EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

GUIDELINES

Assurance Continuity - Practical Change Scenarios for certified ICT Products

Version 1, October 2025

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
07/04/25	V1 draft1	Creation	Version presented to EsEm for review Based on JIL "Assurance Continuity – Practical cases for Smart Cards and similar devices " https://www.sogis.eu/documents/cc/domains/sc/JIL-Assurance-Continuity-Practical-Cases-for-Smart-Cards-and-similar-devices-v1-0.pdf
30/06/25	V1 draft2	Draft 2	Update according to EsEm comments
26/08/25	V1 draft3	Draft 3	Update according to ANSSI comments
01/10/25	V1	Editorial review for publication	Version for publication

LEGAL NOTICE

LEGAL NOTICE

This publication is a guidelines document supporting Commission Implementing Regulation (EU) 2024/482.

This document is established with the support of the European Cybersecurity Certification Group (ECCG) sub-group on EUCC maintenance and review (EsEm) and may be updated whenever needed to reflect the developments and best practices in the field of assurance continuity.

This document should be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf for the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

This guidance document is developed in the context of the European Common Criteria-based cybersecurity certification scheme (EUCC), specifically focusing on assurance continuity activities as defined under Annex IV of the Implementing Regulation (EU) 2024/482.

It supports practical implementation of the provisions laid down in Annex IV of the Implementing Regulation (IR), providing illustrative guidance on how to identify and manage minor and major changes to certified targets of evaluation (TOE) or their environments, and seeks to provide some practical examples to help identifying the cases where evaluation work previously performed would need or not to be repeated. This document mainly focuses on the AVA class and its dependencies on other CC classes.

1.2 REFERENCES

1.2.1 Normative references

Regulations

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)[1].

Standards

Note: Unless otherwise specified, the versions of the Common Criteria and Common Evaluation Methodology standards defined in Article 2 of the EUCC scheme apply.

ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model.

ISO/IEC 15408-2:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components.

ISO/IEC 15408-3:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components.

ISO/IEC 15408-4:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities

ISO/IEC 15408-5:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements.

ISO/IEC 18045:2022 - Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation.

1.2.2 Informative references

[1] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj

[AC] CCDB - Assurance continuity: CCRA requirements, latest approved version[2]

1.3 ACRONYMS AND DEFINITIONS

1.3.1 Acronyms

ADV	Development
ADV_ARC	Security Architecture
ADV_FSP	Functional Specification
ADV_TDS	TOE Design
ADV_IMP	Implementation Representation
AGD	Guidance
AGD_OPE	Operational User Guidance
AGD_PRE	Preparative Procedures
ALC	Life-Cycle Support
ALC_CMC	Configuration Management Capabilities
ALC_CMS	Configuration Management Scope
ALC_DEL	Delivery
ALC_DVS	Development Security
ALC_FLR	Flaw Remediation
ALC_LCD	Life-Cycle Definition
ALC_TAT	Tools and Techniques
ATE	Tests
ATE_COV	Coverage
ATE_DPT	Depth
ATE_FUN	Functional Testing
ATE_IND	Independent Testing
AVA	Vulnerability Assessment
AVA_VAN	Vulnerability Analysis
CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
CSA	Cybersecurity Act
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EU	European Union
EUCC	European Common Criteria-based Cybersecurity Certification Scheme
GDPR	General Data Protection Regulation
IAR	Impact Analysis Report

[2] Current version is available at https://www.commoncriteriaportal.org/files/operatingprocedures/CCDB-014-v3.1-2024-February-29-Final-Assurance_Continuity.pdf

ICT	Information and communications technology
IEC	International Electrotechnical Commission
IR	Implementing Regulation
ISO	International Organisation for Standardisation
IT	Information technology
ITSEF	Information Technology Security Evaluation Facility
NAB	National Accreditation Body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;
NCCA	National cybersecurity certification authority
PP	Protection profile
SFR	Security functional requirement
SMEs	Small and medium enterprises
SOG-IS	Senior Officials Group – Information Systems Security
ST	Security target
TOE	Target of evaluation
TS	Technical specification
TSFI	TOE security function interfaces

1.3.2 Definitions

The definitions used under Article 2 of Regulation (EU) 2019/881 (Cybersecurity Act) and under Article 2 of the Implementing Regulation (EU) 2024/482 apply to this document. The following definitions as defined in [AC] also apply to this document.

a) the certified TOE refers to the version of the TOE that has been evaluated and for which a certificate has been issued;

b) the changed TOE refers to a version that differs in some respect from the certified TOE;

c) the maintained TOE refers to a changed TOE that has undergone the maintenance process and to which the certificate for the certified TOE also applies. This signifies that assurance gained in the certified TOE also applies to the maintained TOE;

d) the reassessed TOE refers to a previously certified TOE that has undergone a re-assessment;

e) the development environment addresses all procedures relating to development, production (depending on TOE type), delivery, start-up and flaw remediation of the TOE. It includes all concepts covered by the ALC class, together with the AGD_PRE family;

f) the subset evaluation relates to the re-evaluation only of those assurance components that are impacted by changes to the development environment, producing a partial ETR. A subset evaluation covers also the evaluation tasks when adding ALC_FLR to the assurance baseline.

g) a partial ETR is the output from the subset evaluation and provides, for the impacted assurance components, a level of detail that is commensurate with the corresponding sections of the ETR for the original certified TOE.

