographic keys used for patching, development and maintenance of patching policy, the infrastructure required for security monitoring and incident response and even changes that may be required to the production process.

There are several requirements for ensuring a secure patch management process[6], to avoid malicious update of the ToE, these include:

Authenticity	Authentication of patching can be achieved by implementing code signing during patch release and secure boot during boot-up of devices. Typical activities of code signing for embedded devices include generation of platform specific signature, proper protection of private code signing key across its use and distribution.
Bootstrap and Trusted Channel	A "bootstrap" mechanism for providing initial parameters on the device so that it can be brought under management and a "Trusted Relationship" between the device and management server established
Remote Access enabled	A process for adding information about the device to the management server so that remote access and management of the device is achievable
Unique ID	Support a unique ID to identify the device
GET STATUS	Support the remote retrieval of the installed firmware name and version of the device
Secure Communication	Support secure communication between the device and the server managing the update
Mutual Authentication	Support a mechanism for mutual authentication between the device and the server managing the update
Firmware update	Support a mechanism to authorise the firmware update
Firmware update Integrity	Support a mechanism for ensuring the integrity of the firmware update (includes firmware code integrity).
Confidentiality	Support a mechanism for confidentiality
Anti-Downgrade	Support a mechanism to prevent a downgrade attack

[6] These requirements where defined by the IoT Security Foundation WG3 – Patching Constrained Devices

From the date a vendor is notified, he will have 1month to provide a temporary fix (eg in 3.1.1) or a permanent fix altogether.

3.1.2 ToE Owner Notification

There should be a mechanism where Security Advisories are issued to the ToE Owners to notify them of latest fixes/patches for a vulnerability (whether temporary or permanent).

pilot

3.2 Risk Calculation

3.2.1 Application vs Platform

As a platform-level certification, vulnerabilities emanating from higher layers (application-level) will be assessed and evaluated with regards to how it affects the platform/ToE as defined in this Scheme.

Note that in case the ToE is extended to include the IoT application and Mobile application (please refer to the ToE extended definition in the **GPP [TR-E-IOT-SCS-PART-2]**) and the update is related to the application layer, patching with Integration mechanisms could be verified once by the CAB-R during the certification process. In that case, vendors can securely update the application while preserving the validity of the certificate.

4 Vendor Notification & Reaction

Once a vulnerability has been assigned a Risk Level, the CAB-E shall notify the CAB-R who will notify the Vendor. The Vendors or Products impacted by a Security Vulnerability will never be shared outside of the CABs.

Risk Calculation could be re-evaluated more than once during the lifecycle of a vulnerability. In the case that the risk is updated (for example, from Severe to Moderate) a new Notice will be sent to the vendor with the new Risk calculation. When a Notice is distributed it voids any previous notices and restarts the Vendor Response and the Permanent Mitigation step.

4.1 Permanent Mitigation

Upon receiving notice from the CAB-R, the Vendor will be required to respond back within 48h.

Within the Vendor Deadline for "Permanent Mitigation" in Table 2, the Vendor has the option to correct the implementation and show their intent to remain certified by filing an application for a Delta Certification. If the Vendor chooses not to make any corrections to their implementation the vendor may request Revocation by filing a Revocation Request.

If the Vendor does not agree with the assigned Risk Calculation of the vulnerability, the Vendor may file a Dispute Report with the CAB-R.

Note: Filing the Application, Request, or Dispute is the beginning of the respective processes and all that is required to fulfil the Permanent Mitigation requirements. Permanent Mitigation means that the process to maintain the Certification against the Security Vulnerability has been started, but completing the entire process is not required within the Deadline for Permanent Mitigation.

5 Delta & Derivative Certification

The Delta and Derivative Certification are intended to simplify the maintenance of the certificate and minimize the costs when certifying a family of IoT devices. The criteria are defined in the Impact Analysis Report provided in **[TR-E-IOT-SCS-PART-9]** allowing, when possible, a straightforward judgement on the nature of the changes.

- A "Major" change will require a full recertification,
- a "Minor" change will require a Delta certification relying on existing artefacts and
- a "Non-Interfering (with the security requirements)" change will be required only a new stamp.