2. ASSURANCE CONTINUITY IN THE EUCC

Assurance continuity as defined in EUCC IR Annex IV.1 considers that changes made to a certified ICT product (i.e., to the certified TOE or its certified environment) and changes to the threat environment of an unchanged certified ICT product imply different types of analysis, and do not necessarily require evaluation work previously performed to be fully repeated in all circumstances.

More particularly, the assurance continuity rules establish different processes for re-assessment (in case of unchanged certified ICT product), handling changes to a certified ICT product and patch management.

These guidelines focus on the case of changes to a certified ICT product. They propose to differentiate evaluation activities and the types of reports to be established, based on the characterisation of the changes: minor or major.

3. CHARACTERISATION OF CHANGES

The classification of changes as minor or major follows the rules of the EUCC Implementing Regulation, in particular those set out in its Annex IV.

This section provides guidance to distinguish these types of changes and to ease consistent application of the assurance continuity process.

3.1 MINOR CHANGES

Minor changes are those that do not adversely impact the assurance expressed in the EUCC certificate of the certified product and can be addressed via the establishment of a maintenance report to the initial certification report, without requiring re-evaluation. Such changes include:

- editorial changes (e.g., typographical or formatting modifications);
- changes to the TOE environment that do not alter the certified TOE, such as:
  - migration to new hardware not included in the TOE.
  - use of software components outside the TOE boundary, with unchanged interfaces and security behaviour.
- source code or hardware schematic updates that do not alter existing assurance evidence;
- changes to development environment if it can be shown to have no follow-on effect on other assurance measure;
- changes to the ST front matter (change to the ST's identification or to the TOE identifier like product name change).

3.2 MAJOR CHANGES

Major changes are those that may adversely impact the assurance expressed by the certificate. These changes require a re-evaluation of the affected parts of the TOE. Examples include:

- changes to the set of claimed security assurance requirements (except ALC_FLR);
- changes to the set of claimed functional requirements;
- changes to the confidentiality or integrity of the development environment where such modifications could affect the secure development or production of the TOE;
- changes to the TOE to resolve an exploitable vulnerability;
- changes to the TOE boundary;
- a series of minor changes that may collectively alter the threat surface or level of assurance;
- changes whose impact on assurance is uncertain or unpredictable (e.g., bug fixes in security-enforcing components).

3.3 REMARKS

The determination of the change classification lies with the certification body, following its review of the submitted Impact Analysis Report (IAR).

It is important to understand that the size or visibility of a change does not always reflect its impact on security assurance. A large change that affects many parts of the TOE may have little or no effect on its certified security, while a small change to a specific function could significantly impact assurance if it touches critical security mechanisms.

Therefore, there is no fixed rule to decide whether a change is major or minor. Each change should be assessed in its own context, based on how it affects the certified security functions, the evaluation evidence, and the overall assurance provided by the certificate.

The following section provides general guidance to help identify whether a change is likely to be considered major or minor, including examples of cases where a small change may still require deeper review.

4. PRACTICAL EXAMPLES

This chapter provides examples of changes that may occur in certified ICT products or their environments, along with guidance on how to qualify them as minor or major under the EUCC.

The examples are grouped into:

- common changes (apply to all products);
- specific changes to smart cards and similar devices;
- specific changes to hardware devices with security boxes;
- specific changes to network devices.

Each example includes a description, expected impact analysis, testing considerations, and whether the change is typically minor or major.

Note: This list is not final and may be extended in the future to cover other product categories.

The classification of a change as minor or major may vary depending on the product's Evaluation Assurance Level (EAL). A change that introduces moderate architectural or implementation differences may be acceptable under lower assurance levels typically associated to AVA_VAN.1 and 2 and assurance level substantial, where evidence and testing depth are limited. However, the same change may be treated as major for higher assurance levels, where there are stricter requirements for completeness, systematic design, vulnerability assessment, and verification depth.

While the classifications of the following examples offer general guidelines, the final determination of whether a change is minor or major remains the responsibility of the Certification Body. In cases requiring technical assessment of the changes or when doubt arises, the ITSEF may be involved to provide the necessary technical expertise and analysis to support this determination. It is important to note that assurance requirements scale with the target assurance level. A change that may be acceptable with limited justification at lower assurance levels could, at higher ones, require deeper analysis, including retesting, code review, toolchain validation, and architectural impact analysis. This guidance outlines typical expectations, but the actual classification should be assessed in the context of the specific assurance level and requirements defined in the ST.

4.1 COMMON EXAMPLES

4.1.1 Guidance changes

A functional change in the guidance documentation will be considered as minor and therefore no penetration tests will be required whereas change to a mandatory security recommendation in the guidance will be considered as major and therefore a minimum set of appropriate tests may be required; however, in certain cases, such as a refinement of a security recommendation solely for clarity or precision that does not alter its fundamental security posture, tests may not be necessary.

4.1.2 Changes to underlying OS or Hardware platform

The impact of migrating to a different OS or hardware platform depends on whether these components are included within the TOE boundary or out of scope but still interact with or influence the TOE. This section provides an analysis of the impact classification under two distinct cases.

4.1.2.1 OS / Hardware platform out of TOE scope

This case assumes the OS or hardware is not part of the TOE but is part of the assumed IT environment. Such components may support the TOE’s correct and secure operation but are not themselves evaluated.