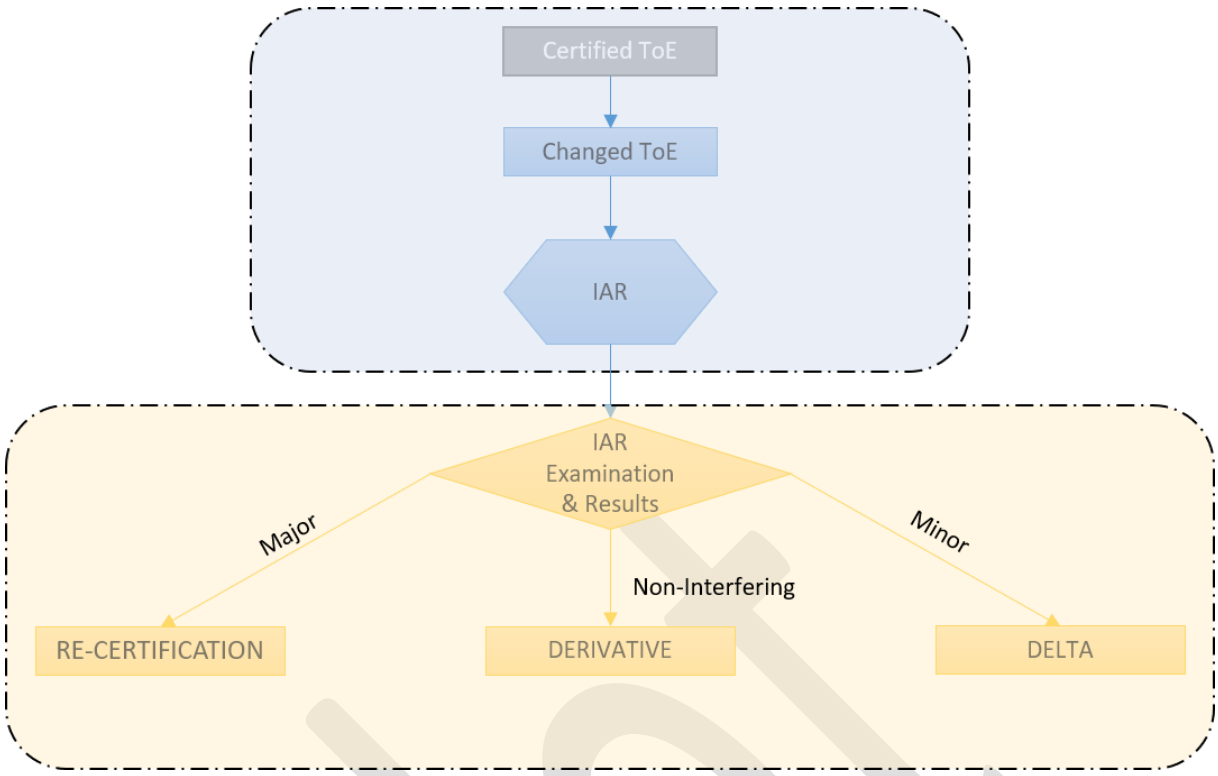

Figure 2: Impact Analysis Report - Delta & Derivative Concepts

Vendors with proven capabilities in processing vulnerability disclosure, upgrades and incident response could be granted a full autonomy in processing an internal Impact Analysis Report and applying adequate actions to preserve active status of their certificate.

To acquire a full autonomous delta & derivative certification capability a Vendor must go through the following steps:

Process Step	Responsible Party	Process Steps
REQUEST	Vendor	Fills-in the Vendor Processes Assessment Application that could be found in **[TR-e-IoT-SCS-Part-9]**. This application contains all the requirements on the development environment and processes that the vendor should put in place before and after issuing the ToE.
	Vendor	Submits it to a qualified CAB
	Vendor & CAB	(Optional) Completes mutual NDAs, signs a Certification agreement, pays necessary fees, signs certification mark agreement, etc.
REVIEW	CAB	Reviews the Application for completeness, communicates with the Vendor as needed to clarify any questions. Approves the Application when it meets all requirements
	CAB	(OPTIONAL) In case the application requires an audit or a re-audit, the CAB makes the necessary arrangements with the Vendor for the assessment in accordance with the Vendor Processes Assessment Requirements defined in **[TR-e-IoT-SCS-Part-6].** The goal is to ascertain if the vendor enforces required physical, procedural, personnel, and other security measures that are necessary to

		protect the confidentiality and integrity of the ToE design and implementation in its development and maintenance environments.
ATTESTATION/MARK	CAB	Following the review process, the CAB grants an autonomous delta & derivative certification statement. **[TR-E-IOT-SCS-PART-9]** gives an example of information to be included in this statement.
	Vendor	(if applicable) submits the metadata certification statement to the CAB and or ENISA centralized certification server
SURVEILLANCE	CAB	The CAB carries out surveillance as defined in this scheme policy **[TR-E-IOT-SCS-PART-1]** to provide confidence that products manufactured after the initial certification continue to fulfil the specified requirements.

6 Certification Metadata Status Updates

The Certification Status could be updated at least twice,

1. right after the vulnerability is being triaged and the vendor has been notified to apply the temporary mitigation.
2. After finalizing the permanent mitigation phase.

Pilot

7 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.

8 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**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **SGS**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **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.

pilot

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com