Table 1: Impact classification criteria for platform changes

Dimension	Consideration	Impact classification with assurance level consideration
ST Assumptions (e.g., A.PLATFORM)	If the platform does not meet stated assumptions (e.g., memory protection, process isolation, RNG, crypto module)	Always major regardless of the assurance level – requires re-evaluation
Interfaces / Dependencies	If the TOE depends on platform security APIs (e.g., RNG, crypto module), and the new platform complies with the assumptions stated in the ST while providing the same APIs, behaviour, and security guarantees, then the change may be considered minor.	Minor at lower assurance levels if proven in IAR. At higher assurance levels, indirect dependencies (e.g., kernel syscall behaviour, entropy sources) should be examined in more detail; could be major.
Platform certification	If the new OS/hardware is evaluated/certified at an equivalent or higher assurance level	Generally minor, especially when the platform is certified under the same scheme. At higher assurance levels, composability evidence should show that residual risks are negligible.
TSFI impact	If the change does not affect TSF Interfaces	Minor across all assurance levels
Indirect effects (timing, power)	If migration causes measurable changes to timing or resource behaviour of TOE (e.g., affecting crypto)	Always major at AVA_VAN.4 and 5, due to side-channel attacks. At lower assurance levels, may be minor if no impact is shown.

Below are example scenarios illustrating possible changes:

Table 2: Sample platform migration cases and their security impact

Scenario	Impact	Rationale
Change from Ubuntu 20.04 to Ubuntu 22.04	Minor	Same kernel family, interfaces unchanged, assumptions met
Change from Intel to ARM hardware	Major	Changes in boot chain, memory model, crypto acceleration
Change to a hardened hypervisor-based platform	Minor	TOE hosted in virtual appliance, verified platform isolation maintained
OS migration violating ST assumption (e.g., no MMU)	Major	TOE no longer benefits from assumed memory isolation

4.1.2.2 OS / Hardware platform partially or fully inside TOE scope

This case occurs when some or all of the platform elements are inside the TOE boundary. That is, the certified TOE includes the embedded OS, secure boot chain, crypto libraries, drivers, or a specific hardware chip.

Table 3: Change impact when OS or Hardware is within the TOE scope

Dimension	Consideration	Impact classification with EAL consideration
TOE component replacement	If an in-scope component is changed (e.g., embedded OS, secure driver)	Always major regardless of assurance levels – requires re-evaluation
Cryptographic or bootloader dependency	Any change to crypto kernel, secure boot, key manager	Always major regardless of assurance levels – requires re-evaluation
Patch-level change within same baseline	Kernel minor update (e.g., 5.10.1 → 5.10.14) with no security difference	Always minor regardless of assurance levels
Recompilation for new hardware	If source is unchanged but compiled for new CPU/platform	Minor at lower assurance levels if cryptographic behaviour is unchanged. Major at AVA_VAN.4 and 5, especially if timing, fault injection, or side-channel risks may change.
Delta in timing, Resource behaviour	Change in crypto timing, entropy, race conditions	Always major from AVA_VAN.2 upward, due to impact on both FCS_RBG/FCS_RNG and potential for side channel attacks or fault attacks (AVA_VAN and FPT_FLS).

Below are example scenarios illustrating possible changes:

Table 4: Example scenarios for platform-level changes and their impact

Scenario	Impact	Rationale
Updating bootloader hash algorithm (SHA-1 → SHA-256)	Major	Direct change to trust anchor verification
Porting TOE from Linux Yocto to Linux Debian base	Major	Different kernel trees, toolchains, syscall behaviour
Applying verified patch (no security logic touched)	Minor	No change to SFR logic; IAR can justify as minor
Replacing SoC with same instruction set, same crypto IP	Major	Even if crypto logic is reused, timing, noise, and leakage may differ

4.1.3 Modification to TSF architecture

Description:

The change concerns modifications to the architecture of the TSF (TOE Security Functionality)—specifically, the internal logic, structure, or enforcement pathways that were originally part of the evaluated and certified design. Examples include:

- removal or deactivation of specific TSF components (e.g., disabling cryptographic modules, integrity checks, or self-tests);
- modifications to access control enforcement (e.g., re-coding RBAC logic or removing checks on credential types);
- changes in how credentials are parsed, stored, or validated (e.g., new password hash algorithm, skipping certificate validation steps);
- structural refactoring such as:
  - Kernel-level redesign (e.g., shift from monolithic enforcement to modular policy engine);
  - Introduction of privilege separation (e.g., breaking monolithic admin logic into isolated processes);
- disabling or replacing secure logging or audit mechanisms;
- boot and initialisation changes that affect secure startup:
  - replacement of bootloader code that previously enforced integrity check;
  - modification of the update verification chain (e.g., new public key or format);
  - changes that impact how trust anchors are provisioned or verified.

Impact Analysis Report (IAR):

These changes alter the security boundary and may invalidate critical assumptions of the prior certification:

- affected security objectives and SFRs may include FPT_TST (self-test), FAU_GEN (audit), FMT_MSA (security attributes), FCS_CKM (key management) and others;
- new or removed components should be reflected in architectural evidence (e.g., ADV_ARC, ADV_TDS);
- changes in policy enforcement or boot integrity may introduce new attack vectors or invalidate previously applied AVA_VAN testing results;
- trust assumptions about the startup chain, module isolation, or audit reliability that are no longer valid;
- the IAR should document the rationale for each architectural deviation, updated module interaction, and traceability of the new design to security objectives.

Testing Impact:

Full evaluation is required to verify that:

- the new architecture enforces equivalent or stronger security measures;
- all security policies are properly implemented and protected against bypass or tampering;
- vulnerability analysis and penetration testing are needed to validate secure boot logic, access control boundaries, and enforcement reliability;
- any change affecting trust anchors or update verification should be tested for resistance to rollback, tampering, or incorrect certificate validation.

Change Type: Major

4.1.4 Cryptographic implementation changes

Description:

This type of change relates to modifications to the cryptographic mechanisms used by the TOE. Cryptographic components are central to the security posture of any TOE and are often directly tied to claimed SFRs such as FCS_COP, FCS_CKM, and others. Common examples include:

- replacing RSA with ECC (e.g., for digital signatures or key exchange);
- migrating to a different cryptographic library (e.g., from OpenSSL to WolfSSL);
- adding support for post-quantum cryptography (e.g., CRYSTALS-Kyber, Dilithium);
- replacing secure communication protocols (e.g., from SSH to TLS 1.3) or changing protocol profiles;
- modifying default key lengths, modes of operation (e.g., CBC → GCM), or trust anchor handling.

Impact Analysis Report (IAR):

These changes directly affect the cryptographic boundary of the TOE and typically impact:

- functional correctness: new cryptographic modules or algorithms should be validated for correct implementation and integration;
- protocol behaviour: changes to TLS affect authentication and data protection guarantees and might invalidate previous AVA_VAN and FPT testing;
- assurance claims: the TOE should maintain equivalence or improvement in security strength (e.g., 128-bit → 256-bit security level);
- developer evidence (ADV_FSP, ADV_TDS, AGD_OPE) and cryptographic documentation (e.g., algorithm certifications, configuration guidance) should be updated;
- legacy assumptions about side-channel resistance, key management (FCS_CKM), and cryptographic services should need re-validation;
- any integration with external key stores (e.g., HSM) or protocol changes (e.g., TLS client/server roles) should be clearly documented.

Testing Impact:

A re-evaluation should be required, potentially including:

- AVA_VAN, FCS_xxx families, and full protocol re-verification;
- side-channel and fault injection tests if implementation is changed or new primitives are introduced;
- key generation, exchange, destruction and storage validation to match original assurance claims;
- for post-quantum primitives, resistance to quantum attack models may also be claimed and verified where applicable.

Change Type: Major

4.1.5 Random Number Generation (RNG) changes

Description:

This change refers to modifications in how the TOE performs random number or bit generation, which is foundational for secure cryptographic operations such as key generation, nonce creation, and protocol initialisation. Such capabilities are defined under:

- FCS_RBG family (Random Bit Generation), covering deterministic and entropy-based designs with various seeding strategies;
- FCS_RNG.1 (Random Number Generation), which captures physical or true random number generators and quality metrics.

Common examples of changes include:

- switching the RBG algorithm (e.g., Hash_DRBG → HMAC_DRBG) as per FCS_RBG.1;

- changing or updating the seeding mechanism, e.g., from software-based to hardware-based entropy source or vice versa, impacting FCS_RBG.3 or FCS_RBG.4;
- introduction of external entropy sources (FCS_RBG.2) or use of multiple seeding channels (FCS_RBG.5);
- changes to output interfaces used by external entities (FCS_RBG.6);
- migration from deterministic RBGs to physical FCS_RNG.1-based true RNGs;
- altering entropy estimation methods, sampling rates, or combining operations.

Impact Analysis Report (IAR):

Changes to the RNG directly affect the core entropy and unpredictability guarantees on which secure key generation and cryptographic protocol security rely. An impact analysis should consider the following aspects:

- impact on key-dependent functionalities, such as validated key generation, session keys, and nonce generation processes;
- updates required in developer evidence, including: ADV_FSP (functional specification), ADV_TDS (design description), ADV_ARC (security architecture), AGD_OPE/AGD_PRE (guidance documents), and ATE (test coverage for the new RNG behaviour);
- validation and characterisation of noise sources, including startup tests, continuous health checks, and entropy estimation;
- platform dependency changes, such as switching to a platform TRNG or CPU instruction (e.g., Intel RDRAND);
- changes to entropy source or reseeding logic, especially when combining multiple sources, requiring re-evaluation of minimum entropy assumptions and reseeding behaviour;
- modifications in hardware timing, jitter sources, or noise combination logic, which may influence side-channel resistance or fault sensitivity;
- SFRs such as FPT_TST.1 (TSF self-testing) and FPT_FLS.1 (failure handling) may be affected and should be reviewed accordingly.

Testing Impact:

RNG changes require dedicated testing including:

- statistical entropy validation should be performed using approved suites (e.g., NIST SP 800-90B, SP 800-22, or AIS 31) to confirm the quality and unpredictability of generated random bits;
- functional correctness testing is required to ensure that RNG output is properly integrated into cryptographic operations (e.g., ephemeral key generation, nonce construction), in alignment with FCS_CKM, FCS_COP, and FCS_RBG;
- source code review should cover the entire RNG pipeline: entropy acquisition, conditioning, seeding, reseeding, instantiation, and error handling logic;
- penetration testing is often mandatory, especially when:
  - a hardware-based entropy source (e.g., analog TRNG) is introduced or modified;
  - RNG output is externally exposed under FCS_RBG.6;
  - the implementation may be susceptible to:
    - fault injection (voltage, clock, EM);
    - side-channel leakage (timing, power);
    - perturbation of data or control paths (e.g., reseed suppression or force failure);
- health testing and robustness analysis should evaluate RNG behaviour under boundary operating conditions (e.g., temperature, voltage variations);
- AVA_VAN activities should be revisited, especially where key generation processes or protocol initialisation (e.g., TLS) depend on RNG outputs;
- self-test logic under FPT_TST.1 should be re-tested or updated to cover any change in seeding, entropy source, or RNG behaviour.

Change Type: Major

4.1.6 New externally exposed interfaces

Description:

This change introduces new external points of interaction with the TOE, such as:

- adding physical management ports (e.g., USB, serial console, Ethernet for admin);
- exposing new network-based APIs (e.g., RESTful APIs, SNMP interfaces, gRPC services);
- making previously internal components remotely accessible;
- enabling remote diagnostics, telemetry, or firmware update interfaces over unsecured or less-hardened paths.

These interfaces typically allow access to configuration, monitoring, or update functions and may be used by administrators, external IT systems, or automation tools. However, they increase the attack surface and may introduce new vectors for compromise, especially if:

- not authenticated or not protected via secure channels;
- not included in previous security boundary assumptions;
- they reuse internal components or services not designed for external exposure.

Impact Analysis Report (IAR):

The IAR should address:

- whether the interface is within the TSF boundary or interacts with it indirectly;
- what services, data, or operations the interface exposes;
- whether authentication**,** authorisation, and encryption mechanisms are applied to the new interface and match previous assurance claims (e.g., FTP_ITC.1, FTP_TRP.1, FIA_UAU);
- interface documentation (FSP) and guidance documents (AGD_OPE) may need updates;
- any shared state with other interfaces should be checked for cross-interface vulnerabilities;
- the presence of new threat vectors, especially those requiring additional vulnerability analysis (AVA_VAN).

Testing Impact:

A re-evaluation is needed, especially under AVA_VAN, ADV_FSP, and potentially ADV_TDS/AGD depending on the depth of the interface integration, including:

- functional and interface testing for all exposed methods, commands, or protocols;
- authentication and access control testing specific to the new interface;
- penetration testing focused on:
  - protocol misuse;
  - input validation flaws;
  - authorisation bypass;
  - improper error handling.

Change Type: Major

4.1.7 Factory or supply chain integrity changes

Description:

This type of change involves modifications to the physical production, assembly, or secure provisioning of the TOE, which may include:

- migration to a new manufacturing or integration facility (e.g., chip packaging, appliance casing);
- use of a new wafer foundry or hardware component supplier for ICs used in the TOE;
- introduction of a new key injection or personalisation facility, such as a new HSM initialisation centre;
- updates to the logistics chain, including secure transport procedures or warehouse handover processes.

These changes impact the life-cycle phase (ALC) of the TOE and can undermine supply chain trust anchors (e.g., secure key provisioning, firmware authenticity, tamper-evident seals) if not properly controlled.

The change could affect:

- ALC_DVS (Developer Environment Security): if the new facility has different physical/logical protections or lacks trusted roles enforcement;
- ALC_DEL (Delivery): if transport or packaging conditions change;
- ALC_FLR (Flaw Remediation): if issue tracking/resolution in the new facility differs from the certified environment;
- ALC_CMC/ALC_CMS: if the configuration management or build environment changes as a result.

Impact Analysis Report (IAR):

The IAR should provide:

- a detailed comparison of the old and new facilities, including access control, tamper detection, employee vetting, monitoring, and secure zones;
- assurance that secure build, key provisioning, and distribution procedures are either unchanged or equivalently replicated;
- confirmation that firmware or hardware signing and injection processes remain secure and verifiable (e.g., use of certified HSMs, signing key control);
- a review of updated ALC evidence, including:
  - facility security policies;
  - toolchain or provisioning system relocation evidence.

Testing Impact:

These changes can be managed under the Maintenance process with a partial ETR, provided that the IAR and the assessment of ALC changes demonstrate an equivalent security assurance level to the initial certification.

Change Type: Minor

4.2 FOR SMART CARDS AND SIMILAR DEVICES

4.2.1 Examples of Hardware changes

This chapter describes few practical cases for changes done at hardware level or on the dedicated software and evaluated during the hardware evaluation.

The Impact Analysis is delivered by the IC developer including a differential description from the design sources to confirm which parts of the implementation have been modified and/or a source code and build outputs (e.g., assembly listings) differentials to confirm which parts of the implementation have been modified when the dedicated software or the cryptographic library is concerned. The type of description shall be in a way enabling examination of the differences on the lowest level of design, if appropriate down to transistor level.

4.2.1.1 Functional extension

Description:

The considered change in this example is due to a functional extension in one hardware block or addition of one communication interface, and it induces limited difference within RTL code but with full re-synthesis and new place and route.

Impact Analysis Report (IAR):

Due to the full re-synthesis and new place and route, the chip is physically as a completely new chip, and this is therefore considered as a major change. Although functionality/concepts/interfaces may be equal, physical behaviour, signal run times, related analogue behaviour, perturbation and LFI vulnerability are expected to be different with relevance on overall security level. In this case the hardware block change is regardless.

Testing impact:

Full testing will be required in such a case.

Change type: Major

4.2.1.2 Limited change on RNG hardware block

Description:

The considered change in this example is due to a limited change on the RNG hardware block (limited difference within RTL code but with partial re-synthesis).

Impact Analysis Report (IAR):

If the change is located:

a) on interfaces of the RNG only: it can be considered as a minor one;
b) in the analogue logic, respectively the entropy source: it is considered as a major one.

Partial re-synthesis is a matter of the area affected with regard to size and also other modules involved. By default, it is relevant for being a major change.

Testing impact:

Based on the above description, no penetration tests would be required in case a) and statistical testing based on a Quality metric will be required in case b) whereas additional tests such as Physical testing (FIB), fault injection should be considered when appropriate.

Change type:

a) digital interface only: Minor;
b) analog entropy source: Major.

4.2.1.3 Change through metal fix

Description:

The considered change in this example is due to limited metal fixes following ESD issues on VDD regulator or metal fix enabling a feature at functional level.

Impact Analysis Report (IAR):

Different cases may occur:

a) if the module is for example regarding interfaces, memory logic or other modules not computing/managing sensitive data or signals, it could be non-relevant and considered as minor change;
b) if the metal fix is on voltage regulation it could be relevant regarding perturbation on external voltage and information leakage and considered as major change;
c) metal fix enabling a feature on functional level, it could be relevant regarding perturbation on external voltage and information leakage and considered as major change.

Testing impact:

Based on the above description, perturbation testing by spiking / glitching and side channel, no penetration tests would be required in case a), verification testing (when appropriate) would be required in case b), whereas additional tests should be considered in case c) when appropriate.

Change type:

a) non-sensitive modules: Minor;
b) voltage regulation or timing: Major;
c) feature-enabling fix: Major.

4.2.1.4 Change in NVM size

Description:

The considered change in this example is due to a different NVM memory size.

Impact Analysis Report (IAR):

1. the Impact Analysis is delivered by the IC manufacturer including a differential description from the design sources to confirm which parts of the implementation have been modified;

2. NVM memory size change is achieved by:
   a) blocking and this is therefore considered as minor change;
   b) a new module of different size with localised and limited new place/route and re-synthesis (only linked to NVM size change) and this is therefore considered as minor change.

Testing impact:

Based on above description, no penetration tests will be required for minor changes whereas depending on the area affected and amount of changes affecting surrounding modules of the NVM, a change of the side channel leakage or fault injection resistance can be expected and would require to be tested.

Change type: Minor

4.2.1.5 Wafer production change

Description:

The considered change in this example is due to transfer of design sources from one wafer production facility to another.

Impact Analysis Report (IAR): the Impact Analysis is delivered by the IC manufacturer. A change in wafer production is typically considered as a major change.

Testing impact:

A minimum set of penetration tests would be required: side channel analysis (at least use of metrics to demonstrate similar leakage for hardware cryptographic-core and CPU and equivalent resistance) and fault injection to identify any difference on related countermeasures.

Change type: Major

4.2.1.6 Technology node shrink change

Description:

The considered change in this example is due to a technology node shrink, the design sources are transferred to a new technology node from one wafer production facility to another.

Impact Analysis Report (IAR):

A technology shrinks with such design sources transferred to a new technology node will in general be “limited”, as a big step in the technology node will require a new design, however this change is considered as major.

Testing impact:

Full testing is required as the shrink always impacts the behaviour of the chip regarding its leakage, physical entropy source and fault injection tolerance as the physical characteristics of the chip change.

Change type: Major

4.2.2 Examples of Software changes

This chapter describes few practical cases for changes done at software level and evaluated during composite evaluation.

The Impact Analysis is delivered by the IC or ICC product developer including source code differential to confirm that only out of scope parts of the implementation have been modified, build outputs (e.g., assembly listings) and toolchain versioning information.

4.2.2.1 Change of non-security relevant functionality

Description:

The considered change in this example is performed on non-security relevant functionality or not related to security decision.

Impact Analysis Report (IAR):

Change of non-security relevant functionality can be: functionality of code used for initialisation/personalisation, return codes, flow/checks for different return codes, correction of functional bug using patch mechanisms, non-security relevant command, additional application compliant with the security guidance (e.g. non-Payment application on Payment cards, basic Java Card applet/Multos application, native application, GP Issuer Security Domain, transmission protocol, Telco functionality). These changes can be considered as minor if no side effect during the security impact analysis is identified.

Testing impact:

Based on the above description, no penetration tests will be required for minor changes.

Change type: Minor

4.2.2.2 Change of security relevant functionality

Description:

The considered change in this example is done on security relevant functionality.

Impact Analysis Report (IAR):

Change of security relevant functionality can be cryptographic implementation, security measures, flow of security checks (e.g., PIN verification), handling of assets, low level memory access (copy/write NVM, etc..). These changes are therefore considered as major.

Testing impact:

A minimum set of penetration tests may be required: side channel (use of metrics to demonstrate equivalent resistance), fault injection (at least verification testing) and any further tests needed such as software attacks.

Change type: Major

4.2.2.3 Code relocation within the same memory

Description:

The considered change in this example occurs after relocation of part of the Embedded Software without functional change.

Impact Analysis Report (IAR):

Relocation of code without functional change can be applications loaded in a different order and impacting the logical/physical address (within the same memory) of the application under certification, adding/changing non-security related code for e.g., personalisation, change of buffer sizes. These changes can be considered as minor if no side effect during the security impact analysis is identified.

Testing impact:

Based on the above description, no penetration tests will be required for minor changes.

Change type: Minor

4.2.2.4 Code relocation in a different memory

Description:

The considered change in this example occurs after relocation of Embedded Software in a different memory (e.g., from ROM to EEPROM) without any source code change.

Impact Analysis Report (IAR):

Loading an application or a cryptographic library under certification in a different memory is considered as major.

Testing impact:

A minimum set of verification testing may be required; however experience gained from the lab on several similar changes (similar products) could mitigate the potential impact and thus avoid these penetration tests.

Change type: Major

4.2.2.5 Configuration parameter(s) change

Description:

The considered change in this example is due to different configuration parameter(s) for non-security relevant functionality which was/were not included in the previous evaluation without any change of the code.

Impact Analysis Report (IAR):

Change of configuration parameter(s) for non-security relevant functionality without any change of the code can be Java Card package AID change, MIFARE/DESFIRE on/off or Transmission protocol. These changes can be considered as minor if no side effect during the security impact analysis is identified.

Testing impact:

Based on the above description, no penetration tests will be required for minor changes.

Change type: Minor

4.2.2.6 Similar product on similar IC reference

Description:

The considered change in this example is due to the use of a new IC reference with almost the same source code.

Impact Analysis Report (IAR):

This is almost the same product as the one originally certified but on a new IC reference, say from the same IC family - same physical layout - with only limited code changes due to the IC change. These changes are usually considered as major.

Testing impact:

A minimum set of verification testing may be required however experience gained from the lab on several similar changes (similar products) could mitigate the potential impact and thus avoid these penetration tests.

Change type: Major

4.2.2.7 Change in Flash Bootloader code

Description:

The considered change in this example is due to issues in Flash Bootloader code.

Impact Analysis Report (IAR):

A functional change in the Bootloader is relevant as it could open access points for perturbation and also side channel attacks, if this is not covered by accompanying reasonable further hardware and software means:

a) if the Flash Bootloader is applied in secure environment only and permanently blocked prior reaching phase 7 (delivery to the end-user) the change can be considered as minor;
b) if the Flash Bootloader is protected against fault injection/SCA and source code review done by the ITSEF associated with developer functional verification demonstrate there is no security impact, the change would be considered as minor;
c) if there is no justified protection and the change implements e.g., cryptographic calculation, address-depending jumps etc. it is therefore considered as major change.

Testing impact:

Based on above description, no penetration tests will be required for minor changes, cases a) and b). Else perturbation and side channel attacks should be considered for case c). For example, perturbation could block required security settings / configurations at start-up, software handling with secrets and address-depending jumps could be subject of SPA.

Change type:

a) Locked pre-user: Minor
b) Protected & reviewed: Minor

c) Adds crypto or jumps: Major

4.2.2.8 Change in cryptographic library code

Description:

The considered change in this example is due to functional issue in the cryptographic library code as for example an RSA key length update.

Impact Analysis Report (IAR):

A functional change in the cryptographic library code is relevant as it could open access points for failure and side channel analysis. RSA key length update by itself is not that relevant however this might have an impact on the efficiency of data randomisation and/or blinding of exponents and it is therefore considered as major.

Testing impact:

Based on above description, full testing might not always be necessary and verification testing could be considered sufficient.

Change type: Major

4.3 FOR HARDWARE DEVICES WITH SECURITY BOXES

This section provides representative examples of hardware and software changes specific to hardware devices with security boxes.

4.3.1 Examples of hardware changes

4.3.1.1 Addition of new physical interfaces in security boxes

Description:

Addition of an external interface (e.g., extra network port, USB, debug UART, JTAG, or PCIe expansion slot) to hardware devices with security boxes.

Impact Analysis Report (IAR):

Although core security functionality may remain unchanged, the new interface alters the external attack surface. Even disabled interfaces may be reactivated by fault injection or debug backdoors. PCB layout modifications could impact signal timing, EM leakage, or interference with tamper-detection mesh. The potential for invasive attack vectors or physical probing increases significantly.

Testing impact:

- Tamper detection and mesh integrity should be retested.
- Side-channel leakage (DPA/EMA) and electromagnetic interference tests are required.
- Penetration testing should validate the interface cannot be misused to gain unauthorised access.

Change type: Major

4.3.1.2 Change in security box assembly or manufacturing location

Description:

The manufacturing of the secure hardware device moves to a new foundry, assembly site, or integration facility. This may include changes to the entity applying tamper-evident labels, integrating anti-tamper mesh, or performing final sealing of the security box. These changes involve a modification to ALC related to the physical production, assembly, and secure provisioning of the secure hardware device. Specifically, it addresses the relocation of the manufacturing, assembly, or final integration of the TOE to a new foundry, assembly site, or integration facility.

Impact Analysis Report (IAR):

The IAR should provide an analysis of how the change in manufacturing or assembly location impacts the TOE's assurance baseline and its certified security properties. This includes:

- a comparison of the security controls and procedures at the old and new facilities, specifically addressing ALC_DVS elements;
- assurance that secure build, key provisioning, and distribution procedures (per ALC_CMC/CMS and ALC_DEL) are either unchanged or equivalently replicated and controlled in the new environment;
- confirmation that firmware or hardware signing and injection processes remain secure and verifiable (e.g., use of certified HSMs, robust signing key control).

Testing impact:

These changes can be managed under the Maintenance process with a partial ETR, provided that the IAR and the assessment of ALC changes demonstrate an equivalent security assurance level to the initial certification.

Change type: Minor

4.3.1.3 Tamper response circuit modification

Description:

Changes to tamper detection systems such as wire mesh logic, tamper sensors (voltage, temperature, motion), erase logic, or battery-backed volatile memory.

Impact Analysis Report (IAR):

Tamper response is core to the secure erase capability. Any change may delay detection, increase response latency, or permit key retention. Improperly configured erase triggers could result in permanent compromise of secrets in NVM or SRAM.

Testing Impact:

- Physical penetration testing (e.g., mesh breach, cold boot attempts),
- Timing validation of tamper-response latency,
- Simulation of environmental triggers (voltage, temp).

Change Type: Major

4.3.2 Examples of software changes

4.3.2.1 Reuse of certified firmware on another hardware variant

Description:

Firmware is ported to a new hardware version—e.g., different SoC, different microcontroller variant, new cryptographic coprocessor.

Impact Analysis Report (IAR):

Differences in instruction timing, bus width, or crypto accelerator implementation may affect deterministic behaviour, leakage profile, or fault tolerance. Timing of key generation, entropy collection, or signature validation may differ.

Testing Impact:

- full AVA_VAN testing to confirm no added vulnerability;
- re-verification of secure boot and firmware update processes;
- review of crypto primitive behaviour on the new platform (e.g., AES speed, RNG entropy).

Change Type: Major

4.3.2.2 Firmware patch affecting tamper handlers or GPIO triggers

Description:

Changes to interrupt routines, tamper GPIOs (General Purpose Input/Output), or software reaction to tamper events (e.g., logging method, timing of key zeroisation).

Impact Analysis Report (IAR):

Tamper response timing is critical. A patch that defers erasure or disables interrupt pathways could undermine trust. Changes to audit trails, event logs, or masking behaviour can expose latent vulnerabilities.

Testing Impact:

- functional and fault-injection testing of tamper event handling;
- ensure erase-on-tamper logic remains reliable and responsive;
- code inspection of interrupt handling and memory clearing.

Change Type: Major

4.4 FOR NETWORK DEVICES

This section provides representative examples of changes specific to network devices (e.g., firewall, VPN, switch).

4.4.1 Examples of changes

4.4.1.1 Addition of audit events

Addition of non-SFR-impacting audit events
Description:

A new audit event is introduced to help with the TOE monitoring or functional operations. This new log event is not a part of the TOE's defined SFRs and does not change how the TOE enforces security. It is just adding extra useful information.

Audit event example: Logging detailed CPU or memory usage for an application, which is for performance monitoring.

Impact Analysis Report (IAR):

This enhances observability without modifying core TSF logic. Logging modules are extended, but the audit record format, triggering conditions, and policy enforcement remain consistent. The new audit event does not constitute a change to any existing SFR or the introduction of a new SFR within the certified scope.

Testing Impact:

This does not require extensive functional testing. The change operates within well-defined, existing TSF functionality. No change to TSF boundary or attack surface.

Change Type: Minor

Addition of SFR-impacting audit events
Description:

This type of change involves modifying or adding to the TOE's SFRs about what must be logged. This means the TOE is now required to log new types of security events or log existing events in a more detailed way, as mandated by a security policy.

Audit event example:

- Change to existing SFR (e.g., previously only failed logins were required to be logged; now all logins are required including successful ones)
- Introduction of a new SFR (e.g., new SFR requiring logging of all attempts to access sensitive data)

Impact Analysis Report (IAR):

This change directly affects the certified security functionality, introduces new security audit events that could modify core TSF logic. Modifications to developer evidence (ADV_FSP, ADV_TDS, ADV_IMP) are required to reflect the revised or new SFRs and their implementation.

Testing Impact:

Functional testing analysis is needed for testing existing or new SFRs affected by the audit change. Potential for change to TSF boundary or attack surface depending on the nature of the SFR modification.

Change Type: Major

4.4.1.2 Cryptographic library version update

Description:

Upgrade from OpenSSL 1.1.1 to 3.0, retaining all ciphers and protocols used by the TOE.

Impact Analysis Report (IAR):

Possible differences in:

- Default cipher suite priorities
- Internal entropy handling
- Timing behaviour and padding routines

ADV_TDS, ADV_FSP, and AGD should reflect new cryptographic boundaries and assumptions.
FCS_CKM/FCS_COP evidence should be revised.

Testing Impact:

Crypto conformance testing. Fault injection and side-channel leakage analysis due to changed implementation.
FPT_TST.1 self-tests may need adjustment.

Change Type: Major

4.4.1.3 Self-Test failure handling policy change

Description:

Device now enters maintenance mode instead of rebooting on POST failure.

Impact Analysis Report (IAR):

Affects FPT_TST.1 and secure state transition claims. ADV_ARC and AGD_OPE should show continued isolation and minimal services in maintenance state.

Testing Impact:

Simulate test failures, verify error logs and access controls. Penetration test required to validate integrity in degraded state.

Change Type: Major

4.4.1.4 Enablement of automatic update

Description:

Device now supports automated patch fetch and install via signed bundles over HTTPS.

Impact Analysis Report (IAR):

Introduces new trust boundaries and timing triggers. For example, FTP_TRP.1 and FPT_TUD_EXT.1 should be revalidated. Signature validation, rollback, and dependency checks needed. Developer evidence for patch validation should be updated.

Testing Impact:

Trigger update conditions, simulate signature failures, rollback attempts. Verify no code injection.
Penetration testing required.

Change Type: Major

4.4.1.5 Addition of admin interfaces

Description:

Admin access now available via both SSH and HTTPS (previously only HTTPS). This introduces a new protocol stack for administrative access, which involves new or modified SFRs for authentication, access control, and secure communication channels.

Impact Analysis Report (IAR):

This significantly increases the attack surface by introducing a new administrative interface. It requires validation of authentication equivalence and isolation between interfaces. Given the introduction of a new protocol (e.g., SSH) for administrative purposes, updates to developer evidence (e.g., ADV_FSP, AGD_OPE, FCS, FIA, FDP families) are required to reflect how the new interface meets existing or new SFRs.

Testing Impact:

Testing is required including authentication, access control, and session termination testing.
Penetration testing is likely to be required to assess the resilience of the new interface.

Change Type: Major

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu