EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cyber Resilience Act implementation via EUCC and its applicable technical elements

Annexes

Final version: 27/01/2025

Contents

1. ANNEX I. Mapping the CRA Requirements for EUCC certification process (detailed analysis)

This analysis currently focuses on the necessary SFRs, but not on the security objectives and elements of the security problem (e.g., threats or policies) that need to be included in the Security Target in relation to those SFRs. The elaboration of security problem definition and security objectives will be documented in the custom-tailored security target for CRA conformance claim.

The below subsections include a proposal of the SFRs and SARs that can cover the requirements in the CRA annexes. When, aside from the proposal done in this document, there could be an alternative way to obtain the conformance with other technical elements, it is indicated with purple text after the proposal.

1.1. CRA Annex I, Part I, ESRs

ESR (1)

Requirement:

Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

Analysis

CC standard utilises an approach in which the security functionality under evaluation is ultimately defined based on a series of threats to assets under protection of the TOE which the Security Functional Requirements aim to mitigate. Such security problem definition includes the definition of a number of assets and the threats against which they need to be protected, along with some conceptual security objectives that outline those functionalities that the TOE shall provide in order to achieve that protection. Ultimately, the security objectives are met by means of a number of SFRs that describe the TOE security functionality that is responsible for implementing the protection of the assets against the designated threats.

The above-described approach is included in the Security Targets of the TOEs under evaluation by means of the assurance components in the ASE_SPD, ASE_OBJ and ASE_REQ families. In the case of ASE_OBJ family, the security objectives of the TOE (describing TOE functionalities oriented towards mitigating the threats on the assets protected by the TOE), as ASE_OBJ.1 only requires the definition of security objectives for the operational environment, and not for the TOE (this aspect would be covered by ASE_OBJ.2 requirement). However, the inclusion of ASE_OBJ.2 in the evaluation should not be mandatory for the objective of meeting this ESR, as ASE_REQ.1 alone would address such aspect. The reason is that [CC2022P3] defines the related content and representation requirement ASE_REQ.1.8C as follows: “The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.” Regarding ASE_SPD.1, these are required for any evaluation assurance levels starting from EAL2, as defined in [CC2022P5] (e.g., not included in EAL1). ASE_REQ.1, on the other hand, is included in any evaluation assurance level starting from EAL1.

As Security Targets complying with ASE_SPD.1 define a security problem with list of assets to be protected by the TOE and the threats (as adverse actions carried out by threat agents aiming to vulnerate the security of the assets), these can be seen as the risks that the TOE faces. Moreover, ASE_REQ.1 requires to describe the security functionality of the TOE in terms of SFRs that will meet the security requirements and requires a rationale demonstrating that the SFRs counter all threats for the TOE (together with the security objectives for the environment). In order to make the rationale complete, ASE_OBJ.1 needs to be included in the evaluation as well, although when including ASE_OBJ.2 in the evaluation, alternatively, the rationale would demonstrate that the SFRs meet the security objectives for the TOE, which counter the threats. Therefore, those assurance requirements together ensure that the cybersecurity requirements implemented by the TOE are based on a risk analysis.

Proposal

The Security Target of the TOE shall include the following assurance components: ASE_SPD.1, ASE_OBJ.1 and ASE_REQ.1. These requirements are directly met in evaluations in conformance with EAL2 or above.

Guidance

Manufacturers of products undergoing a EUCC evaluation shall include in the Security Target the assurance components ASE_SPD.1, ASE_OBJ.1 and ASE_REQ.1.

ESR (2)(a)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) *be made available on the market without known exploitable vulnerabilities;*

Analysis

EUCC evaluations will directly address the search of exploitable vulnerabilities of products under evaluation pursuant to AVA_VAN assurance family. AVA_VAN includes 5 assurance components (AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4 and AVA_VAN.5) among which an individual component is chosen for the evaluation based on the criticality of the assets to be protected by the TOE, or on the general assurance level of the evaluation. Each of the components in the AVA_VAN family include evaluation work units that require evaluators to carry out a search of public domain sources to identify potential vulnerabilities in the TOE, along with conducting a penetration testing campaign based on the identified potential vulnerabilities. However, the different AVA_VAN.X components differ in two factors:

a) The considered *attack potential* for an attacker trying to exploit vulnerabilities in the TOE, which is a numeric factor calculated in terms of elapsed time to conduct an attack, required expertise, knowledge of the TOE, windows of opportunity and available equipment. The higher AVA_VAN component, the higher values of the mentioned parameters are considered for the attacker. The [CEM2022] defines the bounds of attack potentials that fall under the scope of each AVA_VAN component.
b) The amount and depth of the information about the TOE (e.g. design, implementation representation) that is available to the evaluator when performing the vulnerability analysis.

The two assurance levels considered in EUCC directly map with the AVA_VAN levels of the Common Criteria: substantial level maps with AVA_VAN.1 and AVA_VAN.2, while high level maps with AVA_VAN.3 to AVA_VAN.5.

Proposal

The Security Target of the TOE, and therefore the evaluation, shall include the assurance component AVA_VAN.1 or higher.

Guidance

Any EUCC evaluation with assurance level “substantial” or “high” will immediately fulfils this requirement.

ESR (2)(b)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

(b) *be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;*

Analysis

Secure configurations are contemplated in EUCC as part of the assurance component AGD_PRE.1. This component describes the requirements that manufacturers need to include in the preparative guidance of the TOE, which is a specific part of the guidance aiming to provide instructions for secure acceptance, secure configuration and secure installation of the TOE. As a result of end-users following these instructions, the delivered product transitions to a secure state (e.g. by having the administrator disabling unused network ports or insecure communication interfaces). In fact, the product is considered to be in its evaluated configuration only after such preparative steps have been followed. After that, then the TOE can move to operational use stage.

It must be considered that CC allows TOEs to be delivered in a state that is not secure by default at the moment of delivery. For example, the product might be configured by default with enabled insecure interfaces, weak initial passwords, or non-recommended cryptographic algorithms used to protect communications. The purpose of AGD_PRE.1 in this situation is forcing the user to modify that initial configuration and replacing it by a one that is secure.

As such, AGD_PRE.1 ensures that the TOE is in a secure state after following the preparative guidance and before being ready to operational use. However, the requirement states that the TOE needs to be delivered in a secure by default configuration. The way that CC contemplates the delivery and acceptance flow of the product to end-users does not guarantee that the TOE is delivered in a secure state. In fact, in some cases, the TOE needs to be put in a secure configuration by the end-user, after delivery, and by following the preparative instructions included in AGD_PRE.

This CRA requirement assumes until certain extent that users could put the product into operation before having followed the security guidance for secure installation and configuration, with risk that they could deploy it in an insecure configuration with potential adverse impact for the product itself or other entities in the environment.

Since the requirement strictly mandates a secure configuration at the moment of delivery, then there is no EUCC requirement that matches the CRA requirement. In this case, it would be needed to create an ad-hoc extended assurance component in order to meet this requirement.

An extended component forcing the product to be delivered in a secure-by-default state could translate into several different possibilities depending on the type of products and the functionality that it offers. It could contemplate ranging from delivering the product with all interfaces disabled except those strictly required to complete the initial configuration, through pre-establishing secure cryptographic algorithms, key lengths and key provisioning, to limiting the initial functionality to a minimum that does not compromise security, until further configurations are carried out. In short, the details on how this requirement is addressed by manufacturers is largely dependent on the type of technology, and it would not be affordable to create a detailed assurance component that covers all possible scenarios. Therefore, the requirement needs to be defined in a generic way, providing some additional guidance (e.g. typical examples), to manufacturers on how to address it.

A proposal for this requirement is given in the section named **"Security Architecture with default secure configuration (ADV_ARC.2) – Extended."**

The following additional analysis cover the second part of the requirement stating that the product shall include the possibility to reset to its original state (which would match with the secure-by-default initial configuration). The function to reset the TOE to is default state can be included as a management action within the SFR *"FMT_SMF.1 Specification of Management Functions"* from [CC2022P2]. This SFR is included in ST to indicate which management functions are provided by the TOE. These functions are interfaces that allow, according to [CC2022P2] administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery.

This SFR includes an assignment that is used to indicate the management functions that are in scope of the evaluation. In order to comply with this ESR, the assignment shall include a management function describing the possibility to return or reset the TOE to its default initial configuration.

On the other hand, the text of this requirement also allows for an exception when an agreement between a manufacturer and business user for a tailor-made product with digital elements, in which the implementation of this requirement could be skipped. In such cases, no equivalent SFR shall be added to the Security Target and a proof of the aforementioned agreement should be provided along with the Technical Documentation.

Proposal

The Security Target of the TOE shall include:

- The definition and instantiation of the extended assurance security requirement ADV_ARC.2 Security Architecture with Default Secure Configuration (Extended) as defined in the section named "**Security Architecture with default secure configuration (ADV_ARC.2) - Extended.**"

FMT_SMF.1 Specification of Management including in its assignment an explicit management function indicating that the TOE can be reset to its default configuration. Alternatively, these SFRs can be skipped if:

a) An agreement as mentioned in the ESR is provided with the technical documentation.
b) If the SPD in the ST identifies other measures in the operational environment that compensate the need for a secure default configuration, such as declaring an assumption for trusted administrators, ensuring that they shall receive the TOE perform a secure initial configuration following the AGD_PRE .1 guidance.

Note: the requirement secure default state/configuration could be covered by the definition of alternate SFRs and/or SARs that model equivalent functionality and associated assessment activities.

Guidance

When FMT_SMF.1 Specification of Management is included in the ST in order to comply with this CRA ESR, then the assignment in that SFR must include a management function indicating that the TOE can be reset to its default configuration.

If the ability to reset to default configuration needs to be restricted to certain user roles only, then the ST author should include in the ST the SFRs FMT_MOF.1 Component levelling and FMT_SMR.1 Security Roles together with FMT_SMF.1.

ESR (2)(c)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

Analysis

[CC2022P2] doesn't include at the date of release of this study any security functional requirement that fully addresses the installation of security updates in the TOE. EUCC, however, addresses **partially** this ESR with the technical mechanism included in [EUCC] section *IV.4 Patch Management*, with "*the technical mechanism and functions for the adoption of the patch into the ICT product*;". This technical management would ensure that the TOE incorporates functions that allow the installation of updates. However, s of the date of release of this report, [EUCC] doesn't further describe technical details of the technical match mechanism, and [EUCC] doesn't refer either to technical specifications describing such mechanism. Therefore it doesn't constraint aspects of the ESR under study such as:

- Automatic updates setting activated by default with automatic installation happening within an appropriate timeframe.
- An easy-to-use opt-out mechanism to disable automatic updates.
- Notification of available updates to users.
- An option to temporary postpone the updates.

Certain protection profiles in the industry define extended SFRs for the purpose of modelling updating functionalities on TOEs, as an example it can be mentioned the FPT_TUD_EXT.1 defined in the NIAP Protection Profile for Application Software [PP_APPSW]. However, the extended SFRs existing in the PPs of the industry reviewed during the elaboration of this study don't fully cover all the constraints and functional requirements on the updating mechanism.

Since [EUCC] provides a technical patch mechanism, this study encourages the usage of such mechanism so as to comply with this ESR. In order to do so, hereby we propose restrictions on the patch mechanism as an alternative. [EUCC] states in *IV. Patch management (4) the following:*

The patch management procedure for an ICT product will be composed of the following elements:

(a) the process for the development and release of the patch for the ICT product;

(b) the technical mechanism and functions for the adoption of the patch into the ICT product;

(c) a set of evaluation activities related to the effectiveness and performance of the technical mechanism.

In order to ensure compliance with this ESR, the mechanism in (b) shall include:

(1) Automatic updates enabled by default with installation of updates after a timeframe.
(2) An option to disable automatic updates.
(3) Notification of available updates to users.
(4) An option to temporary postpone the updates.

Proposal

The Security Target of the TOE shall include SFRs implementing the (technical) patch mechanism involved in EUCC's patch management procedure including or refined to include in the technical mechanism referred in [EUCC] IV.4 Patch management (4)(b):

a. Automatic updates enabled by default with installation of updates after a timeframe.

b. An option to disable automatic updates.

c. Notification of available updates to users.

d. An option to temporary postpone the updates to be installed when the automatic updates setting is enabled

Moreover, the Security Target shall include as well SARs implementing the patch management procedure, in the set of evaluation activities referred in [EUCC] IV.4 Patch management (4)(c):

a. With specific evaluation activities to assess during the EUCC evaluation the points (a), (b), (c) and (d) referred in the previous column.

Guidance

No further guidance is required.

ESR (2)(d)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

Analysis

CC includes families of Security Functional Requirements that directly model security features related to identification, authentication and authorisation through access control. They cover the generic features described by the requirement without the necessity of defining extended functional requirements.

In the case of the **identification mechanism**, there are two SFRs belonging to FIA_UID family in [CC2022P2] that require the TOE to implement user identification. “FIA_UID.2 User identification before any action” requires that users are identified before allowing any TSF-mediated action in the TOE on behalf of that user, while “FIA_UID.1 Timing of identification” allows to specify a subset of TSF-mediated actions that are allowed before user identification (in this case, those actions should have no security concerns with users incorrectly identifying themselves prior to being authenticated). The decision to use FIA_UID.1 or FIA_UID.2 should be technology-dependent as there are some technical scenarios in which it makes sense to allow a subset of actions before stating the claimed user identity, but there are others in which no action should be allowed before identification.

Authentication functionality is covered by Security Functional Requirements in family FIA_UAU of [CC2022P2]. Analogously to the identification case, there are two SFRs that serve to model this functionality. “FIA_UAU.1 Timing of authentication”, allows a user to perform certain actions prior to the authentication of the user's identity, whereas “FIA_UAU.2 User authentication before any action” requires that users are authenticated before any other action will be allowed by the TSF. The choice of one requirement or the other should be responsibility of the author of the ST, depending on the particular needs of the evaluated product. In any case, both SFRs are valid to meet the authentication part of the CRA requirement.

For both cases of identification and authentication SFRs, if the EUCC requirements are included in a Protection Profile or PP Module, CC 2022 allows to use optional conditional requirements. In this case, the PP can specify optional functionality, depending on whether the TOE implements it or not, then the ST author will choose between one SFR or another. In this case, the PP would specify that, if the TOE allows to perform TSF-mediated actions before user identification/authentication, then FIA_UID.2/FIA_UAU.2 can be included, otherwise FIA_UID.1/FIA_UID.2 will be included.

Regarding **access management**, CC includes a number of SFRs that are usually used together to model an access control Security Function Policy (SFP), which is a set of rules describing the specific security behaviour enforced by the TOE in the purpose of implementing an access control policy in terms of subjects, objects accessed by them, operations on the objects, security attributes, and rules for access. The minimum subset of those SFRs that would meet the access control part of the CRA requirement would be as follows:

- FDP_ACC.1: Subset access control, which requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.
- FDP_ACF.1: Security attribute-based access control, which allows the TSF to enforce access control based upon security attributes and named groups of attributes, and contemplates the ability to explicitly authorise or deny access to an object based upon security attributes.
- FIA_ATD.1: User attribute definition, that specifies the security attributes used to enforce the access control SFP.
- FMT_MSA.1: Management of security attributes, that allows authorised users (roles) to manage the specified security attributes.
- FMT_MSA.3 Static attribute, which ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.
- FMT_SMF.1 Specification of Management Functions, that requires that the TSF provide specific management functions associated to the access control policy.
- FMT_SMR.1 Security roles, that specifies the roles with respect to security that the TSF recognises, when they are used as an attribute to make decisions on the rules that are part of the SFP.

The above SFRs together comprise the minimal set of requirements that are needed in order to model an access control policy and, as a consequence, they need to be included in the Security Target. However, the core SFRs for such purpose are FDP_ACC.1 and FDP_ACF.1. The rest of them are dependencies of these ones that should be analysed and included or not on a per-case basis.

Regarding **notification of unauthorized access**, [CC2022P2] includes various security components in the class FAU that can model properly the functionality required to report on possible unauthorised access. First, *"FAU_GEN.1 Audit data generation"* is needed in order for the TSF to be able to generate audit records, it is to say, for example in the form of activity logs for several events, as it could be an unauthorised access attempt. Second, regarding how these generated events would lead to the actual detection of an unauthorised access event, there could be different options, and two are proposed in this study:

A) *"FAU_SAA.1 Potential violation analysis"* requires the TOE to be able to specify the set of auditable events whose occurrence or accumulated occurrence held to indicate a potential violation of the enforcement of the SFRs, as it could be certain number of unauthorized access attempts.

B) *"FAU_STG.1 Audit data storage location"* requires indicating where the TOE stores the generated audit records. It provides the PP/ST author with the option to specify that audit records are sent to an external IT entity through a secure channel. This could serve, for example, as a way to aggregate the audit records in an external IT to potential violation analysis. It must be noticed that, in this scenario, the operational environment of the TOE would potentially take responsibility for detecting those potential violation situations.

The combination of these two SFRs would enable the TOE to be able to detect possible events of unauthorized access and notify them through the audit trail.

Proposal

In order to meet this ESR, the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- In order to model user identification: FIA_UID.1 or FIA_UID.2.
- In order to model user authentication: FIA_UAU.1 or FIA_UAU.2.
- In order to model access management: FDP_ACC.1, FDP_ACF.1 . Other dependencies of these (FIA_ATD.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1 and FMT_SMR.1) should be analyzed and decided to be included or not on a per-case basis.
- For reporting unauthorized accesses: FAU_GEN.1 and either one of FAU_SAA.1 (for potential violation analysis to be carried out locally in the TOE) or FAU_STG.1 selecting the option to transmit the generated audit data to an external IT entity (for a potential violation analysis to be carried out by an external IT entity).

Note: authorization requirements could be also modelled using extended SFRs that define a straighter access-control mechanism suited for the particular use-case of the product. For example, a single extended SFR could describe an ad-hoc use case for

Guidance

Depending on the particular architecture and implementation of the product under evaluation, the ST author shall choose to include in the ST FIA_UID.1 or FIA_UID.2, depending on whether the TOE allows to perform a number of TSF-mediated actions on the half of the user before user identification

(FIA_UID.1 would be chosen), or no action is allowed before user identification (FIA_UID.2 would be chosen).

If FIA_UID.1 is claimed, then the Security Target author shall indicate in the assignment which TSF-mediated actions are allowed before user identification.

In the same way, the ST author shall choose between the inclusion of FIA_UAU.1 if a number of TSF-mediated actions are allowed on behalf of the user before user authentication, and the inclusion of FIA_UAU.2, if no actions are allowed before user authentication.

If FIA_UAU.2 is claimed, then the Security Target author shall indicate in the assignment which TSF-mediated actions are allowed before user authentication.

In FAU_SAA.1, the ST author shall indicate the subset of auditable events and related rules that would allow to conclude that an unauthorized access event has occurred.

In FAU_GEN.1, the ST author shall indicate that the TOE generates audit logs for detected or suspected unauthorized access events.

If FAU_STG.1 is used and the potential violation analysis performed to detect unauthorized access attempts is delegated to an external IT entity, then the ST author shall choose the option *"transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC"* in the selection of FAU_STG.1.

ESR (2)(e)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> (e) *protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;*

Analysis

Confidentiality of data is addressed by various SFRs defined in [CC2022P2] that cover protection of this security dimension when data is both on transit and at rest.

For protection of confidentiality of the data at rest, the FDP_SDC.1 Stored data confidentiality SFR requires protection of confidentiality of the user data while it is stored in different memory areas. This SFR provides some degree of flexibility in terms of which user data needs to be protected (e.g. the protection for that specific data will be verified during the evaluation), allowing to select all the user data controlled by the TOE, or only a subset of user data, that would be specified by the author of the Security Target in order to scope the confidentiality protection only to relevant portions of user data. On the other hand, it also allows to specify the memories in which the protection of user data confidentiality is implemented, allowing to choose between temporary memory, persistent memory, or any memory. This allows to cover also the case of confidentiality protection of the user data while it is being processed (e.g. while it is in RAM).

The confidentiality of data at rest in volatile or non-volatile memories can be provided by other security mechanisms depending on the use case. Below some of the most common ones are detailed:

- Memory encryption, through the implementation of cryptographic algorithms by means fo "FCS_COP.1 Cryptographic operation”. The assignments in this SFR shall be filled-in in order to indicate the cryptographic operation performed (e.g. encryption/decryption), algorithms implemented (e.g. AES-CBC), key sizes used (e.g. 256) and the list of standards with which the implemented algorithm is conformant (e.g., NIST SP 800-38A). FCS_COP.1 brings a chain of dependencies with other SFRs that should be either included or justified as not necessary in the PP/ST. In order to provide an effective protection, the algorithms used to protect the user data by cryptographic encryption techniques shall be robust enough. For instance, the guidelines of the SOGIS agreed cryptographic mechanisms guide [SOGIS_CRYPTO] should be followed in the selection of cryptographic algorithms dedicated to memory encryption.
- Isolation and/or access control to memory areas, through access control policies defined by “FDP_ACF.1 Security attribute-based access control” and “FDP_ACC.1 Subset access control” or controls in information flow between components and entities through “FDP_IFC.1 Subset information flow control” and “FDP_IFF.1 Simple security attributes”. These SFRs must be linked to an access control SFP or information flow control SFP that explicitly target the protection of the data stored in the TOE memories.
- Protection against physical attacks, specific for devices where potential attackers possess physical access to the TOE and the attack potential associated to them enables them to develop attack scenarios such as reverse engineering, manipulation of hardware in general or memory contents, probing on TOE physical surface, measurement of galvanic contacts, or attempts to perform leakage of information through covert channels, among others. Some of these are attacks appear specifically in scenarios linked to high-assurance evaluations in which the attack potential allows sophisticated techniques. Some examples of SFRs that could be used to protect against such attack scenarios are:
    a) FPT_PHP.3 “Resistance to physical attack” providing protection against threats such as side-channel attacks or fault injections.
    b) FDP_ITT.1 “Basic internal transfer protection” protecting confidentiality or integrity of user data when transferred between separate parts of the TOE.
    c) FPT_ITT.1 “Basic internal TSF data transfer protection”, protecting TSF data from disclosure or modification when transmitted between separate parts of the TOE.

The above SFRs can be included in an evaluation as an alternative or in combination with FDP_SDI.1 so any combination of them would be, in principle, a valid way to ensure confidentiality of data at rest.

Protection of confidentiality of data in transit is also contemplated by a number of SFRs included in [CC2022P2], part of the assurance class *FPT Trusted path/channels*. There are two specific cases in which data at rest needs to be protected according: when the data is transferred between the TOE and another IT entity, and when the data is transferred between the TOE and a user through a communication channel.

When the protection of the confidentiality in communications between the TOE and another IT product (e.g. a non-human entity, such as device, a running software, etc.) is applicable, then the SFR *FTP_ITC.1 Inter-TSF trusted channel*, needs to be included in the Security Target. This SFR requires the TOE to protect the communication between the TOE and the other IT entity in both confidentiality and integrity through the establishment of a trusted channel. The author of the ST shall specify in this SFR who, between the TOE and the other IT entity, is able to initiate the communication, and the list of functions for which a trusted channel is required.

The author of the ST should include one iteration of FTP_ITC.1 for each distinct IT entity in the operational environment with which the TOE establishes communications where the confidentiality of the transferred data needs to be protected.

When the communication of data that needs to be protected in confidentiality occurs between the TOE and a user (e.g. an administrator through a remote console), then the ST shall include the *FTP_TRP.1 Trusted path* SFR. This SFR requires the TOE to implement a trusted path with users in which the communication needs to be protected. This path includes identification of its endpoints. Also, the ST author shall choose in which dimensions the transferred information needs to be protected, and the SFR allows to choose between modification (integrity), disclosure (confidentiality), or other types of integrity or confidentiality protection, or a combination of them. In order to meet the CRA requirement under analysis, the ST author shall choose *disclosure* in the corresponding assignment of FPT_TRP.1 (note: modification shall be chosen as well, as it will help to cover the CRA requirement analysed in the following section). The author of the ST shall also indicate in the operations of FPT_TRP.1 if the protected communication is with local or remote users, which end points are entitled to initiate the communication, and for which services the trusted path is required).

The author of the ST should include one iteration (a different instance) of FPT_TRP.1 for each distinct communication channel between the TOE and users in the operational environment where confidentiality of the transferred data needs to be ensured.

In case that the EUCC requirements needed to comply with CRA are included in a Protection Profile or PP Module, the [CEM2022] allows to include in the Security Target the necessary SFRs, between FTP_ITC.1 and FPT_TRP.1, depending on whether the TOE implements functionality to communicate with trusted IT entities, with users, or with both, in communications where protection of the confidentiality is required.

Moreover, even when the FPT_TRP.1 and FTP_ITC.1 don’t have any dependency, the cryptographic mechanisms involved in the protection of the confidentiality of the communications should be part of the EUCC evaluation. For such purpose, the ST author should include the necessary iterations of FCS_COP.1 that model the cryptographic operations, key sizes and implemented standards, involved in the trusted channel or path. The below paragraphs indicate which considerations need to be taken into account and how to handle the dependencies of FCS_COP.1

It must be mentioned as well that some protection profiles in the CC industry include extended SFRs that model the communication of specific protocols protecting communication channels. For example, the NIAP’s Protection Profile for Application Software [PP_APPSW] defines:

- The extended SFRs FCS_HTTPS_EXT.1 and FCS_HTTPS_EXT.2 that model security aspects of an HTTPS communication channel.
- In the NIAP’s functional package [PPFP_TLS] defines FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1. for TLS communications and FCS_DTLSC_EXT.1 and FCS_DTLSS_EXT.1 for DTLS communications.

The inclusion of FCS_COP.1 in the Security Target leads to some dependent SFRs that need to be incorporated to the ST as required by [CC2022P2], depending on how the TOE generates or imports the keys used for the cryptographic operations related to protection of user data (at rest or in transit), and how the TOE performs cryptographic key access. The chain of dependencies is complex and will depend on the particular use case. This study won’t go deeper into details on these dependencies as it is somehow beyond its objectives, e.g., as long as the cryptographic mechanism SFR FCS_COP.1 is in the ST, then the CC rules enforce the inclusion of dependencies. However, the following can be mentioned for illustrative purposes:

- If the TOE generates the keys used in the cryptographic algorithms employed for protection of the user data, then *FCS_CKM.1 Cryptographic key generation* needs to be included, and it shall specify the cryptographic key generation algorithm, the key sizes supported in generation, and the standards used in generation. FCS_CKM.1 has other dependencies:
  a) FCS_RNG.1 Generation of random numbers, describing a robust random bit or number generation that supports the generation of cryptographic keys. **Note**: FCS_RBG.1 Random bit generation (RBG) could be included as an alternative to FCS_RNG.1, however it would lead to a more complex chain of dependencies with other SFRs that should be avoided, when possible, to keep simplicity.
  b) *FCS*_CKM.*6 Timing and event of cryptographic key destruction*, in which the ST author needs to specify the cryptographic keys that are destroyed by the TOE (the ones used for protection of data at rest or in transit, need to be indicated), the list of key destruction methods and associated standards used, and the timing in which the keys are destroyed.

- If the keys used for protection of the data at rest or in transit, are derived by the TOE, then the SFR *FCS_CKM.5 Cryptographic key derivation* needs to be included in the ST. This SFR shall indicate the type of keys that are derived, from which input parameters, the key derivation algorithm used, the sizes of the derived keys (matching with those keys used for protection of confidentiality of data at rest or in transit), and the list of standards used.
  a) If FCS_CKM.5 is added to the Security Target, then *FCS_CKM.6 Timing and event of cryptographic key destruction* needs to be included, and the specification of timing and destruction of the derived keys used for protection of confidentiality of data at rest or in transit need to be included.

- If the TOE does not generate or derive keys used for confidentiality protection of data, then FDP_ITC.1 or FDP_ITC.2 need to be included. One SFR or the other shall be included depending on whether the import of the keys includes security attributes linked to the keys or not.

- When FDP_ITC.1 or FDP_ITC.2 is included, then there are a series of dependencies that need to be added to the ST as well, linked to the access control policy linked to the security attributes or the trusted path or channel used for key importing. The analysis of those SFRs has been excluded from this section as it is a large chain of dependencies that are not related with the protection of the user data per-se. The ST author shall include the necessary dependencies according to what is specified in [CC2022P2].

- *FCS_CKM.3 Cryptographic key access* should be added to the ST optionally as it is only intended to allow for the specification of requirements on key usages outside the TOE, which is not supported by all TOEs. It requires access to cryptographic keys to be performed in accordance with a specified access method which can be based on an assigned standard. That key access method and the related standards need to scope the keys used for confidentiality protection of user data at rest or in transit.

As already mentioned, the above chain of dependencies is described with illustrative purposes and they won't be added to the list of minimum SFRs required to meet the ESR under study, that is summarized in previous sections of this study.

Proposal

In order to meet the Essential Cybersecurity Requirement (3), point (c) of Annex I, subclause "Security requirements relating to the properties of products with digital elements" of [CRA], the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- For the confidentiality protection of data at rest, this study proposes a combination of the following techniques and associated SFRs:
  - a) *FDP_SDC.1 Stored data confidentiality* to declare explicit confidentiality protection of the memory contents. It shall be included in the ST, indicating the user data that is confidentiality-protected and the memory areas where such protection is active while the data is at rest.
  - *b) FCS_COP.1 Cryptographic operation* providing memory encryption with robust cryptographic algorithms (i.e, according to [SOGIS_CRYPTO]).
  - *c)* Isolation and/or access control to memory areas (*"FDP_ACF.1 Security attribute-based access control"*, "FDP_ACC.1 Subset access control") or information flow controls ("FDP_IFC.1 Subset information flow control" "FDP_IFF.1 Simple security attributes") with specified SFPs targeting data in memories.
  - *d)* Protection against physical attacks and tampering, through one or more of FPT_PHP.3 "Resistance to physical attack", FDP_ITT.1 "Basic internal transfer protection", and FPT_ITT.1 "Basic internal TSF data transfer protection".

- For the confidentiality protection of data in transit between the TOE and another IT entity in the operational environment, FTP_ITC.1 Inter-TSF trusted channel needs to be included in the ST, with one iteration per communication channel with other IT entities in which the transferred data needs to be confidentiality-protected.
- For protection of the confidentiality of data in transit between the TOE and users, FTP_TRP.1 Trusted path needs to be added to the Security Target, with an iteration of this SFR for each distinct communication channel in which the confidentiality of the data needs to be protected. The ST author shall include "disclosure" in the selection of FPT_TRP.1.
- FCS_COP.1 needs to be added to the Security Target, describing the cryptographic algorithms, key sizes and standards involved in confidentiality protection of the data at rest and in transit. It involves a chain of SFR dependencies that need to be added, depending on the precedence of the keys used to perform cryptographic operations. It is up to the ST author to include the necessary ones.

Note: Trusted paths / channel requirements could be replaced by extended SFRs modelling exactly the protocol using for protection of communications. Moreover, if cryptography is not involved, or it is included in an alternative extended component, the FCS class requirements could be removed.

Also, some of the requirements proposed will be applicable or not depending on the functionality implemented by the product: e.g., if it does not implement communications, then FTP_ITC.1 will not be needed; if no storage of information is done, then FDP_SDC.2 won't be needed.

Guidance

FDP_SDC.1 shall cover each memory container for which confidentiality protection is implemented by the TOE. When data being processed needs to be protected, ST authors shall include in FDP_SDC.1 volatile memories (e.g. RAM) as target of the confidentiality protection.

When confidentiality of data in TOE memories is provided through access control or information flow control, then if FDP_ACC.1 and FDP_ACF.1, or FDP_IFC.1 and FDP_IFF.1 are included in the ST, then the access control SFP or information flow control SFP must target specifically the protection of the data in TOE memories. When the TOE communicates with other IT entities in the operational environment, ST authors shall add one iteration of FTP_ITC.1 in the ST for each distinct IT entity in the environment with which the TOE establishes communications where the confidentiality of the transferred data is protected by the TOE.

When the TOE communicates with users in the operational environment in the operational environment, ST authors shall add one iteration of FPT_TRP.1 in the ST for each distinct IT entity in the environment with which the TOE establishes communications where the confidentiality of the transferred data is protected by the TOE.

In FPT_TRP.1, the ST author shall explicitly select “disclosure” in the second selection of FPT_TRP.1.1 (along with “modification” in order to also cover the protection of the integrity of the data being transferred).

The author of the ST shall include one iteration of FPT_TRP.1 for each logically distinct communication channel between the TOE and users in the operational environment where confidentiality of the transferred data needs to be ensured.

When confidentiality of the data at rest or in-transit is protected by cryptographic algorithms, then an iteration of FCS_COP.1 need to be added for each of the algorithms involved in the protection. Additional SFRs shall be added to the ST depending on whether the keys used in these algorithms are generated by the TOE (FCS_CKM.1, FCS_RNG.1, FCS_CKM.6), if the TOE derives the cryptographic keys (FCS_CKM.5, FCS_CKM.6), or if the TOE imports the keys (FDP_ITC.1 or FDP_ITC.2, plus their chain of dependencies).

ESR (2)(f)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;*

Analysis

The analysis of this requirement is break-down according to how EUCC requirements can address its different parts. First, protection of the integrity of stored data is analysed, then protection of integrity of data and transit, and finally reporting of corruptions.

Integrity protection of data at rest of data is addressed by the FDP_SDI family included in [CC2022P2]. This family includes two SFRs: *FDP_SDI.1 Stored data integrity monitoring*, which requires the TOE to monitor integrity errors in containers controlled by the TOE, and *FDP_SDI.2 Stored data integrity monitoring and action*, which also requires the TOE to take actions as a result of an error detection.

Because the CRA requirement under analysis also includes the **report on corruptions**, it results more adequate to choose FDP_SDI.2 over FDP_SDI.1, as the first allows the ST author to indicate the actions to be taken upon detection of an integrity error, which can include also reporting the error. However, the managements actions of FDP_SDI.1, as described in [CC2022P2], include the generation of an audit record upon the event of a corruption (integrity error), although it is a recommendation and not a mandatory action. In this case, it shall be made mandatory to include in the Security Target a FAU_GEN.1 SFR including a compulsory event of integrity error reporting when a detection is triggered by FDP_SDI.1.

Depending on the type of product, it might be more convenient to choose a particular option between including FDP_SDI.1 or FDP_SDI.2 in the ST. This analysis considers that both options have the same potential to cover the requirement, and both are equally valid.

Lastly, both FDP_SDI.1 and FDP_SDI.2 are general enough to contemplate any type of protection of data stored in different containers or memories of the TOE, both non-volatile and volatile, which implicitly covers data being processed (e.g. when it is held in volatile RAM).

Regarding **protection of the integrity of data in transit**, the analysis is similar to that carried out in the previous section for protection of the confidentiality. Depending on which entities need to communicate with the TOE (IT entities or users in the operational environment), for transmissions that require protection of the data transferred, the ST author shall add iterations of FTP_ITC.1 or FPT_TRP.1.

FTP_ITC.1 covers protection of both confidentiality and integrity of the data transferred, whereas FPT_TRP.1 requires the ST author to explicitly select "modification" in the second selection of FPT_TRP.1.1 (along with "disclosure" in order to also cover the protection of the confidentiality of the data being transferred). As in the analysis of the confidentiality, one or other SFR shall be chosen depending on whether the communications are carried out with IT entities or with users.

Reporting of integrity errors detected on communications is not covered by either FTP_ITC.1 or FPT_TRP.1. For this reason, the ST author would need to include in the Security Target the **FAU_GEN.1 SFR,** with a mandatory generation of audit records upon integrity detection errors on communications.

As in the previous requirement, other options existing in the CC industry for specific communication protocols could be used, like those for HTTPS channels from [PP_APPSW] or TLS/DTLS channels from [PPFP_TLS].

Lastly, if the cryptographic mechanisms involved in integrity protection of data at rest or in transit could be included in the evaluation by including the necessary iterations of FCS_COP.1 and its related dependencies. The analysis done for the inclusion of this requirement in the previous section still holds, considering that it shall scope the cryptographic algorithms, key sizes, key handling methods and standards of related to protection of data integrity.

Proposal

In order to meet this ESR, the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- For the integrity protection of data at rest, two alternatives exist:

a) Inclusion FDP_SDI.1 Stored data integrity monitoring, plus FAU_GEN.1 Audit data generation refined so that generation of audit records upon integrity error detection on stored data is mandatory.

b) Inclusion of FDP_SDI.2 Stored data integrity monitoring and action, and the ST author shall indicate in the assignment of FDP_SDI.2.2 that integrity error detection shall be reported.

- For the integrity protection of data in transit between the TOE and another IT entity in the operational environment, FTP_ITC.1 Inter-TSF trusted channel needs to be included in the ST, with on iteration per communication channel with other IT entities in which the transferred data needs to be integrity-protected.
- For integrity protection of the integrity of data in transit between the TOE and users, FTP_TRP.1 Trusted path needs to be added to the Security Target, with an iteration of this SFR for each distinct communication channel in which the integrity of the data needs to be protected. The ST author shall include “modification” in the selection of FPT_TRP.1.1.
  FCS_COP.1 needs to be added to the Security Target, describing the cryptographic algorithms, key sizes and standards involved in integrity protection of the data at rest and in transit. It involves a chain of SFR dependencies that need to be added to the ST according to the particular case.

Note: Trusted paths / channel requirements could be replaced by extended SFRs modelling exactly the protocol using for protection of communications (as those in some NIAP protection profiles). Moreover, if cryptography is not involved, or it is included in an alternative extended component, the FCS class requirements could be removed.

Also, some of the requirements proposed will be applicable or not depending on the functionality implemented by the product: e.g., if it does not implement communications, then FTP_ITC.1 will not be needed; if no storage of information is done, then FDP_SDI.1 won’t be needed.

Guidance

If the ST author chooses to include, for integrity protection of data at rest, FDP_SDI.1 along with FAU_GEN.1, then FAU_GEN.1 shall include generation of records upon detection of an integrity error of stored data carried out by FDP_SDI.1. Otherwise, if the ST author chooses to include FDP_SDI.2 alone for integrity of stored data, then the assignment of FDP_SDI.2.2 shall indicate that integrity error reporting is performed as response to a detected integrity error on stored data.

Either way, FDP_SDI.1 or FDP_SDI.2 shall list all the containers for which the integrity of stored data is monitored by the TOE. If the monitoring of integrity of processed data is applicable, then FDP_SDI.1 or FDP_SDI.2 shall include the user data attributes in volatile memory that they monitor.

When the TOE communicates with other IT entities in the operational environment, ST authors shall add one iteration of FTP_ITC.1 in the ST for each distinct IT entity in the environment with which the TOE establishes communications where the integrity of the transferred data is protected by the TOE.

When the TOE communicates with other IT entities in the operational environment, ST authors shall add one iteration of FPT_TRP.1 in the ST for each distinct IT entity in the environment with which the TOE establishes communications where the integrity of the transferred data is protected by the TOE.

The author of the ST shall include one iteration of FPT_TRP.1 for each logically distinct communication channel between the TOE and users in the operational environment where confidentiality of the transferred data needs to be ensured.

In FPT_TRP.1, the ST author shall explicitly select "modification" in the second selection of FPT_TRP.1.1 (along with "disclosure" in order to also cover the protection of the confidentiality of the data being transferred).

FAU_GEN.1 shall include the generation of records for the event of detection of integrity violation in FTP_ITC.1 or FPT_TRP.1 (whichever is included in the ST).

When integrity of the data at rest or in-transit is protected by cryptographic algorithms, then an iteration of FCS_COP.1 need to be added for each of the algorithms involved in the protection. Additional SFRs shall be added to the ST depending on whether the keys used in these algorithms are generated by the TOE (FCS_CKM.1, FCS_RNG.1, FCS_CKM.6), if the TOE derives the cryptographic keys (FCS_CKM.5, FCS_CKM.6), or if the TOE imports the keys (FDP_ITC.1 or FDP_ITC.2, plus their chain of dependencies).

ESR (2)(g)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

(g) *process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (minimisation of data);*

Analysis

The current set of security functional requirements or security assurance requirements of [CC2022P3] does not include any component that covers functionality related to data minimisation. Therefore, the definition of an extended requirement is necessary in order to achieve the necessary coverage.

The requirement focuses in data processing, which can be seen as a data proceeding from or acquired by input interfaces to the product and that could be potentially outputted through output interfaces of the product. Due to the nature and the wide scope of the intention behind the requirement, and given the complexity of the architectures of certain products, designing an extended SFR for this feature would result in scenarios where it would be extremely difficult, if not unfeasible, to perform adequate testing of a requirement implemented by the TOE. For example, complex TOEs with multiple parts, different storage containers, multiple processing units and several transmissions of data between internal TOE components, or between the TOE and external parties, would lead to increasing difficulty in the verification of the requirement, in a way that is proportional to the complexity of the TOE architecture. Moreover, while transfer of information between the TOE and non-TOE entities might be potentially part of this requirement (in the hypothetical scenario where the communication channels allow to disclose the transferred information), it might happen that an interface for verification of internal transfers or internal processing does not simply exist.

According to this reasoning, it could be a more feasible approach to require the vendor to provide documentary evidence describing the details of the internal and external flows of data transfers and processing, enumerating all data involved and specifying the paths that such information travels during its lifespan. This evidence could also include a developer's rationale demonstrating why the set of data processed by the TOE is minimal in relationship with the intended use of the TOE.

This would lead to the definition of an extended Security Assurance Requirement linked to the TOE design, hence belonging to the ADV class. The definition would include the assurance activities for evaluators to conduct on the related evidence describing data minimisation in the design and a justification of minimality, so that they can judge whether the processing of each type of data done by the TOE is justified.

In order to capture the requirements for the vendor evidence and for the evaluator assessment, the ADV class have been extended in order to include extended family *ADV_PDM Processed data minimisation* and the component ADV_PDM.1 of the assurance family Processed d*ata minimisation (ADV_PDM) – Extended*. The complete definition of this class is included in the section named "***Processed Data Minimisation (ADV_PDM) – Extended***" of this document.

The approach chosen in the definition of ADV_PDM class focuses on examination of the user interfaces (e.g., API functions) described in AGD_OPE user operational guidance evidence, which contains information at high-level on all the user-accessible interfaces of the product.

Proposal

In order to meet this ESR, the Security Target of the TOE shall define and include the extended assurance family ADV_PDM, as described in the section named "***Processed Data Minimisation (ADV_PDM) – Extended***". The ST shall instantiate the ADV_PDM.1 extended component.

The vendor shall prepare the rationale for minimisation of data, as described in the definition of the ADV_PDM family.

Note: The minimization of data could be also achieved by defining other alternative extended SARs containing assurance activities that ensure data minimization.

Guidance

Manufacturers should provide in the technical documentation a rationale for data minimisation, indicating which data is processed by the TOE, and the input/output user-accessible interfaces of the user operational guidance used for inbound or outbound transmissions of such data.

ESR (2)(h)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> (h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

Analysis

[CC2022P2] includes requirements in the family FRU_FLT: Fault Tolerance, that are meant to require the TSF to ensure the operation of a number of capabilities upon a list of failures. This family has two components: FRU_FLT.1 Degraded fault tolerance, that permits to specify a list of essential capabilities that the TOE shall maintain during a failure situation, and FRU_FLT.2 Limited fault tolerance, requiring the TOE to maintain all its capabilities during a failure situation.

Among them, FRU_FLT.1 Degraded fault tolerance seems to be a more reasonable option, as it would be too ambitious to require maintaining the full operation of all capabilities of the TOE in failure situations for any type of product. Therefore, this SFR is chosen to cover part of the CRA requirement under analysis.

In FRU_FLT.1, the author of the ST shall indicate the list of capabilities that the TOE shall maintain upon a failure situation, as well as the type of failures in which those capabilities are maintained. In order to comply with the CRA requirement, the ST author should indicate, when applicable, in the second assignment of this SFR that denial of service attacks is one of the failure situations in which the TOE can still offer some capabilities, as a mitigation strategy for those attacks.

Adding FRU_FLT.1 to the ST introduces the dependency of FPT_FLS.1, Failure with preservation of secure state SFR, which requires the TOE to preserve a secure state when certain types of failure (to be chosen by the ST author) occur. The ST author would need to add FPT_FLS.1 to the Security Target and include in the open assignment at least denial of service attacks as one type of failure upon which the TOE shall preserve a secure state.

Proposal

In order to meet this ESR the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- FRU_FLT.1 Degraded fault tolerance, and the ST author shall include in the types of failure, at least, denial of service attacks.
- FPT_FLS.1 Failure with preservation of secure state, and the ST author shall include in the types of failure, at least, denial of service attacks.

Note: alternatively, other extended SFRs modelling protection of the TOE against DoS attacks could be defined and used by the manufacturer.

Guidance

When protection against denial-of-service attacks is implemented by the TOE, the second assignment of FRU_FLT.1 shall indicate that denial of service attacks is one of the failure situations in which the TOE can still offer some capabilities. Other capabilities that the TOE maintains upon a failure situation shall be added to this SFR as well.

In the same manner, the ST author shall indicate in FPT_FLS.1 assignment denial of service attacks as type of failure upon which the TOE maintains a secure state.

Note: it must be noticed that this ESR depicts and addresses a threat scenario that could be very specific, for example due to DoS attacks being not applicable to a wide variety of IT scenarios. As such, the ST author must consider that this ESR might be deemed as not applicable through the corresponding risk assessment and, therefore, the proposed SFRs wouldn't be needed in the EUCC evaluation.

ESR (2)(i)

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;*

Analysis

This requirement refers to the adverse scenario in which an attacker could use the TOE, e.g. by managing to execute code in it, with the intent of attacking other devices or systems in the environment.

Currently, there isn't any requirement in the [CC2022P2] that models this specific type of protection or use case. However, the protection against misuse of the TOE in this scenario can be achieved by ensuring the integrity of the TOE code, in order to detect and react to manipulations of the code run in the TOE that could be used to potentially execute malicious code that affects other IT entities in the operational environment.

The verification of the integrity of the code can be done at startup, during operation, on-demand or under other conditions, and it aims to ensure the correct operation of the TOE, including the detection of possible manipulations. The verification could also consist in an authenticity check (e.g. by checking a digital signature), that also would detect modifications in the TOE code.

This protection can be achieved by using various SFRs of the class FPT, that are defined in [CC2022P2].

First, FPT_INI.1 TSF initialisation requires the TOE to provide a TSF initialisation function that brings the TSF into a secure operational state at power-on. This secure state can include a verification of the authenticity, integrity or correct version of the TOE code (e.g. the firmware, software), or even the TOE data. FPT_INI.1 also requires that the initialisation function of the TOE is self-protected for integrity and authenticity. Moreover, it allows to indicate the actions to carry out upon the detection of an error (e.g. halting or booting with reduced functionality), with flexibility to specify different types of behaviour.

Second, FPT_TST.1 TSF self-testing, provides the ability to test the TSF's correct operation. These tests can be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and TSF itself. This SFR requires the TOE to run a suite of self-test that can be executed during initialisation, periodically, at request of the users, or under other conditions, and allows to specify the self-tests that need to be run. This SFR also allows to indicate whether the full TSF or parts of the TSF are tested, as well as if the full TSF data or only parts of it are tested.

The author of the ST should include FPT_TST.1 in the Security Target and the SFR should force self-tests to be executed at least during boot and, on products intended to run during long periods and with access to the network, also periodically. The list of self-tests run should cover at least the integrity of the TOE code and, possibly, monitoring of TOE communications during runtime to detect possible anomalous behaviour.

This ESR also refers to the capability of the product with digital elements of minimising the impact by "connected devices" and is not limited by that on the TOE itself. Although using an appropriate combination of SFRs in CC it is reasonable to achieve certain degree of protection in the TOE itself, controlling the behaviour of other devices connected to the TOE is not a feasible objective to be meet in a general manner for any kind of ICT product. This feature makes sense exclusively for those products that have a dedicated role of controlling the activities of the devices in the network, such as perimetral protection systems, IDS or IPS products, for example filtering or limiting the outbound connection of such devices.

[CC2022P2] includes some SFRs that are quite flexible and permit to model protection against Denial-of-Service attacks in the network, for cases here the TOE implementing such protection is meaningful. That protection would be provided by means of filtering certain flows of information based on determined attributes or parameters, as those that could identify an attack of this type. The following SFRs are candidates for this purpose:

- *FDP_IFC.1 Subset information flow control* to establish a security functional policy determining the allowed flows of information. These can be made dependent on parameters of the network traffic indicative a possible DoS attack from an entity in the network.
- *FDP_IFF.1 Simple security attributes* is used to define those attributed based on which the network traffic would be allowed or denied, e.g., if they are suspicious of constituting an attack from a device in the network.

This study also considers and recommends the usage of other extended components in mature and consolidated protection profiles in the industry, that are usually employed in specific use cases such as firewalls or IDS, and that are recognized by the industry:

- In the case of firewall products, the requirement FFW_RUL_EXT.1 from the NIAP's approved collaborative Protection Profile for Stateful Traffic Filter Firewalls [CPP_FW].
- In the case of IDS products, the requirements of the extended assurance class IPS of PP-Module for Intrusion Prevention Systems (IPS) [PPMOD_IPS].

Proposal

In order to meet this ESR, the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- FPT_INI.1 TSF initialisation. The ST author shall indicate in the operations the properties to be checked, including at least the integrity of the TSF code, as well as the actions carried out to respond failures during initialisation.
- FPT_TST.1 TSF self-testing: ST authors shall indicate in the operations that self-tests are run at least during initial start-up and, for connected systems, periodically during normal operation. They shall indicate as well in the operations the list of self-tests that are performed in order to ensure that the TOE is not used or has not been altered to maliciously attack other entities in the network.
- In specific cases where the TOE can control the activity of devices connected to it (e.g., in the same network), in order to prevent these devices to perform a negative impact in the network, the ST shall incorporate FDP_IFC.1 Subset information flow control and FDP_IFF.1 Simple security attributes, or alternatively, applicable SFRs from [CPP_FW] or [PPMOD_IPS], depending on the type of product, that implement the same functionality.

Guidance

ST authors shall indicate in FPT_INI.1 as properties to be checked, the integrity of the TSF code, as well as the actions carried out to respond failures during initialisation.

In FPT_TST.1, ST authors shall indicate in the operations that self-tests are run at least during initial start-up and, for connected systems, periodically during normal operation, along with the operations the list of self-tests that are performed in order to ensure that the TOE is not used or has not been altered to maliciously attack other entities in the network.

When ST authors include the FDP_IFC.1 and FDP_IFF.1in the ST, a security functional policy must be defined, with a series of attributes in which it is decided whether the traffic of the devices in the network is allowed or not, e.g., as those indicative of a possible DoS attack.

ESR (2)(j)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(j) be designed, developed and produced to limit attack surfaces, including external interfaces;*

Analysis

This requirement refers to design principles that shall be taken into account by the developer during the design of the TOE. Given the nature of the requirement, it should be addressed by assurance components to be evidenced by the vendor, and it is not suitable to be covered with security functional requirements, since the related design principle is not an observable property that can be modelled by any of the SFRs in [CC2022P2] or with any other extended SFR that could be defined ad-hoc.

The list of SARs in [CC2022P3] does not include currently any assurance requirement that explicitly requires a limitation of the attack surface in the TOE. However, the ADV assurance class includes multiple families and components that require the evaluators to assess the design of the TOE, including accessible interfaces. The most relevant family in this component would be *ADV_FSP functional specification*, which manufacturers to describes the external interfaces to the TSF (that can be directly used as attack surface) and evaluators to assess them during the evaluation.

During the vulnerability analysis required by the AVA_VAN assurance family (Vulnerability Analysis), evaluators are tasked with performing a vulnerability assessment. An AVA_VAN component is included in the evaluation to ensure that the TOE's attack surface does not expose any exploitable vulnerabilities. The thoroughness of the vulnerability assessment depends on the AVA_VAN level selected for the evaluation, with higher levels incorporating more detailed information about the TOE (e.g., TOE design details). For the purposes of compliance with the ESR under review, AVA_VAN.1 is considered sufficient as the assurance component.

The interfaces of the TOE play a crucial role in the vulnerability assessment associated with AVA_VAN. Although AVA_VAN.1 does not require a detailed review of the TOE design, it does rely on the ADV_FSP functional specification, Security Target, and user guidance (in line with dependencies on ADV_FSP.1, AGD_OPE.1, and AGD_PRE.1). The user guidance, as required by AGD_OPE.1, must include a description of the user-accessible interfaces of the product, which often overlaps with the interfaces listed in the ADV_FSP.

While a more in-depth analysis of the attack surface would be more effective with additional TOE design details in the AVA_VAN analysis, AVA_VAN.1 sufficiently ensures that the interfaces specified in the ST, AGD_OPE.1 guidance, ADV_FSP.1, and the information presented in the ST are considered during the vulnerability survey and penetration testing. For instance, if the TOE exposes an unnecessary interface that implements a vulnerable protocol, the AVA_VAN.1 analysis should be sufficient to identify such an interface and assess whether it is exploitable.

surface that takes into account if the resulting attack surface of the TOE present vulnerabilities.

Therefore, products that are meant to meet this CRA requirement using the EUCC, shall undergo an EUCC evaluation including at least the AVA_VAN.1 assurance component, together with ADV_FSP.1 and AGD_OPE.1.

Proposal

In order to meet this ESR, EUCC evaluations need to include the following assurance components:

- AVA_VAN.1 Vulnerability survey
- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance

The necessary ADV_FSPADV_TDS, ADV_FSP and ADV_ARC dependencies of the chosen AVA_VAN component shall be included in the evaluation, and the related design evidence will be used as part of vulnerability analysis to determine that the attack surface is limited and not vulnerable.

Guidance

No additional guidance is required.

ESR (2)(k)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;*

Analysis

The coverage of this requirement can be achieved through a combination of security functional requirements in [CC2022P2] and assurance components of the evaluation included in [CC2022P3].

First, the product should offer functional mechanisms to provide mitigation of the impact of incidents, meaning that the product implements functionality to detect and react to such incidents. In order to do so, the following SFRs need to be included in the Security Target (and the TOE needs to implement the functionality described by them).

First, *FPT_FLS.1 Failure with preservation of secure state* SFR, which requires the TOE to preserve a secure state when certain types of failure. These failures can correspond to detected attack events, and the assignment in this SFR should indicate in the ST to which incidents the TOE is able to react by maintaining a secure state, as a mitigation strategy.

Secondly, *FPT_RCV.1 Manual recovery* allows the TOE to react to failures or attacks by entering a *maintenance* mode, with the ability to return to a secure state with human intervention. It is possible also to use *FPT_RCV.2 Automated recovery*, which requires the TOE to return to a secure state using automated procedures (without human intervention) or *FPT_RCV.3 Automated recovery with undue loss*, where the recovery would be also automatic without exceeding a quantification of TSF data.

On the other hand, security assurance components in [CC2022P3] can ensure that the TOE is designed and produced in a way that contributes to mitigation of exploitation attacks.

The *ADV_ARC.1 Security architecture* assurance component requires the vendor to provide a description of the security architecture, in which it is described how the TOE protects itself from attacks such as tampering, TSF bypassing, and how it performs a secure initialisation and how separation of security domains is applied in the design. The principles expressed by the ADV_ARC.1 evidence show how the architecture of the product and its defence layers help to mitigate possible exploitations. The descriptions of the security mechanisms that comprise the security architecture is also supported in other design evidence such as that of ADV_TDS and ADV_FSP families.

Proposal

In order to meet this ESR, the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- FPT_FLS.1 Failure with preservation of secure state, indicating in the ST to which incidents the TOE is able to react by maintaining a secure state.
- FPT_RCV.1 Manual recovery, or a hierarchically higher component of FPT_RCV family.

Moreover, the following SARs from [CC2022P3] shall be included in the EUCC evaluation:

- ADV_ARC.1 Security architecture, along with the corresponding levels of ADV_TDS and ADV_FSP.

Guidance

ST authors shall indicate in FPT_FLS.1 to which incidents the TOE is able to react by maintaining a secure state.

Note: the security functionalities needed by FPT_FLS.1 and FPT_RCV.1 are specific for certain threat scenarios and IT systems, and could not be required in the general case. The manufacturer risk analysis shall assess where the implementation of those security functions is actually necessary in order to meet this ESR.

ESR (2)(l)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;*

Analysis

Generation of security-related information is covered by the *FAU_GEN.1 Security audit data generation* Security Functional Requirement, defined in [CC2022P2]. This component requires the TOE to record the occurrence of security relevant events that take place under TSF control, defines different levels of audits, and enumerates the events that shall be auditable.

FAU_GEN.1 requires, as a minimum, that the start-up and shutdown of the audit function is logged, as well as the auditable events for a selected audit level between minimum, basic, detailed or not specified level of audit. If other than “not specified” is selected in the operations of FAU_GEN.1, then

[CC2022P2] describes the events that should be recorded for each other SFR included in the Security Target. Moreover, ST authors can define other events to be recorded by the TSF.

An important factor to be considered is that, in previous sections of this document, it was mentioned that FAU_GEN.1 should be included in the Security Target with specific auditable events included in its operations. This shall be taken into account by ST authors.

The CRA requirement under analysis also mentions the need for recording the access to or modification of data, services of functions. In the CC terminology, this refers to management actions to administer the TOE or its functionality. Where applicable, the ST authors should include the SFR *FMT_SMF.1 Specification of Management Functions* that allows to indicate which are the management functions that the TOE allows to be performed by administration. The assignment in this SFR shall be filled to indicate the relevant administration or configuration of the product functions that need to be logged.

On the other hand, this ESR requires an "opt-out" mechanism to disable the audit generation function. While in certain security scenarios disabling the audit is a risky practice, it is possible to use technical elements in the CC to model this functionality. Superficially, using *FMT_MOF.1 Management of security functions* components, it is possible to indicate that certain roles can be able to disable and enable the audit function of the TOE. This requirement includes two dependencies:

- *FMT_SMF.1 Specification of Management Functions*, already mentioned. It would be necessary to indicate in this SFR, by the specific assignment, that the enablement and disablement of the audit function is one of the management actions that can be carried out.
- *FMT_SMR.1 Security Roles,* in order to specify which roles have the capability to disable or enable the audit function. Security-wise, it would be a bad practice not segregating this capability through roles.

Lastly, the inclusion of FAU_GEN.1 to the Security Target requires to either include *FPT_STM.1 Reliable time stamps*. The ST author may choose to either include this SFR, if the TOE is able to generate reliable timestamps, or to justify that the requirement is not necessary, if correctness of time is not an issue for the TOE.

Proposal

In order to meet the Essential Cybersecurity Requirement (3), point (j) of Annex I, subclause "Security requirements relating to the properties of products with digital elements" of [CRA], the Security Target of the TOE shall include the following SFRs from [CC2022P2]:

- *FAU_GEN.1 Security audit data generation* needs to be included in the Security Target. The author of the ST needs to fill in the assignments the auditable events specific to the security-relevant events, as well as contemplate the events related to the functionality described by other SFRs in the Security Target. In particular, the management actions of FMT_SMF.1 need to be included in the list of events recorded by FAU_GEN.1.
- FMT_SMF.1 Specification of Management Functions needs to be included in the Security Target, indicating in the assignment those management actions that are available to administrators and that are subject of being recorded by FAU_GEN.1, and indicating as well, that administrators (or other applicable roles) can disable and enable the audit generation function.
- FMT_SMR.1, indicating the roles that are allowed to enable or disable the audit function.

Guidance

ST authors shall include in FAU_GEN.1 generation of records for security-relevant auditable events in relation with the TOE functionality. Moreover, it shall include generation of security-relevant events related with other SFRs in the Security Target, at least the management actions in FMT_SMF.1.

ST authors shall specify in FMT_SMF.1 the management functions available to administrators that are subject to be logged in FAU_GEN.1.

ST authors shall specify in FMT_SMF.1 that administrators (or an equivalent role) are able to enable and disable the audit function.

ST authors shall indicate in FMT_SMR.1 which roles can exercise each of the management actions (including the ones enabling/disabling audit function) in FMT_SMF.1.

ESR (2)(m)

Requirement

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: […]

> *(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.*

Analysis

This requirement can be break down into t parts. The first one would refer to providing a mechanism for allowing users to delete from their product their data and settings. The other one would be transferring data to other products or systems, when possible, in a secure manner.

Regarding deletion of the data and settings upon request of the user, this security behaviour can be modelled as specific management actions through the SFR *"FMT_SMF.1 Specification of Management Functions"*. This SFR allows to specify a particular management function that would allow the erasure of the data or settings upon request of the user.

Some PPs in the industry have defined purpose-specific extended SFRs, such as [CPP_HARDCOPY] which includes "FPT_WIPE_EXT.1 Data Wiping". However, this study offers the proposal for a more generic extended SFR to be usable without the need for a specific technological context as per the above proposal.

Since this ESR requires the erasure to be permanent, the requirement *"FDP_RIP.1 Residual Information Protection"* would ensure that no residual information can be recovered after the deletion of the data or setting. This requirement should be refined to indicate explicitly that it scopes explicitly the data or settings removed upon request of the user.

With **regards to the second part of the requirement, transferring the data t**o other products or systems, it can be met with the joint effort of two SFRs in [CC2022P2].

For this option, it is also required to include in the ST "FMT_SMF.1 Specification of Management Functions", this time with a management function that would allow users to transfer data or settings to another entity.

First, *FDP_ETC.1 Export of user data without security attributes* allows to the TSF to export user data (e.g., personal data or settings) outside the TSF, and it does so by enforcing an appropriate security policy. This security policy may define factors such as which users are allowed to export which data, e.g., to prevent a user exporting the data, and it shall be defined by the author of the ST according to the particular use case. Moreover, FDP_ETC.1 requires the data to be exported without security attributes (e.g., identity of the user owning the data, or encryption according to user's key), but it might result more convenient to maintain those attributes upon export, in which case the ST author should use *FDP_ETC.2 Export of user data with security attributes.* In both cases, it is required to define a security policy with the dependencies on the components FDP_IFC.1 or FDP_ACC.1, but that won't be analyzed in-depth in this study.

The second SFR required is *FTP_ITC.1 Inter-TSF trusted channel*, already discussed in previous sections, that ensures that the TOE establishes a secure channel between the TOE itself and the entity receiving the exported data.

Proposal

In order to meet this ESR, the Security Target shall include the following SFRs:

- **For removal of data:**
  a) *FMT_SMF.1 Specification of Management Functions*, with a specific management function allowing users to remove their user data or settings from the TOE.
  b) *FDP_RIP.1 Subset residual information protection*, to ensure that the removed data or settings are permanently deleted.
- **For transfer of data to another system:**
  a) FMT_SMF.1 Specification of Management Functions, with a specific management function allowing users to transfer their data or settings outside the TOE.
  b) One of *FDP_ETC.1 Export of user data without security attributes* or *FDP_ETC.2 Export of user data with security attributes*, depending on whether the export requires security attributes of the user data to be kept or not.
  c) *FTP_ITC.1 Inter-TSF trusted channel* to establish a secure channel between the TOE and the entity where the data is exported.

Guidance

The ST author shall specify in FMT_SMF.1 assignment a function that allows users to remove their data or settings (indicating further details on such operation if needed) and, if the TOE allows exporting the data or settings outside the TOE, this SFR shall include as well another management function indicating that users can transfer out such data and settings.

FDP_RIP.1 shall be refined to indicate that it refers to user data and settings when it comes to permanent removal.

If the TOE doesn't allow exporting the user data to another entity, then FDP_ETC.1 or FDP_ETC.2 and FTP_ITC.1 aren't required.

If FDP_ETC.1 or FDP_ETC.2 is included in the ST, then the ST author shall model with either FDP_ACC.1 or FDP_ICF.1 the security policy that determines the export of the data.

If FDP_ETC.2 is included in the ST, then the ST author shall indicate in it the security attributes that are exported with the data.

Note: the requirement for data removal other extended SFRs that define equivalent functionality. For example, for example, “FPT_WIPE_EXT.1 Data Wiping” from [CPP_HARDCOPY] would be also a valid way to meet this ESR.

1.2. CRA Annex I, Part II, ESRs

ESR (1)

Requirement

Manufacturers of the products with digital elements shall:

> *(1) identify and document vulnerabilities and components contained in the product with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;*

Analysis

Identification and tracking (including documentation) of the security vulnerabilities of the product is contemplated as part of the flaw remediation procedures required by the ALC_FLR.1 (or higher) component in the [CC2022P3]. ALC_FLR implicitly requires that the scope of the vulnerability tracking comprises the whole TOE, including the parts that comprise it such as third-party libraries.

The identification and tracking of the components containing in the TOE is covered as part of the assurance component ALC_CMS.2 (or higher), which require that the configuration item list of the TOE contains the “parts that comprise the TOE”, including a unique identification, their version, and the identification of the vendor. However, by solely including ALC_CMS.2 requirement in the evaluation, it is not possible to meet the part of the Requirement 1 of Annex I.2 of [CRA] referent to the software bill of materials, due to various reasons:

a. The configuration item list that could include the list of third-party software does not need to be presented in a machine-readable format.
b. It largely depends on the interpretation of each scheme whether the libraries used by the TOE that don’t result in a separate binary (e.g. when static linking is used) are considered as configuration items falling under the scope of ALC_CMS.2.

In consequence, ALC_CMS.2 does not provide full coverage of the CRA requirement under analysis and an alternate assurance requirement needs to be used. For this particular case, EUCC or CC do not contemplate the inclusion and tracking of the software bill of materials as part of the developer evidence in any other assurance family. Therefore, it is required to define an ad-hoc assurance component for this purpose.

In order to address this gap, the extended assurance component ALC_SBM has been defined in the section named “***Software Bill of Materials (ALC_SBM) - Extended***”. ALC_SBM.1 Software bill of materials extended assurance component then needs to be included in the scope of the evaluation.

Proposal

In order to meet this ESR, the EUCC evaluation and the Security Target of the TOE shall include:

- ALC_FLR.1 Basic flaw remediation or a hierarchically higher component of ALC_FLR assurance family.
- ALC_SBM.1 Software assurance requirement (Extended), indicating the machine-readable format in which the software bill of materials is presented.

Guidance

If bill of materials is meant to be made publicly available by the manufacturer, can be delivered as part of the ST (e.g. in an annex or in the TSS), or as a separate deliverable.

ESR (2)

Requirement

Manufacturers of the products with digital elements shall: […]

> *(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;*

Analysis

Regarding the procedures for managing vulnerabilities and providing patches for security vulnerabilities, the analysis performed for previous requirements is still valid, and it can be covered by a combination of the components of the ALC_FLR family in [CC2022P3], and the (technical) patch mechanism involved in EUCC's patch management procedure. As [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

However, this requirement also makes mandatory to address and remediate vulnerabilities (and hence distributing updates) without delay, in relation to the risk posed to the products. In order to address this aspect, there are two possibilities:

- The assurance component *ALC_FLR.3 Systematic flaw remediation* of [CC2022P3] includes a content and presentation element requiring a timely response to vulnerabilities as part of the remediation procedures: ("*ALC_FLR.3.6C: The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.*"). Including this SAR in the EUCC evaluation would address the necessity for addressing vulnerabilities without delay.
- The specific SARs of the (technical) patch mechanism involved in EUCC's patch management procedure – with those in [ISO_TS_9569] as a proposal-, but it shall be ensured that the chosen requirements include a mandatory maximum timeframe in which the vulnerabilities need to be fixed and updates issued, and the that timeframe shall be commensurate with the risk level associated to the update (e.g. as per specification of the vendor's patch policy).

Regarding the separation of functional updates from security updates, there is currently no assurance component in the [CC2022P3] that requires this kind of separation. While it is certain that the activities defined in ALC_FLR family scope the "security flaws" of the TOE, meaning in other words vulnerabilities and their remediation, the requirements in this family don't mandate a necessary separation in the distribution of security updates from other types of updates.

The Patch Mechanism in the EUCC doesn't establish this separation between types of updates either, at least in the version that is available at the date of publication of this report.

There would be two theoretical ways to address this gap:

a) Including this separation as a requirement in the next update of the EUCC Patch Management's text. However, it doesn't seem aligned with the general objectives of this mechanism to establish this separation.
b) To define an extended component in ALC_FLR family that specifically addresses this issue. However, that would require including several activities of ALC_FLR.3 that would overlap possibly some of the contents of the EUCC. Moreover, ALC_FLR family is more focused in how flaw reports are handled internally and less in how updates are distributed, as that aspect falls more under the scope of the EUCC Patch Management.

This study opts for the second options and, as such, the Extended SFR named "*ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended)*" has been defined in section "**ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended)**".

Proposal

In order to meet this ESR, the Security Target of the TOE shall include:

1. **either one of:**
   a) ALC_FLR.1 plus the assurance components of the implementing the (technical) patch mechanism involved in EUCC's patch management procedure -this study proposes to use those in [IS_TS_9569], including a patch policy that requires a timely response to discovered vulnerabilities.
   b) ALC_FLR.3 Systematic flaw remediation, which requires timely vulnerability fixing and distribution of updates to TOE users.
2. **And,** the extended SFR ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended).

Guidance

ST authors can choose between including in the ST either the combination of ALC_FLR.1 and the requirements in [EUCC] (provided that they include a patch policy that requires a timely response to discovered vulnerabilities) or, alternatively, just include ALC_FLR.3 in the ST.

ESR (3)

Requirement

Manufacturers of the products with digital elements shall: […]

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

Analysis

In the context of a EUCC evaluation, security review and testing are required during certain punctual points of the evaluation timeframe, but not as a continuous regular activity. AVA activities linked to the evaluation require the evaluators to conduct vulnerability analysis and penetration testing of the product. When components of the assurance class ATE are included in the evaluation, the developer performs functional testing of the TOE before releasing it, and the evaluators (through ATE_IND activities) perform independent functional testing as well.

From the perspective of the product lifecycle, ALC assurance class assesses the security of the product during its development, and it can include testing requirements whenever the product is released, on when existing functionality is modified or new functionality is introduced. For example, if a vulnerability is found and fixed, the new version of the TOE shall undergo testing before being released.

However, no requirements exist in EUCC or CC that mandate regular security review and testing of the TOE after the end of the evaluation. In order to achieve the required coverage, it would be needed to define an extended assurance component requiring that the developer performs periodic security testing on the TOE, even after it has been released to the customer. This requirement addresses new vulnerabilities that could appear after release or certification, or new attack techniques appearing in the state of art that render the certified TOE vulnerable. If the developers perform periodic testing, it gives them the opportunity to discover the vulnerabilities before end-users or malicious agents do.

In order to address this requirement, the assurance class ALC is extended to create a new family named *ALC_PSR: Periodic security review and testing of the TOE* that includes a requirement for the continuous security review and testing of the TOE after it is released.

Assessment of this requirement by evaluators will require the vendor to elaborate and provide internal policies or procedures for conducting periodic review of the TOE security and internal security testing. Such procedures shall be examined by the ITSEF in order to determine whether the developer is following a continuous security review strategy with the TOE.

The assurance component *ALC_PSR.1 Periodic security review and testing of the TOE* shall be included in the Security Target in order to achieve compliance with the CRA requirement under analysis. This requirement is defined in the section named "***Periodic Security Review and Testing (ALC_PSR) - Extended***".

Proposal

In order to satisfy this ESR, the EUCC evaluation and the Security Target of the TOE shall the extended assurance component ALC_PSR.1 Periodic security review and testing of the TOE (Extended) shall be defined and instantiated in the ST.

Guidance

When ALC_PSR.1 is included in the evaluation, manufacturers need to provide as evidence the procedures for periodic security review and testing of the TOE, such as records of exercising these procedures. If it's a newly developed TOE that hasn't undergo through security review and testing yet, and the developer has produced other similar products, then providing records for these procedures is accepted.

ESR (4)

Requirement

Manufacturers of the products with digital elements shall: […]

(4) *once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;*

Analysis

EUCC evaluations will be able to include the requirements of the assurance family *ALC_FLR Flaw Remediation* (defined in [CC2022P3]) as a requirement for vendors to implement security flaw management procedures. For the coverage of this particular requirement, the ALC_FLR.1 component would be sufficient, as it covers the different aspects of the Requirement 4, as explained below.

The content and representation requirement ALC_FLR.1.4C requires the vendor's flaw remediation procedures to describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. Moreover, ALC_FLR.1.1C requires tracking of all reported security flaws and ALC_FLR.1.2C mandates that the vendor maintains description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

Since ALC_FLR.1 requires the vendor to maintain and track all the relevant information about the vulnerability, and also requires to provide information about the flaw, guidance for mitigation and corrections to the TOE users, it can be sufficient as coverage of the CRA requirement under analysis.

Moreover, the information allowing the users to identify the product with digital elements affected can be considered as implicitly covered by ALC_FLR.1, which scopes the security flaws of the particular TOE under evaluation, and no other. In any case, this aspect needs to be made clear in the flaw remediation procedures of the vendor and, as part of the ALC_FLR assessment, these procedures should be examined to determine that the security flaws disclosed to user are univocally associated to the evaluation version of the TOE or that, at least, it is possible to univocally associate the flaw to a particular version or release of the TOE.

However, there is a nuance that could be open to interpretation. The CRA requirement states that the information about the vulnerabilities shall be publicly disclosed, whereas the ALC_FLR.1 only requires that it is disclosed to TOE users. It could be subject to discussion whether the distribution to TOE users can be considered as a public disclosure, however, it can be considered that once the information about the flaw crosses the boundary of the vendor's organisation it has been made public to a certain extent.

Moreover, the requirement opens the possibility for manufacturers to delay the publication of the information about the vulnerability until users had enough time to apply the patches. **Since this is a marginal case, and largely dependent on the individual vulnerability, that factor should not be considered by the general rules for compliance with this ESR through CC technical elements. Instead, it should be studied on a per-case basis by the Surveillance Authority whether it is justified is justified to exceptionally wait before releasing the information.**

Proposal

In order to this ESR, the Security Target of the TOE shall include the assurance component A*LC_FLR.1 Basic flaw remediation* or a hierarchically higher component of its family.

Guidance

When elaborating the ALC_FLR evidence, vendors should put special attention in ensuring that the flaw remediation procedures allow to match each security flaw and the information about it provided to TOE users with the particular identification of the TOE to which it applies.

ESR (5)

Requirement

Manufacturers of the products with digital elements shall: […]

> *(5) put in place and enforce a policy on coordinated vulnerability disclosure;*

Analysis

This requirement is directly covered by [EUCC] Article 8, point 6b requires the manufacturer to provide to the CAB "a description of the applicant's vulnerability management and vulnerability disclosure procedures.".

Proposal

No additional technical elements are needed.

Guidance

No additional guidance is required.

ESR (6)

Requirement

Manufacturers of the products with digital elements shall: […]

> *(6)* take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

Analysis

As in other requirements of Annex I.2 of [CRA], this requirement is directly covered within the assurance family *ALC_FLR: Flaw remediation defined* in [CC2022P3]. In particular, the assurance component *ALC_FLR.2 Flaw reporting procedures* introduces particular sub-requirements for the vendor to specify the means by which discovered vulnerabilities can be reported by end-users to the vendor.

The sub-component ALC_FLR.2.5 requires that the flaw remediation procedures describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE. Moreover, the sub-component ALC_FLR.2.8C requires that the flaw remediation guidance describes a means by which TOE users report to the developer any suspected security flaws in the

TOE. The combination of these components included in ALC_FLR.2 ensure that there is a contact mean by which discovered vulnerabilities can be reported to the manufacturer.

However, the ALC_FLR.2 requirement does not mandate that the way to report discovered vulnerabilities is through a contact address. Other reporting means could be valid (e.g. through a vendor's web portal, or through social media platforms), but these can be as effective as a contact address for the purpose of vulnerability reporting.

Proposal

In order to meet this ESR the Security Target of the TOE shall include the assurance component *ALC_FLR.2 Flaw reporting procedures* or a hierarchically higher component of its family.

Also, the ESR is implicitly cover in EUCC Article 33.2 *"2.The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.".*

Guidance

As part of ALC_FLR.2, manufacturers need to provide as evaluation evidence the flaw remediation guidance that includes the contact point by which TOE users can report suspected vulnerabilities to the TOE manufacturer.

ESR (7)

Requirement

Manufacturers of the products with digital elements shall: […]

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

Analysis

EUCC evaluations will be able to directly address this requirement by means of the requirements related to the (technical) patch mechanism involved in EUCC's patch management procedure, as well as with the adequate levelling of the assurance components in ALC_FLR family of [CC2022P3].

In this case, ALC_FLR.3 contemplates addressing security flaws in the TOE through automatic distribution of updates.

The analysis of Requirement 2 of Annex I.2 presented in earlier in this document can be reused for this requirement.

Proposal

In order to meet the Requirement 7 of Annex I.2 of [CRA], the same proposal as Requirement 2 of Annex I.2 presented in earlier sections can be reused.

Guidance

Same as in Requirement 2 of Annex I.2 presented in earlier in this document applies.

ESR (8)

Requirement

Manufacturers of the products with digital elements shall: […]

> *(8)* ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Analysis

As in other requirements of Annex I.2 of [CRA] analysed in previous sections, this requirement can be directly covered by including in the evaluation a combination of the SARs in the (technical) patch mechanism involved in EUCC's patch management procedure, and the requirement *ALC_FLR.1 Basic flaw remediation*, with the exception of the point related to providing the updates "free of charge". It must be highlighted that [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

Demonstrating that security updates are distributed free of charge is a condition which, by nature, it is not verifiable in the context of a security assessment. It would require vendors to provide evidence to ITSEFs that their update distribution system for the TOE does not force TOE users to pay for any of the updates. This can be problematic in cases where the distribution of updates has never been exercised before the evaluation of the TOE. Moreover, exercising the distribution of updates by evaluators might not be straightforward depending on the type of products and it also exists the risk that what was verified as free of charge for the sample of updates reviewed during the evaluation, may change to mandatory payment after the product has been certified.

Moreover, the exception given by this requirement in which a commercial agreement for tailor-made products would allow paid updates, isn't either an aspect verifiable by security evaluations.

As such, the conclusion is that there could not always be possible to find effective ways to assess the free-of-charge nature of security update distribution in an EUCC evaluation, considering the current version of the EUCC Implementing act.

The interpretation of this CRA essential requirement is that the manufacturer could sign a statement of the free of charge updates when applying to certification, whose presence should be controlled by the CAB, and further verified under the conditions of market surveillance.

The EUCC scheme could be supported by a template for application that provide the statement to be signed and define who should sign it.

Proposal

This ESR, can be met only in the functional part through technical elements in EUCC certifications; The assessment of free-of-charge nature of the updates or the agreement that exonerates to be that way is not part of a security evaluation.

However, including in the evaluation **either one of** the assurance requirements ALC_FLR.3, or the combination of ALC_FLR.1 and the (technical) patch mechanism involved in EUCC's patch management procedure (this study proposes to implement it through [ISO_TS_9569]), it would cover the functional and security parts of this requirements, except for the free-of-charge nature of the distributed security patches.

Regarding the free-of-cost updates part of the requirement, as a proposal for way forward, manufacturers could sign a statement of the free of charge updates, when applying to certification, whose presence should be controlled by the CAB, and further verified under the conditions of market surveillance. The EUCC scheme could be supported by a template for application that provide the statement to be signed and define who should sign it.

Guidance

No additional guidance is required.

1.3. CRA Annex II requirements

Requirement 1

Requirement

As a minimum, the product with digital elements shall be accompanied by:

1. *the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;*

Analysis

The current version of the EUCC does not include any requirement related to identification of the manufacturer or other information about them included in the requirement. No assurance requirements in [CC2022P3] exist with assurance activities relate to the aforementioned information.

This information, as per the context of requirements in Annex II that refer to that information provided to the user, should be included in one of the deliverable documents that EUCC mandate to be distributed to end-users. These are, as a minimum, the Security Target and the TOE guidance. The assurance activities in an EUCC evaluation that cover such requirements are those in the ASE and AGD classes, related respectively to the contents and evaluation of the Security Target and of the TOE guidance.

However, this document does not recommend adding any extended component to those classes in order to make mandatory the inclusion of the information required by requirement I of Annex II in the user deliverables. The reason is that such activities would be superfluous as they don't add any meaningful contribution to the assessment of the security of the TOE or its surrounding vendor processes.

The analysis presented here leans more towards the option of including this information in the Security Target introduction, but without defining any assessment activities that would require the

ITSEF to verify that the information listed in the requirement has been included in the ST contents. Instead, the related verification activity would fall under the responsibilities of the CAB/CRAs that are analysed in the section of the main part of the report named ***" EUCC CABs and conformity assessment"***.

Proposal

The manufacturer shall include in the Security Target (e.g., in an annex) the following contents mandated by the requirement I of Annex II of [CRA]:

- Registered trade name or registered trade mark of the manufacturer.
- Postal address and the email address at which the manufacturer can be contacted

However, no assessment activities for ITSEF are prescribed by this document, as they don't contribute in any meaningful way to the security of the product, hence they are not security-relevant. The verification of the presence of this information should be part of the CAB/CRA responsibilities defined in the section named ***"EUCC CABs and conformity assessment"***.

Guidance

Manufacturers shall include in the Security Target of the EUCC evaluation, e.g., under an annex, the vendor information listed in the above proposal.

Requirement 2

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

2. *the point of contact where information about cybersecurity vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;*

Analysis

This requirement is directly covered by the existing assurance component ALC_FLR.2 defined in [CC2022P3]. This component requires the manufacturers to elaborate and distribute to TOE users *flaw remediation guidance*. This guidance is addressed to the TOE user ensures, among other dispositions, that they are aware of how to communicate with the developer in order to report security flaws (vulnerabilities).

The following extracts from [CC2022P3] demonstrate the argument above:

- ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.
- ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

Regarding the part of the requirement mandating

Proposal

In order to meet this requirement, the EUCC evaluation and Security Target shall include the assurance component ALC_FLR.2 (or higher) defined in [CC2022P3].

Guidance

The manufacturer shall distribute to end-users the *flaw remediation guidance* in accordance with ALC_FLR.2 assurance requirement. Manufacturers shall ensure that such guidance is included as part of the evaluation deliverables describe the necessary means, including contact point, by which the TOE users can notify TOE the manufacturer suspected vulnerabilities or security flaws in the TOE.

Requirement 3

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

3. *name and type and any additional information enabling the unique identification of the product with digital elements;*

Analysis

A unique reference for univocal identification of the TOE is required in all EUCC evaluations by means of the assurance requirement ASE_INT.1. Below, the related subcomponents of ASE_INT.1 component can be found, extracted from [CC2022P3]:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

The above requirements guarantee that the identification of the TOE included in the Security Target is unique. The evaluation methodology allows for ways to uniquely identify the TOE such as version of the TOE, e.g. by including a version/release/build number, or a date of release.

Regarding corresponding and user information for end-users to identify the TOE and verify that they receive the correct TOE version, AGD_PRE.1 requirement

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

The evaluated methodology associated to AGD_PRE.1 require the ITSEF to verify that the user guidance contains all the necessary information to make sure the delivered TOE is the complete evaluated instance;

ASE_INT.1 and AGD_PRE.1 requirements are included by default in all the EUCC evaluations, so the coverage of this CRA requirement is immediate.

Proposal

No additional items need to be included in the EUCC evaluation in order to cover this requirement. ASE_INT.1 and AGD_PRE.1 requirements shall be included in the evaluation, which are required in all EUCC evaluations and STs.

Guidance

No additional guidance is required.

Requirement 4

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

4. *the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;*

Analysis

This requirement is directly covered by various of the Security Assurance Requirements of [CC2022P3] together as described below.

The intended use of the TOE shall be included in the Security Target as a requirement included in ASE_INT.1.4C assurance component ("*The TOE overview shall summarise the usage and major security features of the TOE.)*

The **security environment provided by the manufacturer** is required to be included in the Security Target as part of the ASE_INT.1.6C assurance component (The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.). This requirement makes necessary to describe in the "TOE Overview" of the ST the elements in the operational environment in which the TOE rely to correctly operate with its claimed security features and properties. Moreover, according to ASE_SPD.1, the Security Target shall include the assumptions about the operational environment, which shall be explained in sufficient detail to enable consumers to determine that their operational environment matches the assumption that are required for the TOE to run in its operational environment in a secure manner.

In addition, ASE_OBJ.1 requires the TOE to describe the security objectives for the operational environment that hold the assumptions about it, and they are expressed as objectives that shall be fulfilled by those elements in the environment that contribute the TOE to operate securely and adequately.

Lastly, the assurance components AGD_PRE.1 and AGD_OPE.1 requires the user guidance to contain instructions for users to making sure that the operational environment meets the security objectives associated to ASE_OBJ.1.

However, the above EUCC requirements don't require that this operational environment is provided by the manufacturer, although it is also not contradictory with it. The listed assurance requirements provide sufficient information about the operational environment that allow to identify whether the elements in it shall be provided by the TOE vendor or by other third-parties.

Finally, regarding **product's essential functionalities and information about the security properties,** it is mandatory to include this information in the EUCC Security Target as per the assurance requirements ASE_INT.1.8C ("ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE."), which requires the ST to describe those security functions in the logical scope that fall under the scope of the evaluation.

Moreover, ASE_REQ.1 assurance requirement requires the Security Target to describe the Security Functional Requirements of the TOE, which are SFRs that specify the security functions and features that a product shall implement to meet specific security objectives. They are used to define the security requirements for a product, and they provide a basis for evaluating the product's security capabilities during the evaluation and certification process.

Proposal

In order to meet this requirement, the EUCC evaluation and Security Target shall include the following assurance components: ASE_INT.1, ASE_SPD.1, ASE_OBJ.1, ASE_REQ.1 and AGD_PRE.1, AGD_OPE.1.

Guidance

When describing the operational environment of the TOE in the Security Target, manufacturers should clearly identify which elements of the environment are provided by the TOE vendor. The TOE user guidance under scope of the evaluation should also clearly describe which part of the secure preparation of the operational environment is done with support of elements provided by the TOE manufacturer and provide, if applicable, the associated instructions for their obtention, installation and configuration.

Requirement 5

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

5. *any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;*

Analysis

CC evaluations contemplate the elements included in this requirement by part of the assurance component AGD_OPE.1 defined in [CC2022P3]. This component describes the contents of the user guidance that TOE manufacturers need to provide to end-users in order to securely use the TOE in its operational environment after it has been adequately deployed and security configured.

The coverage of the requirement is also implicitly achieved, as the users in the operational environment are supposed to follow the user guidance and AGD_OPE.1 includes the instructions that ensure that the usage of the TOE is carried out by end-users in a secure way. In other words, users shall not deviate of the instructions provided in the user guidance for usage of the TOE and this ensures that no misuse of the TOE will be done.

Moreover, AGD_OPE.1 includes the content and requirement component AGD_OPE.1.1C that requires that the user guidance contains warnings regarding the use of the functions and privileges available to all TOE user roles. Warnings (according to [CEM2022]) should address expected effects, possible side effects, and possible interactions with other functions and privileges.

As such, AGD_OPE.1 requires the guidance to include instructions for adequate and secure use of the TOE, along with circumstances that could indicate a security-relevant event that the user needs to address in some manner.

Proposal

In order to meet this requirement, the EUCC evaluation and Security Target shall include the AGD_OPE.1 assurance component.

Guidance

No additional guidance is required.

Requirement 6

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

6. *where applicable, the internet address at which the EU declaration of conformity can be accessed;*

Analysis

This requirement is not directly or indirectly addressed by any requirements existing in the EUCC.

This document does not recommend defining any extended component to those classes in order to make mandatory the inclusion of the information required by requirement 7 of Annex II in the user deliverables. The reason is that such activities would be superfluous as they don't add any meaningful contribution to the assessment of the security of the TOE or its surrounding vendor processes.

The analysis presented here leans more towards the option of including this information in the Security Target introduction, but without defining any assessment activities that would require the ITSEF to verify that the information listed in the requirement has been included in the ST contents. Instead, the related verification activity would fall under the responsibilities of the CAB/CRAs that are analysed in the section named ***"CSA & CRA infrastructure synergies for routes to market involving a third-party evaluator"***.

Proposal

The manufacturer shall include in the Security Target introduction the following contents mandated by the requirement I of Annex II of [CRA]:

- the internet address at which the EU declaration of conformity can be accessed

However, no assessment activities for ITSEF are prescribed by this document, as they don't contribute in any meaningful way to the security of the product, hence this requirement is not security-relevant. The verification of the presence of this information should be part of the CAB/CRA responsibilities defined in in the section named ***"CSA & CRA infrastructure synergies for routes to market involving a third-party evaluator"***.

Guidance

Manufacturers shall include in the Security Target of the EUCC evaluation, under section "ST introduction" the vendor information listed in the above proposal.

Requirement 7

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

Analysis

The EUCC contemplates various aspects related to support to end-users for security updates, including end of support for distribution of patches. These requirements are intended to be addressed by the requirements in the (technical) patch mechanism involved in EUCC's patch management procedure. The coverage of this requirement shall be achieved by including in the EUCC evaluation the SARs related to the patch mechanism that are referenced in EUCC. As [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the corresponding SARs in the (technical) patch mechanism involved in EUCC's patch management procedure -this study proposes to use [ISO_TS_9569] as a reference for implementation of such mechanism those-.

Guidance

No additional guidance is required.

Requirement 8 (a)

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

8. detailed instructions or an internet address referring to such detailed instructions and information on:

   a. the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;

Analysis

CC directly addressed the contents of this requirement by means of two SARs defined in [CC2022P3]:

- AGD_PRE.1 requires the user guidance to include instructions on how to perform secure acceptance, installation and configuration of the TOE. It scopes the timeframe since reception of the product until it is installed in its operational environment and securely configured so that it is compliant with all the claims in the Security Target.
- AGD_OPE.1 requires the user guidance to include instructions for secure operational usage of the TOE, guiding the users on how to ensure security of the TOE during its operational usage.

All default assurance packages from EAL1 to EAL7 include these requirements. In evaluations where no default assurance packages from [CC2022P5] are used, the ST author shall ensure that AGD_PRE.1 and AGD_OPE.1 are included in the evaluation.

Proposal

In order to meet this requirement, the Security Target shall include the AGD_PRE.1 and AGD_OPE.1 assurance requirements.

Guidance

No additional guidance is needed.

Requirement 8 (b)

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

8. *detailed instructions or an internet address referring to such detailed instructions and information on: […]*
    b. *how changes to the product with digital elements can affect the security of data;*

Analysis

EUCC evaluations will include the assurance requirement AGD_OPE.1 defined in [CC2022P3]. This component describes the contents of the user guidance that TOE manufacturers need to provide to end-users in order to securely use the TOE in its operational environment after it has been adequately deployed and security configured.

By definition, end-users are expected to operate the TOE in accordance with the user guidance regulated by AGD_OPE.1, and this should ensure TOE security during its operational usage. If any circumstances or changes in the product configuration affect the security of data, this information shall be documented in the user guidance under EUCC evaluation scope.

As previously explained for other requirements in Annex II, the subcomponent AGD_OPE.1.1C that informs user about security-relevant events and how they should react upon those. If security of data is affected by any circumstance that can be derived from making configuration changes in the product, it shall be described in AGD_OPE.1

On the other hand, the nature of the EUCC evaluations assume that the TOE will be operated with a configuration that is in accordance with the evaluated configuration described in the Security Target. Any changes on this setup (described in AGD_PRE.1 user guidance), would set the TOE in a state that is not according to what was evaluated under the EUCC configuration. The user guidance under AGD scope describes the steps to prepare this configuration and advices against changes in it.

In products supporting updates, changes that could affect the security of data and that user need to be aware of fall under the scope of the (technical) patch mechanism involved in EUCC's patch management procedure. As [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include:

- AGD_OPE.1 assurance requirement defined in [CC2022P3].
- If the product supports security updates, the corresponding SARs in the (technical) patch mechanism involved in EUCC's patch management procedure (this study proposes to follows [ISO_TS_9569] as a way to instantiate that patch management mechanism).

Guidance

In products that support security updates, the manufacturer shall document in the user guidance the considerations for security of the data that can be triggered by applying security updates, as per the SARs related to the (technical) patch mechanism involved in EUCC's patch management procedure.

Requirement 8 (c)

Requirement

As a minimum, the product with digital elements shall be accompanied by: […]

8. *detailed instructions or an internet address referring to such detailed instructions and information on: […]*
    c. *how security-relevant updates can be installed;*

Analysis

Under the context of EUCC evaluations, the guidance for installation of security updates falls under the scope of the (technical) patch mechanism involved in EUCC's patch management procedure.

Proposal

In order to meet this requirement, the Security Target shall include the corresponding SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure. As [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

User guidance

The manufacturer shall document in the user guidance the instructions to install security updates, as per the SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure (with [ISO_TS_9569] as reference proposal).

Requirement 8 (d)

Requirement

8. *detailed instructions or an internet address referring to such detailed instructions and information on: […]*
    d. *the secure decommissioning of the product with digital elements, including information on how user data can be securely removed.*

Analysis

EUCC does not include any assurance requirements in [CC2022P3] that cover the security of the decommissioning of the TOE. It doesn´t include either any requirements related to providing end-users instructions on how to instruct users on performing these decommissioning tasks.

This document defines the security assurance requirements "Decommissioning procedures (AGD_DEC)", that establishes the requirements for manufacturers to provide to TOE end-users documentation describing how to securely perform decommission of the TOE.

The section named "***Decommissioning procedures (AGD_DEC) – Extended***" includes the definition of the necessary requirements to achieve the necessary coverage of the CRA requirement under analysis.

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the extended assurance component *"AGD_DEC.1: Decommissioning procedures"*.

Guidance

Refer to the section named "***Decommissioning procedures (AGD_DEC) - Extended***" for full guidance on how to include AGD_DEC.1 (Extended) in the evaluation.

Requirement 8 (e)

Requirement

> ***8.*** *detailed instructions or an internet address referring to such detailed instructions and information on: […]*
>
> *e. how the default setting enabling the automatic installation of security updates, as required by Annex I, Part I, point (c), can be turned off;*

Analysis

AGD_OPE.1 shall provide information on how to use the interface to the TOE Security Functionality, one of them being the enabling/disabling of automatic updates, according to the patch mechanism chosen to comply with ESR 2(c) in CRA Annex I, part 1.

Proposal

In order to meet this requirement, the EUCC evaluation shall include the assurance component AGD_OPE.1

Guidance

In the user guidance required by AGD_OPE.1, instructions for operating the update mechanism need to be provided, including how to enable and disable automatic updates.

Requirement 8 (f)

Requirement

> ***8.*** *detailed instructions or an internet address referring to such detailed instructions and information on: […]*
>
> ***f.*** where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential requirements set out in Annex I and the documentation requirements set out in Annex VII.

Analysis

The technical documentation required by Annex VII is largely addressed by the assurance families of the EUCC which required the issuance to the CAB of documentation describing the TOE design, TOE lifecycle and related manufacturer procedures, etc.

In general, there is a part of this documentation that can be publicly made available to users, such as the user guidance or the Security Target, and sometimes part of the functional specification. However, even in the scenario of distributing product for integration by 3rd parties, internal information such as design details of the product, or details about the lifecycle (which are required to comply with Annex VII according to this study) are not met. It's

However, this study proposes to comply with this requirement by setting out parts of the technical documentation associated to the SARs mapped to requirements in Annex VII that belong to the evaluation information that is public or that is part of the documentation delivered to the integrator.

The set of documentation of the EUCC evaluation that is delivered to integrators consists of:

- The Security Target (ASE).

- The user guidance (AGD).

As such, the documentation belonging to the scope of other assurance classes is not delivered to third parties (other than CABs).

To address this gap, the following solutions are proposed for the requirements of Annex VII that pose a conflict with the above diffusion policy:

- Requirement 1 (d): "*where the product with digital elements is a hardware product, **photographs or illustrations showing external features, marking and internal layout**; "* => **Way forward**: manufacturers shall include such illustrations and layout and interfaces of the products either in the Security Target or in the guidance for integrators (AGD). Internal design details (i.e., modular decomposition required by ADV_TDS.3 or higher) don't need to be distributed for integration. Documentation of TOE interfaces that is relevant for integration shall be included in AGD rather than in ADV_FSP documentation.
- Requirement 2 (a)**:** manufacturers shall include only high-level design details (i.e., commensurate with ADV_TDS.1) in the Security Target or in the user guidance for integrators (AGD). Internal design details (i.e., modular decomposition required by ADV_TDS.3 or higher) don't need to be distributed for integration.
- Requirement 2(b) Policy for vulnerability handling and disclosure, as well as SBOM shall be made public, at least to integrators. Internal details of vulnerability handling process related to ALC_FLR can be kept in the non-distributable documentation scope.
- Requirement 2(c): same as for requirement 2(b). Moreover, the high-level information about the TOE lifecycle related to production and monitoring processes shall be included in the Security Target.
- Requirement 6: The reports of tests and vulnerability handling aren't items that are necessary for the purpose of technical integration. The integrator can rely on the verification of these reports that is carried out during the CAB during the EUCC evaluation, as the EUCC certification will provide assurance for that.
- Requirement 8: The software bill of materials shall be made available to integrators. No hard gap.

Proposal

N/A

Guidance

N/A

Requirement (9)

Requirement

9. *where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential requirements set out in Annex I and the documentation requirements set out in Annex VII.*

Analysis

EUCC evaluations will not directly support this requirement. However, manufacturers can use the template in section **8 Template: CRA conformance claims for EUCC certified products** of the main part of the report, to provide the information about the location of the SBOM.

Proposal

As above.

Guidance

As above.

1.4. CRA Annex VII requirements

Requirement (1)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements:

1. *a general description of the product with digital elements, including*
    1. *its intended purpose.*
    2. *versions of software affecting compliance with essential requirements;*
    3. *where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;*
    4. *user information and instructions as set out in Annex II;*

Analysis

The coverage of this CRA requirement is achieved by various assurance requirements of a EUCC evaluation together, as described below.

Regarding **intended purpose**, ASE_INT.1 requirement in [CC2022P3] requires that the Security Target introduction, under the TOE Overview describes the usage of the TOE and its major security features, so the coverage is direct.

Regarding **(b)** subclause, the version of the TOE version needs to be univocally identified in the Security Target as per ASE_INT.1 requirement. Under any EUCC/CC evaluation, it is assumed that changing the version of the TOE will render the TOE out of the evaluated version, which is the one compliant with the essential requirements.

With respect to **(c)** subclause, the assurance families ADV_TDS and ADV_FSP defined in [CC2022P3] require to provide an architectonical description of the TOE in the design documentation, breaking down the TOE into design abstractions and specifying the interfaces at a level of detail commensurate with the assurance level. In hardware products it typically means providing illustrations, schematics or drawings of the physical layout of the TOE and its interfaces. Depending on the assurance level, the different hierarchically components in ADV_TDS will provide more detail at fine-grain, but the subclause (c) doesn't specify the level of detail for the illustrations, so in principle ADV_TDS.1 and ADV_FSP.1 assurance components should be sufficient to cover this part of the requirement. However, the contents of ADV_TDS.1 and ADV_FSP.1 are typically trade secrets that are disclosed only to the evaluation facility after a non-disclosure agreement is signed. Therefore, including them in the technical documentation that the manufacturer must put at the disposal of the market surveillance authorities (according to CRA article 19.6) might not appropriate, except in cases the product qualifies as free and open-source software and then the technical documentation will be made publicly available (see CRA Article 32.5). Again, due to the fact that subclause (c) of the ESR doesn't specify the level of detail in the illustrations, such clause can be addressed by information that is available in the Security Target, through ASE_INT.1 requirement, and that is sufficient to understand the adequacy of the Security Problem Definition and Security Requirements included in the evaluation:

- *ASE_INT.1.8C: The TOE description shall describe the physical scope of the TOE.*
- *ASE_INT.1.9C: The TOE description shall describe the logical scope of the TOE.*

As part of those physical and logical scopes, it is possible to include the information required to fulfil what is specified in subclause (c). Further details can be provided as part of the TOE Summary Specification section of the ST, as required by ASE_TSS.1.

Regarding **(d)** subclause, in the section named "***CRA Annex II Requirements***" it has been analysed how the different assurance components of EUCC cover each requirement for user information and instructions included in Annex II of [CRA].

Proposal

In order to meet Requirement I of Annex VII of [CRA], the EUCC evaluation and the Security Target shall include the following assurance components from [CC2022P3]:

- ASE_INT.1
- ASE_TSS.1

Moreover, the assurance components proposed in the section named "***CRA Annex II Requirements***" shall be included as well.

Guidance

Regarding compliance with subclause (c), manufacturers of hardware products should ensure that the TOE physical scope described in the ST or the TOE Summary Specification provide photographs, schematics or diagrams depicting the TOE hardware layout and interfaces.

Requirement (2)(a)

Requirement

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:
    a. necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

Analysis

EUCC evaluations including various assurance components of ADV class will be able to directly meet this requirement.

ADV_TDS assurance family requires the design documentation to describe the design breakdown into design abstractions (subsystems or modules). The design abstractions, depending on the assurance level, match with the different software components in the architecture and, at a minimum, the relationship between them. Moreover, the design information normally includes drawings or schemes of the TOE layout or architecture.

Therefore, compliance with this requirement in a future EUCC evaluation can be achieved by including ADV_TDS.1 or higher in the evaluation.

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the ADV_TDS.1 or hierarchically higher assurance component from [CC2022P3].

Guidance

Developers should ensure that the design documentation associated to ADV_TDS assurance family includes drawings and schemes of the product architecture.

Requirement (2)(b)

Requirement

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including: […]
    - b. necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;

Analysis

The coverage of this requirement, regarding contents of the technical documentation, can be achieved by the joint effort of various assurance components of the EUCC evaluation together, meeting the different parts of the requirement as described below.

The assurance component ALC_FLR.2 (defined in [CC2022P3]) models the requirements for the procedures of security flaw (vulnerability) handling, including the details on how users can report suspected or found vulnerabilities to the manufacturer (e.g. a contact address or other reporting mean).

The remaining parts of the requirement in relation with vulnerability handling process (e.g. vulnerability disclosure policy and technical solution chosen for the distribution of updates) are covered by the SARs implementing the *patch management* that are defined in [EUCC]. It must be highlighted that [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

Moreover, the inclusion of the software bill of materials in the technical documentation, as explained in previous sections, is not covered by any SAR or SFR in CC, but the definition of the extended component ALC_SBM.1 is sufficient to address this requirement, as it mandates the inclusion of the software bill of materials in the technical documentation of the evaluation, and its delivery to final users (see its definition in the section named "***Software bill of materials (ALC_SBM) - Extended***").

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the following assurance components:

- ALC_FLR.2 from [CC2022P3].
- SARs implementing the (technical) patch mechanism involved in EUCC's patch management procedure -this study proposes to use those in [IS_TS_9569].
- Extended assurance component ALC_SBM.1 (Extended), as defined in the section named "***Software bill of materials (ALC_SBM) - Extended***".

Guidance

No additional guidance is required.

Requirement (2)(c)

Requirement

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including: […]
    c. complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.

Analysis

It will be possible for EUCC evaluations to include assurance components of class ALC to assess the security of the development and production processes of the TOE. For the specific mention in this requirement to production processes of the product with digital elements, the assurance class ALC_LCD.1 from [CC2022P3] ensures the assessment of production processes by emphasising the critical importance of well-defined and controlled processes throughout the TOE's lifecycle. It acknowledges that poorly defined or uncontrolled processes can lead to a TOE that fails to meet security objectives. This assurance activity requires the technical documentation to describe the life-cycle models adopted by the manufacturer for development, production, and maintenance processes with the ultimate goal of supporting process improvement and best practices.

For the monitoring processes, as mentioned in Requirement 2.c of Annex VII, this analysis interprets them as monitoring of the product security after it is placed in the market. This procedure, as in other requirements, is directly addressed by both the ALC_FLR assurance family in [CC2022P3] along with the SARs implementing the [EUCC] parts related to patch management processes. Together, they ensure that the technical documentation contains the necessary information about monitoring of product security during its whole lifecycle.

It must be highlighted that [EUCC] doesn't mandate any particular SFRs for the implementation of such mechanism, or SARs for the definition of its evaluation methodology, this study proposes the usage of the SFRs and SARs in the [ISO_TS_9569] as reference implementation of that mechanism.

Lastly, the requirement also mentions validation of those processes. The validation can be implicitly covered by the assessment of both the ALC_LCD.1, ALC_FLR.2 and SARs in the (technical) patch mechanism involved in EUCC's patch management procedure, that is carried out by the ITSEF as part of the assurance activities associated to those requirements. While it is true that the developer doesn’t perform such validation and it is done by the evaluators during the EUCC evaluation, it demonstrates that the vendor procedures comply with the mentioned assurance requirements, and the Evaluation Technical Report elaborated by the ITSEF can be used as evidence for the entities in charge of validation of the compliance of this requirement.

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the following assurance components:

- ALC_LCD.1 of [CC2022P3].
- ALC_FLR.2 from [CC2022P3].
- SARs implementing the (technical) patch mechanism involved in EUCC’s patch management procedure -this study proposes to use those in [IS_TS_9569].

Guidance

Regarding validation of the production and monitoring processes, these activities shall be part of the certification report stated by a Certification Body.

Therefore, the monitoring part of the requirement does not require any action on the side of the manufacturer.

Requirement (3)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

3. *an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 13 of this Regulation, including how the essential requirements set out in Annex I, Part I, are applicable;*

Analysis

EUCC evaluations will include, in the contents of the security target, the definition of a security problem in which the threats to the assets that the TOE shall protect are analysed and they lead to security objectives for the TOE and for the operational environment that are meant to counter those threats. This can be seen as a form of risk analysis that scopes the decisions on which security functionality needs to be planned, designed and developed for the product. As in the analysis of the Requirement 1 of Annex I of [CRA], this would mean including in the evaluation the assurance requirements ASE_SPD.1, ASE_OBJ.1 and ASE_REQ.1 of [CC2022P3].

However, this risk assessment conducted as part of the security problem definition in the Security target does not address aspects that aren’t part of the product security functionality but are related to its production, delivery and maintenance processes. In CC, the assurance requirement ASE_REQ.1 (or ASE_REQ.2) can be included in the evaluation, as it requires the developer to provide a rationale on why the set of SARs included in the evaluation were chosen. These SARs directly relate to the content requirements and evaluation activities that ensure security during the product lifecycle.

This analysis is completed with the rationale included in section ***"Manufacturer risk assessment*** in the main report, especially regarding the justification of the selection of the SARs in the evaluation through ASE_REQ.2, and concluding that coverage of this CRA requirement is possible.

In order to make the coverage sounder and more explicit, this document prescribes manufacturers to carry out a risk analysis whose outcome is the selection of the Security Assurance Requirements to be included in the EUCC evaluation.

However, the list of ESRs which are applicable according to the cybersecurity risk assessment, as required by this requirement, is not explicitly provided by the CC assurance requirements here proposed. This should be addressed by adding specific mappings from the chosen SFRs, as result of the SPD in the EUCC evaluation, and the related ESRs. This information is to be provided separately, e.g., in an annex to the Security Target or Protection Profile, i.e. in the template proposed in the main section of the report named "**Template: CRA conformance claims for EUCC certified products**"

Proposal

In order to meet this requirement, the EUCC evaluation and the Security Target shall include the following assurance components:

- ASE_SPD.1, ASE_OBJ.2, ASE_REQ.1 (or hierarchically higher component) from [CC2022P3].

Guidance

The author of the ST/PP shall also provide an explicit mapping between the SFRs/SARs resulting from the SPD in the EUCC Security Target, and the ESRs of Annex I Part I that describe equivalent functionality.

Requirement (4)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

4. relevant information that was taken into account to determine the support period as referred to in Article 13(8) of the product with digital elements;

Analysis

Although the duration of the lifecycle is usually implicitly considered in the cybersecurity risk assessment linked to the SPD in the ST, EUCC doesn't directly require this information to be provided.

Proposal

This study proposes the usage of the template in the main part of the report, section "**Template: CRA conformance claims for EUCC certified products**" to indicate the factors of the SPD in the ST that were taken into account in relationship with the duration of the support period. Also, ASE_SPD.1 must be included in the Security Target.

Guidance

Manufacturers should indicate in the template in the main part of the report, section "**Template: CRA conformance claims for EUCC certified products**" which elements of the SPD in the ST were taken into account in relationship with the duration of the support period.

Requirement (5)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

5. *a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in of Annex I, Parts I and II, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;*

Analysis

Since the purpose of this document is to provide the guidelines to achieve CRA conformity through EUCC certification, the requirement can be met by simply declaring the EUCC as solution adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I of CRA applied.

Other harmonised standard applied can be declared in the introduction of the EUCC Security Target, or in an annex.

Proposal

The harmonised standard applied, as well as the EUCC itself as solution to meet the essential requirements of [CRA] Annex I shall be declared in the EUCC Security Target introduction or in a ST annex.

Guidance

Manufacturers can use the ST template included in the section named "***Template: CRA conformance claims for EUCC certified products***" and include in it, e.g. under the ST introduction, or a separate annex, the list of harmonised standards used, along with the EUCC claim as strategy to meet the essential requirements in Annex I of CRA.

Requirement (6)

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

6. *reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;*

Analysis

In order to verify the compliance with the applicable essential requirements defined in parts 1 and 2 of Annex I in the context of an EUCC evaluation, it would necessary to demonstrate the compliance with the SFRs and SARs of CC, and other extended requirement, that map to the associated CRA essential requirements. Those mapping SFRs and SARs, are listed throughout the section named "***Annex I requirements***" of this document.

Part of the verification of conformity of those requirement can be done by the manufacturer by including in the evaluation the assurance components *ATE_FUN.1 Functional testing,* that requires the manufacturer to elaborate and execute a test plan that covers the TOE evaluated security functionality. However, this only provides a limited coverage of the CRA requirement 5 of Annex VII, as this vendor testing would verify only compliance with the Security Functional Requirements, but not with the vendor process requirement described by the SARs mapped to essential cybersecurity requirements in Annex I of [CRA].

However, ATE_FUN.1 does not require the manufacturers to test all the security functionality of the TOE, which means that not all the SFRs need to be tested and, accordingly, the testing of some functionality linked to CRA Annex I essential cybersecurity requirements would be missing. This can be solved by adding to the evaluation ATE_DPT.1 assurance component, which requires testing of all the TSF subsystems (design abstractions that implement TOE security functionality), and it would ensure that all the subsystems implementing the SFRs associated to the CRA Annex I SFRs are tested. ATE_IND.1 introduces dependencies with ATE_FUN.1, ADV_ARC.1 and ADV_TDS.2 assurance components.

Therefore, in order to fully comply with this requirement, the Certification Report issued by a Certification Body, where the evaluation activities determined by the SARs and conducted by the evaluators are reported, shall be used as evidence by entities in charge of the validation of this requirement.

On the other hand, with the purpose of compliance with the extended SAR "Periodic Security Review and Testing of the TOE (ALC_PSR.1) - Extended", where possible records of exercising the review and testing activities associated to these processes shall be provided to the CAB.

Proposal

In order to meet the Requirement 5 of Annex VII of [CRA], the EUCC evaluation and the Security Target shall include the following assurance components:

- ATE_FUN.1 and ATE_DPT.1 of [CC2022P3].
- Periodic Security Review and Testing of the TOE (ALC_PSR.1) - Extended.

In addition, the Certification Report issued by a Certification Body shall be provided to the entity in charge of verification of this requirement as evidence.

Guidance

Regarding validation of the SARs linking to CRA Annex I requirements, these activities will be carried out by the ITSEF as part of the EUCC evaluation tasks. The related evidence will be provided in the Certification Report issued by a Certification Body.

Therefore, the monitoring part of the requirement does not require any action on the side of the manufacturer.

Requirement (7)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

7. a copy of the EU declaration of conformity;

Analysis

EUCC or CC standard don't include any requirement related to the EU declaration of conformity, which is a formal CRA-related requirement. Creating extended components under EUCC that would cover this requirement would not contribute in any way to the product security and would be out of the intended scope of the EUCC.

Manufactures should, instead, include this declaration of conformity as supplementary evidence to be examined by the CABs/CRAs.

Proposal

Manufacturers should include the EU declaration of conformity as an annex to the Security Target or within the introduction section of the ST.

Guidance

Manufacturers can follow the ST template included in the section named "***ST for CRA conformance claim – template***" and include in it, e.g., under the ST introduction, or a separate annex, the EU declaration of conformity.

Requirement (8)

Requirement

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements […]:

8. where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.

Analysis

The software bill of materials, while not covered by EUCC or CC standard requirements, becomes a required part of the technical documentation when the extended assurance component *ALC_SBM.1: Software bill of materials* is included in the evaluation and in the security target.

The rest of evidence required to demonstrate compliance with Annex I requirements of CRA is analysed and listed throughout the section named "***Annex I requirements***" of this Annex.

The part of the requirement mandating manufacturers to provide the SBOM and other technical documentation to market surveillance authorities requesting it, falls out of the scope of the cybersecurity-related analysis done in this document, but it can be added as guidance for manufacturers.

Proposal

In order to meet the Requirement 7 of Annex VII of [CRA], the EUCC evaluation and the Security Target shall include the following assurance components:

- Extended assurance component ALC_SBM.1 (Extended), as defined in the section named "***Software bill of materials (ALC_SBM) - Extended***".
- SFRs and SARs listed in the section named throughout the section named "***Annex I requirements***" of this Annex (for compliance with Annex I requirements of CRA).

Guidance

Manufacturers shall provide, upon a request of a market surveillance authority, the SBOM along with other evaluation evidence (technical documentation) among that listed in "***Annex I requirements***".

Requirement 9

1.5. Definition of extended CC SARs for CRA coverage

This section contains the definition of extended SARs that, according to the analysis presented in the ***Annex I*** of this document, are required to obtain coverage of CRA essential requirements in EUCC evaluations.

Security Architecture with default secure configuration (ADV_ARC.2) – Extended

Objectives

The objective of this family is for the developer to provide a description of the security architecture of the TSF. This will allow analysis of the information that, when coupled with the other evidence presented for the TSF, will confirm the TSF achieves the desired properties. The security architecture descriptions support the implicit claim that security analysis of the TOE can be achieved by examining the TSF; without a sound architecture, the entire TOE functionality would have to be examined.

The properties of the security architecture include also the secure default configuration, which means the state or configuration in which the TOE is delivered to the customer, prior to the execution of the preparative steps included as part of AGD_PRE guidance. This property ensures that the TOE is in a secure state, which can be a state in which available functionality and interfaces are limited, and should ensure that, if the TOE is booted up in the state in which it is received by the user, it does not risk the security the TOE itself, of its protected assets, or of any other entity in its environment (e.g., other devices in the network where the TOE is deployed).

Component levelling

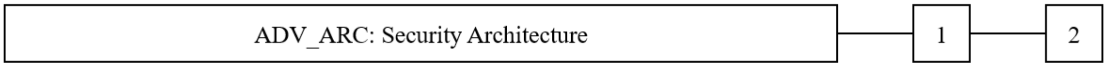

Figure 1: component levelling of ADV_ARC family

The components in this family are levelled based according to the property of secure default configuration. In evaluations of TOEs that require this property, ADV_ARC.2 should be claimed; otherwise, ADV_ARC.1 should be used. ADV_ARC.2 is hierarchically above to ADV_ARC.1 and includes all its assurance components.

At the second level, the requirements also include developer's requirements to provide a rationale for secure default configuration in the security architecture, plus evaluator activities to assess such property.

Application notes

The notions of self-protection, domain separation, and non-bypassability are distinct from security functionality expressed in CC Part 2 SFRs because self-protection and non-bypassability largely have no directly observable interface at the TSF. Rather, they are properties of the TSF that are achieved through the design of the TOE, and enforced by the correct implementation of that design. Also, the evaluation of these properties is less straight-forward than the evaluation of mechanisms; it is more difficult to check for the absence of functionality than for its presence. However, the determination that these properties are being satisfied is just as critical as the determination that the mechanisms are properly implemented.

The approach used is that the developer provides a TSF that meets the above-mentioned properties, and provides evidence (in the form of documentation) that can be analysed to show that the properties are indeed met. The evaluator has the responsibility for looking at the evidence and, coupled with other evidence delivered for the TOE, determining that the properties are achieved. The work units can be characterised as those detailing with what information shall be be provided, and those dealing with the actual analysis the evaluator performs.

The security architecture description describes how domains are defined and how the TSF keeps them separate. It describes what prevents untrusted processes from getting to the TSF and modifying it. It describes what ensures that all resources under the TSF's control are adequately protected and that all actions related to the SFRs are mediated by the TSF. It explains any role the environment plays in any of these (e.g. presuming it gets correctly invoked by its underlying environment, how is its security functionality invoked?). In short, it explains how the TOE is considered to be providing any kind of security service.

The analyses the evaluator performs shall be done in the context of all of the development evidence provided for the TOE, at the level of detail the evidence is provided. At lower assurance levels, there should not be the expectation that, for example, TSF self-protection is completely analysed, because only high-level design representations will be available. The evaluator also needs to be sure to use information gleaned from other portions of their analysis (e.g., analysis of the TOE design) in making their assessments for the properties being examined in the following work units.

The secure by default configuration property shall describe how the TOE security is ensured in the state that the TOE is delivered by the manufacturer. Security of the TOE and its assets shall be ensured by means of this property at the time prior to execution of AGD_PRE guidance instructions.

As an example, some TOEs require users to use an administrative interface in order to close ports exposing insecure protocols, or restricting insecure mechanisms such as weak cryptographic algorithms. In a secure-by-default configuration, it is expected that the TOE does not rely on such configuration steps to ensure security; following the previous example, the TOE would be delivered with the insecure interfaces already closed or restricted without a required action by the administrator.

The way in which the security of the TOE is ensured by a default secure configuration largely depends on the TOE design and interfaces. Therefore, the developer is expected to provide a rationale that is supported in the TOE design and TOE functional specification, at the level of detail

ADV_ARC.1: Security Architecture

Note: *the same definition given in section 10.2 of [CC2022P3] would be inserted here.*

ADV_ARC.2: Security Architecture with default security configuration (Extended)

Hierarchical to: ADV_ARC.1.

Dependencies: ADV_FSP.1 Basic functional specification, ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.2.1D **The developer shall design and implement the TSF so that the security features of the TSF cannot be bypassed.**

ADV_ARC.2.2D **The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.**

ADV_ARC.2.3D **The developer shall provide a security architecture description of the TSF**.

ADV_ARC.2.4D **The developer shall design and implement the TOE so that a secure configuration is enforced in the state in which the TOE is delivered.**

Content and presentation elements:

ADV_ARC.2.1C **The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.**

ADV_ARC.2.2C **The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.**

ADV_ARC.2.3C **The security architecture description shall describe how the TSF initialisation process is secure.**

ADV_ARC.2.4C **The security architecture description shall demonstrate that the TSF protects itself from tampering.**

ADV_ARC.2.5C **The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.**

ADV_ARC.2.6C **The security architecture description shall demonstrate that the TSF enforces a secure default configuration at the state in which it is delivered.**

Evaluator action elements:

ADV_ARC.2.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Evaluation work units for ADV_ARC.1

Note: the work units for ADV_ARC.1 would be inserted here as they are in [CEM2022].

Evaluation work units for ADV_ARC.2 (Extended)

Action ADV_ARC.2.1E

ADV_ARC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

ADV_ARC.2.1C: The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

Work unit ADV_ARC.2-1

Note: same definition as for ADV_ARC.1-1 in [CEM2022] should be inserted here.

Work unit ADV_ARC.2-2

Note: same definition as for ADV_ARC.1-2 in [CEM2022] should be inserted here.

Work unit ADV_ARC.2-3

Note: same definition as for ADV_ARC.1-3 in [CEM2022] should be inserted here.

Work unit ADV_ARC.2-4

Note: same definition as for ADV_ARC.1-4 in [CEM2022] should be inserted here.

Work unit ADV_ARC.2-5

Note: same definition as for ADV_ARC.1-5 in [CEM2022] should be inserted here.

ADV_ARC.2.6C The security architecture description shall demonstrate that the TSF enforces a secure default configuration at the state in which it is delivered.

Work unit ADV_ARC.2-6

The evaluator ***shall examine*** *t*he security architecture description to determine that it presents an analysis that adequately describes how the TSF enforces a secure default configuration at the state in which it is delivered.

A default configuration is that in which the TOE is delivered to the user, prior to execution of the instructions in AGD_PRE guidance. A secure default configuration is that in which it is guaranteed that the security of the TOE or its assets is guaranteed.

The secure default configuration could be based if a number of factors that largely depend on the TOE design and architecture, such as:

- Insecure interfaces or exposed weak algorithms being closed or restricted by default.
- Limited TOE functionality by default, until securely enabled by the administrator.
- The TOE doesn’t allow a full boot-up, and services or connectivity are disabled until all the security configurations have been established by the administrator.
- No data can be accessed, fed to the TOE, generated or outputted by the TOE until the administrator has configured the TOE.
- Etc.

The evaluator assesses the description provided (and other information provided by the developer, such as the functional specification, the design or the security target) to ensure that the state in which the TOE is delivered doesn’t provide any mean or interface to negatively affect the security of the TOE.

The developer’s rationale is expected to describe in the evidence an argumentation on how the default configuration prevents undermining the TOE security, and should be described in terms of protected assets, mechanism for their protection and the state of those mechanisms in the default configuration, interfaces to access the asset and their state in the default configuration, TSF functions or services and their state in the default configuration, etc. For each of these items, the security architecture should describe how their state at default configuration prevents TOE security to be vulnerated.

Software Bill of Materials (ALC_SBM) – Extended

Objectives

This family includes a component that requires the developer to provide a Software Bill Of Materials (SBOM), which is a formal record containing details and supply chain relationships of components included in the software/firmware elements of a product with digital elements. This list usually translates into a list of third-party components (e.g. libraries) used by the TOE, identifying their version and their origin (e.g. developer, or if it's open source code). By providing this evidence, it is possible to maintain a record of third-party components that can be examined at any point in time to determine whether vulnerabilities have been found in any of them.

Moreover, this family requires that the SBOM is provided in a machine-readable format that supports automation when searching for vulnerabilities in the used third-party components.

Component levelling

This assurance family contains only one component.

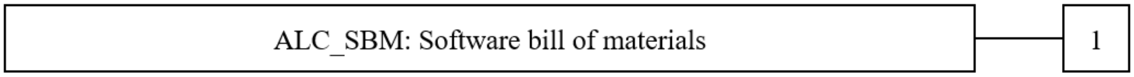

Figure 2: component levelling for ALC_SBM family

Application notes

The software bill of materials does not necessarily need to match with the parts of the TOE contemplated in ALC_CMS.2 or higher. The fact that the third-party software elements are not consistently listed as parts that compose the TOE (especially those that are linked statically and do not result in a separate binary upon TOE generation), in addition to the fact that the format in which the bill of materials provided needs to be machine readable, make ALC_CMS components not suitable to cover the objectives of ALC_SBM in all situations.

ALC_SBM.1: Software bill of materials (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies

Developer action elements:

ALC_SBM.1.1D **The developer shall elaborate the SBOM including the developer and SBOM Uniform Resource Identifier, containing its email address, and the SBOM compilation timestamp in an ISO 8601 format.**

ALC_SBM.1.2D **The developer shall provide the SBOM to TOE users.**

Content and presentation elements:

ALC_SBM.1.1C **The SBOM shall contain at least the top-level third-party software components used by the TOE including, for each, at least its name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.**

ALC_SBM.1.2C **The SBOM shall be provided in machine readable format, using CycloneDX6 in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.**

Evaluator action elements:

ALC_SBM.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Evaluation work units for ALC_SBM.1 (Extended)

Action ALC_SBM.1.1E

ALC_SBM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

ALC_SBM.1.1C The SBOM shall contain at least the top-level third-party software components used by the TOE including, for each, at least its name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.

Work unit ALC_SBM.1-1

The evaluator ***shall examine*** the SBOM to determine that it contains at least the top-level third-party component used by the TOE and that, for each, it includes at least name, version, developer's URI, SPDX-ID structure licence and hash value of the executable component.

For TOEs comprised purely by hardware, without any software or firmware in them, this work unit is not applicable.

For more detail regarding the expected parameters to be included for each third-party component, refer to section 5 in [TR-03183].

ALC_SBM.1.2C The SBOM shall be provided in machine readable format, using CycloneDX6 in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.

Work unit ALC_SBM.1-2

The evaluator ***shall examine*** the SBOM to determine that it is provided in machine readable format using CycloneDX6 in version 1.4 or higher or Software Package Data eXchange (SPDX) in version 2.3 or higher.

The format is defined in the specifications below:

- CycloneDX6 – https://cyclonedx.org/specification/overview/
- Software Package Data eXchange (SPDX)- https://spdx.dev/specifications/

For TOEs comprised purely by hardware, without any software or firmware in them, this work unit is not applicable.

Periodic Security Review and Testing (ALC_PSR) – Extended

Objectives

This family defines a component that requires the developer to perform periodic security review and testing of the TOE. This review and testing are different from that performed during the evaluation during AVA_VAN assessment and it doesn't necessarily overlap either with the testing performed as part of ATE assurance class, which is oriented to functional verification of the TOE behaviour rather than security-oriented.

The security review and testing required by this family shall be carried out periodically, and not only when changes are introduced in the TOE (e.g. when releasing new functionality or modifying existing one). The intention of the periodical review and testing is twofold:

- To regularly verify that no new vulnerabilities have been found for the TOE or its parts.

- To ensure no new attack techniques have appeared, that make the TOE vulnerable, since the previous TOE testing which did not reveal any exploitable vulnerabilities.

Component Levelling

This assurance family contains only one component.

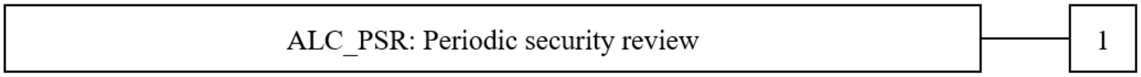

Figure 3: component levelling of ALC_PSR assurance family

Application notes

The evaluation activities linked to this family require the evaluator to examine the security review and testing procedures in order to verify that they require the developer to perform regular security review and testing, and also include review of the developer's records demonstrating that the procedure has been exercised at some moment in the past prior or during the evaluation.

Periodic Security Review and Testing of the TOE (ALC_PSR.1) - Extended

Hierarchical to: No other components.

Dependencies: No dependencies

Developer action elements:

ALC_PSR.1.1D **The developer shall provide the procedures for periodic security review and testing of the TOE.**

ALC_ PSR.1.2D **The developer shall provide evidence of exercising the procedures for periodic security review and testing of the TOE.**

Content and presentation elements:

ALC_ PSR.1.1C **The procedures for periodic security review and testing of the TOE shall require the developer to perform security review and security testing of the TOE with a periodicity of at most once a year and for a period of time covering, at least, five years from the end of the evaluation**

ALC_ PSR.1.2C **The evidence provided by the developer shall demonstrate that the TOE undergoes security review and testing with the periodicity specified in the procedures.**

Evaluator action elements:

ALC_PSR.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Evaluation work units for ALC_PSR.1 (Extended)

Action ALC_PSR.1.1E

ALC_PSR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

ALC_ PSR.1.1C The procedures for periodic security review and testing of the TOE shall require the developer to perform security review and security testing of the TOE at regular intervals, with a periodicity of at most once a year.

Work unit ALC_PSR.1-1

The evaluator ***shall examine*** the procedures for periodic security review and testing of the TOE to determine that they require the developer to perform security review and security testing of the TOE at regular intervals, with a periodicity of at most once a year and for a period of time covering, at least, five years from the end of the evaluation.

These periodical tests most commonly include vulnerability assessments. They play a crucial role in periodically reviewing and testing the security of a TOE to verify the absence of new vulnerabilities. This may involve using automated vulnerability scanning tools to scan the TOE and its components for known vulnerabilities. These scans should encompass the entire technology stack, including third-party components and dependencies. Special attention should be paid to third-party components by cross-referencing them with CVE databases to check for any known vulnerabilities associated with these components.

Other periodical and more in-dept technics may include: Assessing the settings, options, and parameters within the TOE to ensure that they align with established security best practices and organizational policies. Executing red-team exercises, which operates with the goal of finding and exploiting vulnerabilities, providing valuable insights into the TOE's security resilience. Making code reviews, where cybersecurity experts examine the product's source code, searching for coding errors, vulnerabilities, and potential security issues.

The developer's procedures for periodic security review and testing should outline how the manufacturer would react upon the finding of a vulnerability during the review, or point to the applicable ALC_FLR flaw remediation procedures.

Regarding the period of time during which the periodical security review and testing is performed, evaluators shall review the developer's evidence and use as a reference date, that in which it is expected to conclude the evaluation. Evaluators shall review the verdict assigned to this work unit before issuing the final verdict of the evaluation to ensure that the five-year period is still covered at the conclusion of the evaluation.

ALC_PSR.1.2C The evidence provided by the developer shall demonstrate that the TOE undergoes security review and testing with the periodicity specified in the procedures.

Work unit ALC_PSR.1-2

The evaluator ***shall examine*** the evidence provided by the developer to determine that the TOE undergoes security review and testing with the periodicity specified in the procedures.

When possible, the vendor evidence should be provided in the form of records of exercising the procedures in the past. It may be the case of a newly developed TOE that the security review and testing procedures have yet to be exercised. If the developer has produced other similar products, then an examination of records for these procedures in their use may be useful in providing assurance.

Processed Data Minimisation (ADV_PDM) – Extended

Objectives

This family addresses the assessment of the principle of data minimisation in the design of the TOE. This principle requires that the TOE processes (by storing, deriving, transforming, manipulating, importing or transmitting to out-of-TOE entities) only data that is necessary, adequate, relevant and limited to what is necessary in relation to the intended use of the TOE. The assessment of this principle in the TOE allows to ensure that the TOE does not perform processing of data that is not relevant to the intended purpose of the TOE.

Component levelling

This assurance family has only one component.

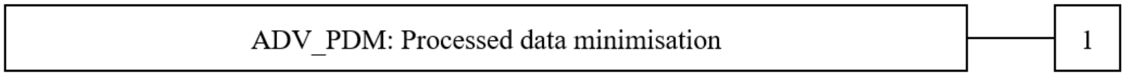

Figure 4: Component levelling of ADV_PDM family

Application notes

The property of data minimisation is not related with the security functionality expressed by CC Part 2 SFRs, as it is not oriented to protection of any of the security dimensions of data being processed by the TOE. Instead, it aims to demonstrate that all the data processed by the TOE is justifiably necessary for the purpose of the TOE.

In the context of this assurance family, data processing comprises that user data that is provided as input to the TOE through any of its input interfaces.

The justification that the TOE meets the data minimisation principle shall be supported in evidence provided by developers in which they shall declare which user data is processed by the TOE. The AGD_OPE is used as supporting evidence, as it is meant describe all the interfaces to the TOE that could be subject of data ingestion to the TOE.

This family does not have any concern on data that is generated inside the TOE.

The developer evidence shall also demonstrate that all the data processed by the TOE is justifiably necessary and adequate in relation with the intended purpose of the TOE. The assessment of this characteristic of necessity and adequateness will require the evaluator to examine the intended use of the TOE in accordance with the TOE overview and TOE description described in the Security Target.

ADV_PDM.1: Processed Data Minimisation (Extended)

Hierarchical to: no other components.

Dependencies: AGD_OPE.1 Operational user guidance

Developer action elements:

ADV_PDM.1.1D **The developer shall design and implement the TOE so that it only processes user data that is necessary and adequate in relation with the intended use of the TOE.**

ADV_PDM.1.2D **The developer shall provide a rationale for data minimisation of the TOE.**Content and presentation elements:

ADV_PDM.1.1C **The rationale for data minimisation shall identify all user data that is processed by the TOE.**

ADV_PDM.1.2C **The rationale for data minimisation shall relate each user data processed by the TOE with the input interfaces from which it is received and with the outbound interfaces where it is outputted to non-TOE entities.**

ADV_PDM.1.C **The rationale for data minimisation shall demonstrate that all user data processed by the TOE is necessary and adequate in relation with the intended purpose of the TOE.**

Evaluator action elements:

ADV_PDM.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Evaluation work units for ADV_PDM.1 (Extended)

Action ADV_PDM.1.1E

ADV_PDM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

ADV_PDM.1.1C The rationale for data minimisation shall identify all user data that is processed by the TOE.

Work Unit ADV_PDM.1-1

ADV_PDM.1-1 The evaluator ***shall check*** that the rationale for data minimisation identifies all user data that is processed by the TOE.

ADV_PDM.1.2C The rationale for data minimisation shall relate each user data processed by the TOE with the input interfaces from which it is received and with the outbound interfaces through which it is outputted to non-TOE entities.

Work Unit ADV_PDM.1-2

The evaluator ***shall examine*** the rationale for data minimisation and the operational user guidance, in order to determine that it provides relationships between all the user data processed by the TOE and the input interfaces from which the data is received and with the outbound interfaces through which it is outputted to non-TOE entities.

The evaluator verifies that, for each user data provided in the rationale, the developer indicates the inbound interfaces from which the user data is ingested to the TOE and, if applicable, the outbound interfaces through which the user data is sent to other entities in the operational environment.

The interfaces in the context of this activity don't have to be necessarily TSFIs; the developer is expected to use the functions or interfaces expressed in the AGD_OPE.1 operational guidance as source for this relationship.

Work Unit ADV_PDM.1-3

The evaluator ***shall examine*** that the rationale for data minimisation and the operational user guidance in order to determine that the user-accessible interfaces in the user operational guidance don't indicate the existence of other user data processed by the TOE that is not declared in the rationale for data minimisation.

The evaluator examines the user-accessible interfaces in the user operational guidance and their parameters in order to examine possible data sources through the interfaces that aren't related to any of the user data in the rationale for data minimisation. If such parameters are found, this activity will fail.

ADV_PDM.1.3C The rationale for data minimisation shall demonstrate that all data processed by the TOE is necessary and adequate in relation with the intended purpose of the TOE.

Work Unit ADV_PDM.1-4

The evaluator ***shall examine*** the rationale for data minimisation in order to determine that it demonstrates that all data processed by the TOE is necessary and adequate in relation with the intended purpose of the TOE.

Decommissioning Procedures (AGD_DEC) – Extended

Objectives

Security of the TOE from the perspective of Common Criteria assurance activities shall be maintained not only during development, delivery and operational usage, but also at the end of life of the TOE. Some TOEs are released in the field without the assumption of physical protection of the TOE assets, and they may contain sensitive assets whose confidentiality or integrity could be vulnerated after operational usage, for example in the event of deterioration of the hardware in charge of providing self-protecting features.

Moreover, end of operational usage could mean that the TOE stops being operated by a diligent administrator and, in combination with possible decaying of the self-protection properties, these assets could lack of the adequate TOE or operational environment protection. Therefore, procedures shall be established for TOE users in order to carry out actions prescribed in guidance for secure decommissioning of the TOE in a way that it is ensured that confidentiality and/or integrity of protected assets is not vulnerated upon the end of operational usage of the TOE.

Moreover, because the TOE is already in its operational environment and out of the control of the vendor when the end of life or decommissioning eventually occurs, it is necessary to provide guidance for the users of the TOE to securely perform TOE decommissioning in a way that ensures that TOE protected assets could not be vulnerated after that event. The objective of this family, therefore, is to provide guidance to the user on how to carry out secure decommissioning of the TOE.

Component levelling

This assurance family contains only one component.

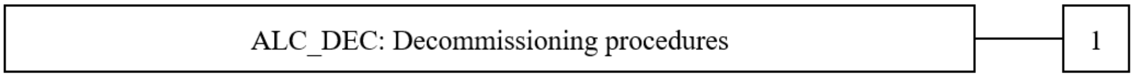

Figure 5: Component levelling of ALC_DEC family

Application notes

The application of the requirements in this family could vary depending on the type of TOE and the kind of protection provided by the operational environment of the TOE.

For example, TOEs whose physical access is protected by restrictions posed by the operational environment objectives may not be too suitable for these requirements, although this would depend on the case. For example, some hardware TOEs to be used “in the field”, such as System-on-a-Chip that is intended for mobile usage, may benefit from secure destruction procedures; they would provide additional assurance of protection against an enlarged window of opportunity in terms of time for an attacker with physical access to the TOE (e.g. to retrieve keys from flash memory), after operational ends, or if malfunction of the device occurs. In other cases, for example software TOEs that store plain-text credentials delegating the protection entirely to the environment may also benefit from these requirements, as upon decommissioning, residual data could not be completely deleted by the TOE from non-volatile storage, unless a secure procedure is used.

Other TOEs evaluated under high assurance evaluation levels may present enough data protection, self-protection and self-testing features that they don’t need any secure decommissioning. In such cases, the requirements included in this family are not needed, unless the TOE vendor decides otherwise.

In any case, after the TOE is out of the control of the vendor there is no way to ensure that a secure decommissioning of the TOE is carried out unless specific guidance is provided by the TOE vendor for it to the TOE users.

In some cases, the guidance could be as simple as providing guidance on how to return the TOE (as a physical asset) to the vendor, who shall then be responsible for secure destruction. In other cases, the TOE users need to be instructed in order to be trained on how to diligently dispose the TOE.

The requirements in this family are separated from AGD_PRE and AGD_OPE ones. However, the requirements of this family are dependent on them, because it is required that, in order to enable the TOE users to follow the decommissioning procedures, they are trained first by following the AGD_PRE and AGD_OPE guidance for TOE secure installation and configuration first, and then for TOE secure operational usage.

AGD_DEC.1 defines the necessary user guidance to be elaborated by the TOE vendor in order to instruct the users on how to carry out secure decommissioning of the TOE.

AGD_DEC.1: Decommissioning procedures (Extended)

Hierarchical to: no other components.

Dependencies: AGD_PRE.1, AGD_OPE.1.

Developer action elements:

AGD_DEC.1.1D **The developer shall provide the decommissioning procedures for the TOE**

Content and presentation elements:

AGD_DEC.1.1C **The decommissioning procedures shall describe all the steps necessary for secure decommissioning of the delivered TOE upon end-of-life of the TOE**

AGD_DEC.1.2C **The decommissioning procedures shall describe all the necessary equipment, tools and auxiliary guidance that is required to perform TOE decommissioning.**

AGD_DEC.1.3C **The decommissioning procedures shall be effective for the purpose of precluding access to the assets protected to the TOE after it has been decommissioned.**

AGD_DEC.1.4C **The decommissioning procedures shall be compatible with the operational environment in which the TOE is operated**.

Evaluator action elements:

AGD_DEC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation work units for AGD_DEC.1 (Extended)

Action AGD_DEC.1.1E

AGD_DEC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

AGD_DEC.1.1C The decommissioning procedures shall describe all the steps necessary for secure decommissioning of the delivered TOE upon end-of-life of the TOE

Work unit ALC_DEC.1-1

The evaluator ***shall examine*** the provided decommissioning procedures to determine that they describe all the steps necessary for secure decommissioning of the delivered TOE upon end-of-life of the TOE.

Decommissioning procedures shall be described and detailed in the guidance provided by the developer. These procedures may vary depending on the type and the nature of the TOE. Some software TOEs could require a to carry out secure deletion of certain data files handled by the TOE from the non-volatile memories of the TOE or of the hardware environment, or it is possible that the destruction procedure may be as simple as running an uninstaller software provided by the TOE. Hardware TOEs, on the other hand, may require either physical destruction of the TOE or some parts of it, or maybe it would be sufficient to run certain commands through its interfaces that could be available as part of AGD_OPE existing user interfaces.

For some physical TOEs, the decommissioning procedure could consist simply in sending the TOE to the vendor, or to a designated contractor, to ensure an appropriate destruction method. In this case, the only required instructions are those necessary to send the TOE to the adequate recipient and the responsibility for effectively perform secure destruction of TOE assets is in the vendor or designated contractor.

In any case, the evaluator shall perform the necessary examination of the guidance in order to determine that the procedure is complete and includes all the necessary steps to be followed.

The destruction procedures should provide detailed information about the following, if applicable:

a) Instructions to stop TOE operation prior to decommissioning procedures, if applicable.

b) Detailed ordered instructions or step to be executed as part of the decommissioning process.

c) Constraints to be met in the procedure steps. For example, it may be necessary to apply some environmental conditions in physical destruction, such as exposing the TOE to a certain temperature and then, the next step cannot be run before waiting some time first.

d) Considerations for human safety when physical procedures are used.

e) Criteria to determine if the decommissioning steps have been adequately executed.

AGD_DEC.1.2C The decommissioning procedures shall describe all the necessary equipment, tools and auxiliary guidance that is required to perform TOE decommissioning.

Work unit AGD_DEC.1-2

The evaluator ***shall examine*** the decommissioning procedures to determine that they describe all the necessary equipment, tools and guidance that is required to carry out and auxiliary guidance that is required to perform TOE decommissioning.

It is not anticipated that any physical or logical equipment in addition to that distributed within the TOE itself is needed by the user to perform the TOE decommissioning. In such case, this work unit is not applicable.

Moreover, if the decommissioning procedures simply consist in sending the TOE to the vendor and the vendor is responsible for the decommissioning, then this work unit isn’t applicable either.

Depending on the type of TOE and the procedures and techniques necessary to perform procedures in order to securely decommission it, it may be required to use special equipment or tools as part of these procedures. Furthermore, specific guidance may be required in order to run the steps associated to the decommissioning procedure that are not trivial, or even guidance may be needed in order to use the required tools.

Tools may vary as well depending on the TOE type. Decommissioning of hardware TOEs may require physical tools such as shredders, chemical substances, or even specialised tools used for degaussing or demagnetisation. It’s possible that the TOE implements external facing interfaces that implement secure information destruction methods and, depending on the TOE type, these may be enough to ensure that the TOE assets have been securely deleted.

Software TOEs, on the other hand, may require only of tools for secure disposal of information stored on the hardware system where the TOE is installed, for example tools that ensure that the contents cannot be recovered from disk after executing the TOE decommissioning procedure.

The documented decommissioning procedures shall identify one by one all the required tools for executing such procedures. Depending on the level of specialisation of the require techniques, it may be enough with specification of generic tools, e.g. without mandating specific commercial brands but just minimum requirements of them. For example, indicating that a generic shredded is required to destroy some TOE would not be an acceptable guidance to fulfil this work unit. Instead of that, indicating a specific commercial model of shredder or the requirements for the measure of the shredded pieces that the shredder shall met is indeed a valid indication.

For software tools, it is not mandatory to indicate specific versions of the software used for decommissioning, as long as the prescribed software meets the requirements needed for destruction of logical data (e.g. various rounds of 73eroization on disk). However, it should be avoided to just reference generic types of software, for example, “a tool for secure disk deletion” is not an appropriate indication but referencing specific commercial or open-source tools, from a certain version on is accepted.

For some software tools, it may be sufficient to run a built-in uninstaller provided with the TOE, without any additional tool required for decommissioning.

For any tool referenced in the decommissioning procedures, the procedures shall provide guidance on how to use such tools for its usage as part of the decommissioning procedure. Depending on the complexity of the procedure and the type of tools used, it may vary between generic instructions, references to section of the publicly available guidance, or detailed specific guidance for the purpose of TOE decommissioning.

Moreover, when no additional tools than the TOE itself are required to run the decommissioning procedures, the guidance shall provide clear instructions on how to use the TOE available interfaces for such purpose. In some cases, referencing specific parts of the TOE operational guidance may be enough. Evaluators shall be aware that referencing parts of the functional specification of the TOE for the same purpose, provided that those parts are not included also in the operational guidance available to the final user, is not a valid way to fulfil this work unit.

The evaluator shall examine the provided guidance in order to determine that they are detailed enough in order to properly carry out the decommission of the TOE.

AGD_DEC.1.3C The decommissioning procedures shall be effective for the purpose of precluding access to the assets protected to the TOE after it has been decommissioned.

Work unit AGD_DEC.1-3

The evaluator ***shall examine** the* decommissioning procedures in order to determine that they are effective for the purpose of precluding access to the assets protected to the TOE after it has been decommissioned.

The effectiveness of the decommissioning procedures described in the user guidance depend mostly on the type of the TOE, the steps provided for its decommissioning and the tools and guidance used for executing such steps.

When the decommissioning procedures consist solely in sending a physical TOE back to the vendor or to a designated contractor, then the evaluator shall judge the effectivity of the procedure following the same criteria as defined for ALC_DEL.1-1 work unit when it is applicable to physical deliveries.

The evaluator shall examine the type of TOE, the nature of the assets protected by it, and the security mechanisms in place to protect such assets, in order to start the analysis for effectiveness of the procedures for TOE decommissioning.

For example, hardware TOE could require physical destruction methods, such as shredders, degaussers, exposition to environmental conditions, etc. when the TOE doesn't provide a method to delete the information stored in its internal non-volatile memories. For example, deleting some areas of a flash memory where sensitive information is stored, such as cryptographic keys, may not be possible without physical destruction because the TOE could implement access restrictions to those assets through the available TOE interfaces. Or it may be possible that the TOE uses read only memories for storage of important assets, hence logical destruction is not possible.

However, hardware TOEs could implement "panic" or "74eroization" mechanisms that are built-in with the TSF and can be triggered through one or more of the available TOE interfaces. This mechanism could be on-demand, for example a "full reset" function of a device, or "collateral", such as entering a number of invalid credentials in the TOE and triggering self-protection mechanisms that effectively destroy the TOE assets.

When physical destruction procedures are applied, the evaluator shall analyse them in order to verify that they leave the TOE in a state where the protected assets are no longer available within the TOE, even as residual information. For example, a TOE that uses SSD storage technology should be physically destroyed and demagnetisation methods are not effective for destroying stored information in them. The evaluator shall judge the adequacy of these procedures with the knowledge gained from the type of TOE and, if necessary, the TOE design.

In the case of software TOEs, the usage of a built-in uninstaller or software logical tools should be enough to destroy TOE assets. However, the evaluator shall carefully examine these techniques in order to verify that they carry out this destruction in a secure way. For example, if the instructions consist in simply "deleting a folder from disk" in a general-purpose operating system, it may be possible to recover information stored in disk by the TOE after deletion. However, if a tool that performs multiple rounds of overwriting disk sectors is used, then the method should be effective and adequate.

The developer may need to consult the TOE design documentation in order to gain enough knowledge of how the TOE implements protection of its assets in order to be able to judge the effectivity of the decommissioning methods.

Moreover, the evaluator shall carefully examine the assets protected by the TOE as defined in the Security Target. Then, the evaluator shall judge if all the assets to be protected by the TOE result effectively destroyed or rendered unusable or unrecoverable as a consequence of running the decommissioning procedures.

AGD_DEC.1.4C The decommissioning procedures shall be compatible with the operational environment in which the TOE is operated.

Work unit AGD_DEC.1-4

The evaluator ***shall examine*** the decommissioning procedures to determine that they are compatible with the operational environment in which the TOE is operated.

The inputs of the Security Target that are of interest as input of this work unit are the description of the operational environment provided in the TOE Overview or TOE Description sections, the description of the non-TOE required hardware/software/firmware and the objectives for the operational environment.

The objectives of the operational environment described in the Security Target may set some restrictions on the type of actions that can be included in the decommissioning procedures. These objectives could involve some constraints in the environment that would prevent an administrator for running them. However, evaluators shall be aware that the objectives for the operational environment are intended to be met while the TOE is operational, and not during or after decommissioning.

For example, a TOE that is assumed to be isolated from physical access to the environment, even from administrators, could not be subject of physical destruction required by the decommissioning procedures. In this case, the procedures shall include instructions to securely stop TOE operation (e.g. through logical means) and once it is out of operation, then the related operational environment objective could be dismissed.

Another factor to consider is the list of required hardware, software or firmware in the TOE environment needed for TOE operation. This could impact in the compatibility of the destruction procedures.

For example, a software TOE may run only in Windows operating systems. Then, a recommendation to use a secure disk deletion tool that runs only in Unix systems would be incompatible.

In the case of physical TOEs, the environment may require some sort of additional protection that makes difficult to execute the decommissioning procedures. As an example, a TOE could be required to be physically locked to its physical environment, but the decommissioning procedure involves physical destruction. Then, the procedure should require first to stop the TOE from operation (if applicable), then unlocking it, and then moving it to the appropriate physical destruction machine used. This example is applicable also if the procedure requires the TOE to be sent back to the developer for its decommissioning.

The evaluator shall take all the above factors into consideration when judging whether the decommissioning procedures are compatible with the TOE operational environment.

ALC_FLR.4 Flaw remediation with distinction between security and functional flaws (Extended)

Objectives

[The same text of the objectives for the ALC_FLR family, as in [CC2022P3] section 16.2, shall be inserted here]

Component levelling

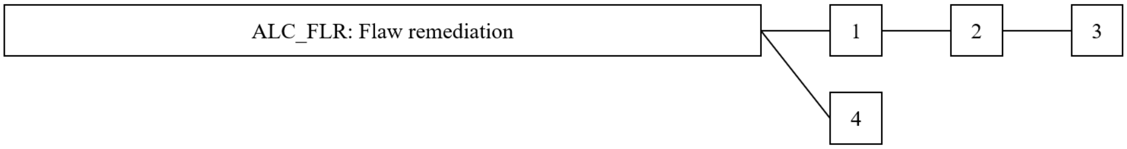

Figure 6: component levelling of ALC_FLR family (extended)

[The same text of the component levelling for the ALC_FLR family, as in [CC2022P3] section 16.2, shall be inserted here, with the following addition]:

A non-hierarchical component aims to require separation in the developer's procedures between the procedures used to handle security flaws and those used to address other issues (e.g., functional) in the TOE.

Application notes

[The same text of the application notes for the ALC_FLR family, as in [CC2022P3] section 16.2, shall be inserted here, with the following addition]:

The extension of this family with the component ALC_FLR.4 intends to introduce in the assessment of the developer's flaw remediation methods particular verifications to ensure that the actions taken into remediating flaws, especially when it comes to distribution of corrective actions in the form of updates, are organized in a way that ensures separation between correction of security flaws and other type of flags, such as functional.

ALC_FLR.4 Flaw remediation with distinction between security and functional flaws

Hierarchical to: None.

Dependencies: ALC_FLR.1 Basic flaw remediation

Developer action elements:

ALC_FLR.4.1D **The developer shall document and provide flaw remediation procedures addressed to TOE developers.**

Content and presentation elements:

ALC_FLR.4.1C **The flaw remediation procedures documentation shall describe shall describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.**

Evaluator action elements:

ALC_FLR.4.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

Evaluation work units for ALC_FLR.4.1 (Extended)

Action ALC_FLR.4.1E

ALC_FLR.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

General

ALC_FLR.4.1C: The flaw remediation procedures documentation shall describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.

Work unit ALC_FLR.4-1

The evaluator ***shall examine*** the flaw remediation procedures documentation to determine that it describe how a separation is established in the distribution of flaw corrections to TOE users, separating corrections of security flaws from other flaws that address non-security flaws.

Work unit ALC_FLR.4-1 indicates that, when a flaw is discovered not to be security-relevant, then there is no need for the flaw remediation procedures to track it further. However, the remediation procedures for security-flaws shall describe how they are separated, e.g., prioritized or handled through a different internal fixing pipeline, with respect to those that aren't security related.

When a flaw is categorized as security-relevant, then the procedures describe how the subsequent actions are designed and conducted in a way ensuring that, when the flaw requires a corrective action to be distributed to TOE users, for example through the distribution of a patch, then that corrective action is separated from and not mixed with other corrections that aren't security-relevant.

The separation in the distribution between security-related corrections and security-non-relevant corrections to users can be evidenced in various ways. First, the written procedures support this separation, for example by enforcing that the generation of patches or other types of corrections that address security-related flaws don't include in any case other type of features, e.g., functional. Second, the updates themselves may contain a distinguished naming convention, e.g., in the filename or in the description provided to users, that clearly identifies if the patch consist in security updates or in other type of updates. The dissemination methods may also establish separate paths depending on the type of correction.

The evaluator may also review, whenever they are available, records of the flaw remediation procedures that were conducted e.g., in previous versions of the TOE in order to judge whether the aforementioned separation has been exercised in past releases of corrections to previous versions of the TOE.

1.6. Definition of extended CC SFRs for CRA coverage

This section contains the definition of extended SFRs that, according to the analysis presented in ***Annex I*** of this document, are required to obtain coverage of CRA essential requirements in EUCC evaluations.

2. ANNEX II: Options for implementation of CRA through EUCC technical elements in STs/PPs

The initial sections in the main body of the report analysed in detail in which ways the technical elements in EUCC can be used to implement CRA (i.e., comply with the CRA Essential Security Requirements) through the appropriate usage of SFRs/SARs and other considerations.

This section aims to explore the ways in which those elements can be incorporated in certification processes, either new or existing, so that it can be ensured that a particular EUCC certification contains the required elements that would help (to the extent that could be feasible in each case), to meet the requirements of the CRA.

As described in the main part of the study, the key elements for implementation CRA through EUCC technical elements consist of:

- Including in the evaluation SFRs and SARs that are equivalent or cover the same requirements as the ESRs in CRA Annex I.
- Defining a security problem definition in the EUCC ST/PP that serves as a simplified formal cybersecurity risk analysis as the one required by CRA, and that results in the selection of SFRs and SARs (that are equivalent to ESRs)
- Defining an adequate scope of the TOE under evaluation that matches the whole product with digital elements or, otherwise, study alternatives to demonstrate that the parts of the product not covered by the EUCC certification also meet with the CRA essential requirements.

This section aims to study in detail the mechanisms that would allow to implement the first point of the previous list, contemplating their advantages and drawbacks, and whether they would be interoperable with existing certification process in the market. **Judgements on which option would be more suitable are not included in this section, the analysis is provided strictly from a technical point of view.** Further sections of this study analyse the suitability of some options over in relation with the certification landscape.

The diagram below shows a summary of the studied mechanisms:

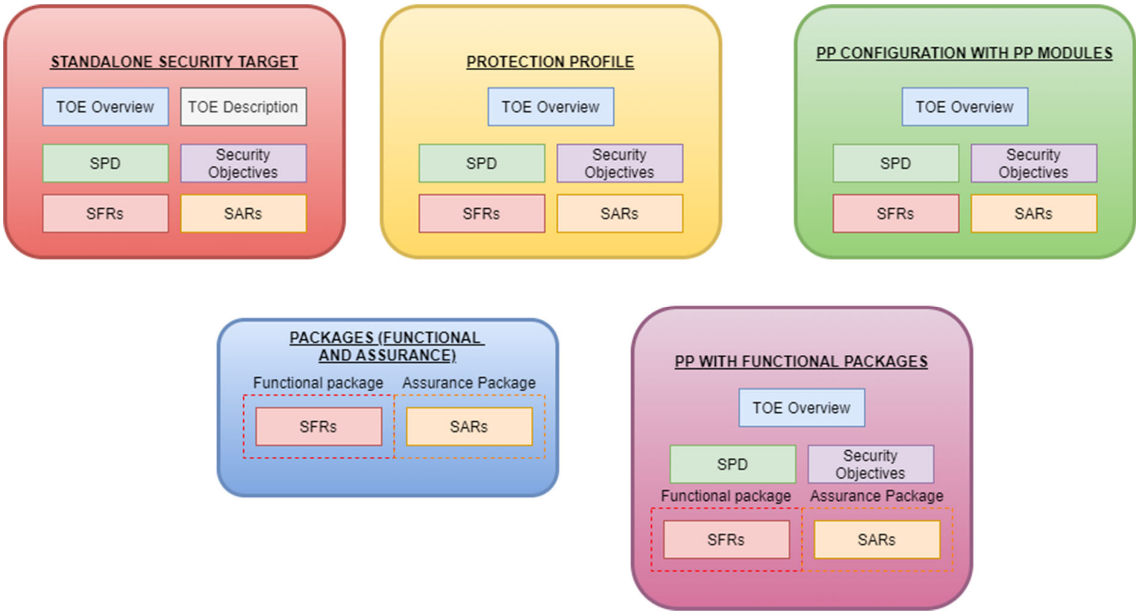

Figure 7: illustrative summary of options

2.1. Standalone Security Target

This option allows manufacturers to create a tailored ST from scratch without claiming conformance to any protection profile. Manufacturers are entitled to choose whichever assurance components, security functional requirements, elements of the security problem definition and security objectives with full freedom in the most convenient way that fits their product features, as long as EUCC/CC rules are met. They are not constrained by any particular scope of the security functions or of the assurance components and activities to be included in the evaluation: manufacturers can choose the scope of the product functionality that is evaluated and the depth of the assurance activities by selecting any existing SFRs/SARs or defining custom ones.

As there is full flexibility in the requirements chosen to be included in the ST, this option allows manufacturers to incorporate in their Security Target all the SFRs and SARs that have been identified in the study as required for to meet CRA essential requirements, so this option provides immediate support for this objective.

Also, since manufacturers have to select which SFRs and SARs among those discussed in this study based on their own cybersecurity risk analysis, the full flexibility given by this option doesn't require the use of any formal CC elements to justify the decision for inclusion or exclusion of SFRs/SARs (as may happen in other options).

When elaborating the ST, manufacturers are required to define (or take from existing sources) elements of the Security Problem Definition and Security Objective that ultimately relate with the SFRs identified in this study as required in order to meet the CRA essential requirements. The reason for this is that the study is focused on the necessary security functional and assurance requirements, immediately linked to the ESRs, without considering other CC elements that support them (e.g., optional SFRs).

The proposal for SARs in this study includes ASE_REQ, in order to support specifying a relationship between the manufacturer's risk analysis and the SARs chosen in the evaluation. Therefore, **direct**

rationales are not supported with this option to order to meet the CRA essential requirements with the current selection of SARs**.**

2.2. Protection Profile for CRA conformance

This option consists in elaborating a **single protection profile** including all the SARs and SFRs that are necessary in order to meet the CRA essential requirements. The protection profile would define the main sections that need to be used in STs of products that declare conformity to such PP, including a TOE Overview, TOE type, Security Problem Definition, Security Objectives, SFRs and SARs.

The main advantage of this option is that, once the PP is approved, it would provide direct harmonization between interpretation of schemes and vendors, and would make validation of conformant STs easier than evaluation of individual standalone STs (e.g., doesn't require a case-by-case analysis in each evaluation for the security problem and objectives).

A significant challenge to address in this option is that the content of the PP sections, in particular its security problem and objectives, should be designed in a way that is generic enough to be suitable for a wide range of product types and highly diverse operational environments, but without introducing too much looseness that can lead to challenges during PP validation.

This option can be supported in the following common tools of the CC:

- **Optional SFRs**: these are SFRs that can be included in the PP but the ST author is allowed to decide whether they are included or not in the PP-conformant ST and, therefore, they can be excluded for the evaluation. For example, this formula would provide powerful flexibility in situations where a ESR is considered not-applicable. For example:
    - With regards to ESR 2.b and 2.c in Annex I, if the TOE does not perform network communications, then FDP_ITC.1 or FPT_TRP.1 could be excluded from the conformant ST.
    - If the TOE does include any configuration data and its state is immutable, then ESR (2)(b) in CRA Annex I shall not be applicable. Then, the optional SFR would allow to exclude FMT_RDC.1 (Extended) from the conformant ST.

  This option directly supports with tools in the CC standard the inclusion/exclusion of SFRs based on the manufacturer's risk analysis.
  However, there is no equivalent tool for SARs in the standard (e.g., no extended SARs). The inclusion and exclusion of SARs shall be addressed by combination with other options, such as assurance packages and PP-Modules (both compatible with PPs).

- **Selection-Based SFRs:** this tool would allow the PP to include SFRs that will be included in or excluded out of the ST that claims conformity with the PP, depending on the option selected by the ST author in another SFR of the protection profile. Although the SFRs considered in this study don't include are not-selection based, it would be possible to model some of them in a way that they become selection-based and permit to include/exclude other related SFRs depending on the value selected in the ST.

- **Direct PP-rationales:** it would allow to omit the security objectives for the TOE in the PP and directly map the threats with the SFRs. However, as this study proposes the ASE_REQ.2 assurance component as required to support the manufacturer's risk analysis on the justification for the selection of SARs, this option cannot be used.

In summary, optional SFRs and/or selection-based SFRs are the principal mechanism to make this option as flexible as possible. For flexibility in choosing SARs, we rely in definition of the extended SARs in a flexible way, so that assurance activities can be skipped whenever they are considered as not applicable.

Refinement: Multiple PPs for groups of similar products in Annex III

Although the main approach consists in creating a single generic PP usable in all CRA Annex III product types, however, this option could be refined to create, instead of a single PP, **multiple PP non-generic vertical PPs** for the most important or significative product types in classes 1 and 2 of Annex III CRA. This would allow to define more specific TOE scopes that fit well for particular categories or group of categories (e.g., network devices, endpoint-installed software…).

In this refined option, the technical elements to be used would be the same proposed in the study, but each PP for a product type or type group would start with a base of SFRs/SARs that have been pre-analysed and determined relevant for the product type. For example, a specific PP for ASICs wouldn't need to include any SFR/SAR related to SBOM, as this type of product doesn't include software or firmware parts.

2.3. PP-Configuration - Modular PP(s) with PP-Modules

This option uses a Protection Profile in a modular way that provides additional flexibility in the adaptation of the PP to presence of absence of functionality characteristic for certain types of technology.

The option is based on the CC concepts of PP-Modules and PP-Configurations that work together to compose a complex but powerful solution. Such concepts are presented below.

PP-Modules

PP-Module is a cohesive collection of elements including SPD, security objectives for the TOE, the operational environment, and SFRs. They can also include SARs. These are defined within the scope of one or more PPs and potentially other PP-Modules. A PP-Module complements one or more PPs and optionally other PP-Modules

Unlike PPs, PP-Modules specifically address security features that are not universally applicable to all products of a particular TOE type. PP-Modules cannot be used independently; they are exclusively employed within PP-Configurations.

The PP-Modules rely on the requirements defined in its Base(s) to provide a complete set of security specifications within a given PP-Configuration. It shall contain a consistency rationale that states the correspondence between the PP-Module and its Base;

Regarding conformance, PP-Modules can claim conformance to CC Part2 (extended), Functional and Assurance Packages, CC Part3 (extended). More than one assurance package may be claimed by a PP-Module. A PP-Module shall provide conformance statements:

- Exact conformance. If and only if all its PP-Module Base(s) are of exact conformance.
- Strict conformance.
- Demonstrable conformance.

PP-Configurations

A PP-Configuration is a specification for the construction of a set of requirements to which conformance can be claimed. **A PP-Configuration shall contain a set of PPs and PP-Modules that compose it, two components at least**. PP-Configurations may contain SARs and claim conformance to assurance packages. **A PP-Configuration shall define the TOE type to which it applies.**

In cases where a combination of functionality is needed in exact-conformance PPs, this can be achieved by creating a PP-Configuration that consists of the PPs to which conformance is desired to be claimed.

Use of PP-Configurations to incorporate technical elements required to meet CRA ESRs

Regarding their application as tool to incorporate the SFRs and SARs required in order to meet the CRA essential requirements, as previously indicated, PP-modules **cannot be used as an independent option, but require combination with a protection profile.** Moreover, **they can be used only as part of a PP-configuration**, and not independently. As such, an option considering PP-modules would be as follows:

1) A PP needs to be defined including the SARs and SFRs (and related SPD and security objectives) that are expected to be common in most product types under scope.
2) Create a number of PP-Modules each of them including groups of SFRs and SARs that are common to a particular functional context that could not be present in all the products (e.g., protection of network communications, configuration reset, etc.)
3) Define a number of PP-Configurations, as meaningful combinations of the base PP plus one or more PP-modules that make sense for certain types of products or groups of types in Annex III of CRA. Example: a PP-Configuration for network appliances with configuration reset and protection of communications. Note: it would be necessary to study and propose options for the types of products in Annex III of CRA.

The principal way in which this solution provides flexibility is by placing the SFRs and SARs that are susceptible of being non-applicable in the majority of product types in separate PP-modules. Then, the available PP-configurations would allow to choose meaningful combinations of PP-modules together with the base PP, to include in the evaluation the group of SARs and SFRs better fit the product under evaluation.

The main drawback of this option is that the number of PP-configurations (combinations of PP + PP-modules) is fixed, so it does not allow for a free selection of any possible combination by the manufacturers. Therefore, it requires a precise elaboration of PP-configuration based on combinations of the available components.

Refinement: Multiple set of base PPs

This option is the same as Option 3, but would involve creating multiple base PPs instead of a single general one. It would allow to tailor more precisely security problems and objectives for particular types of products. This option should avoid creating a PP for each type of product, but rather should the minimum possible number of PPs for groups of similar products, e.g., network appliances, host-software, server-software, and then define a flexible number of PP-modules to be used in different configurations.

2.4. Standalone Functional and assurance packages

A package can be defined by any party and is intended to be re-usable. It contains requirements that are useful and effective in combination.

Packages may be claimed by PPs, PP-Modules, PP-Configurations and STs, and used to construct larger packages.

Assurance packages

Set of assurance components or requirements that may be drawn from CC Part 3, may be extended assurance components, or maybe some combination of both.

Functional packages

Set of functional components or requirements that may be drawn from CC Part 2, or that may be extended functional components or requirements or some combination of both. A functional package may include an SPD and security objectives derived from that SPD.

They can be used in:

1. STs
2. PPs
3. PP-Modules

Functional packages cannot be claimed directly by a PP-Configuration; they shall be part of a PP-Configuration component.

Use of packages of SFRs and SARs to meet CRA ESRs

The approach for this option consists in defining**:**

- **i.** **One or more functional packages** including the SFRs required in order to meet the CRA essential requirements either all together in a single package, or disaggregated into multiple packages containing groups of functionally-related SFRs.
  - **i.** The functional packages can as well include the necessary security problem definition and security objectives that link with the SFRs.
  - **ii.** Security objectives for the TOE cannot be omitted (by direct rationales) since ASE_REQ.2 is included in this study.
- **ii.** **One or more assurance packages** including the SARs required in order to meet the CRA essential requirements.

This option can provide flexibility with regards to inclusion or exclusion of SFRs/SARs of the ST, based on the manufacturer's risk analysis, and it is supported either in:

- a) Fine-grain design of the packages (e.g., including few requirements each).
- b) Thick-grain packages, but using conditional elements such as optional or selection-based SFRs.

The main advantage of this option is its flexibility and the high degree of interoperability with other options. It can be integrated in standalone STs or in PPs that don't claim exact conformance.

2.5. PP with functional packages

This option consists in the definition of one (or a minimal number) of PPs that claim conformance with functional and assurance packages that include the SFRs/SARs required in order to meet the CRA essential requirements.

The approach is very similar to the PP-configurations but this option allows the manufacturer to choose any possible combinations of packages claimed by the ST, and it is not restricted by a fixed number of PP-configurations.

Therefore, the main advantage that this option offer is flexibility in the selection of groups of requirements in accordance with the selection of ESRs done by the manufacturers on the basis of their risk analysis.

2.6. Informational: Common CC formulas for all options

This section describes CC formulas or tools that can be used to support some of the options previously described in this chapter.

Direct rationales

In some cases, defining a ST that omits security objectives for the TOE and directly maps the SFRs to the SPD is appropriate. This is a “Direct Rationale” ST, and is explained in detail in 11.3.3 and Annex D of [CC2022P1].

It is not possible to use this formula when the SARs include ASE_REQ.2, which require an explicit mapping between TOE security objectives and SFRs.

Optional SFRs

Optional requirements are “optional” in the sense that they do not need to be included in a PP/ST in order for the PP/ST to claim conformance (of any type) to a PP or PP.

The first category of optional requirements is elective: requirements in this category do not need to be included in a PP/ST in order for the PP/ST to claim conformance (of any type) to the PP or PP-Configuration where the requirement is defined. In this case, it is not obligatory that the PP/ST includes the requirement, even if the TOE implements the functionality described by the requirement.

The second category of optional requirements is conditional. If the TOE implements the described

functionality then the optional requirement shall be included in the PP/ST. If the TOE does not implement the functionality covered by the optional requirement, then the requirement is not included in the PP/ST.

Selection-Based SFRs

Packages, PPs and PP-Modules may identify a set of selection-based SFRs. In this case, the author additionally ensures that the package/PP/PP-Module clearly indicates the dependencies between a particular selection in a security functional component and/or SFR included in the package/PP/PP-Module and the associated selection-based SFR(s) that shall be included if that selection is chosen by another PP/ST author.

2.7. Interoperability of options with existing certification strategies

When it comes to implementation of CRA through EUCC, and after having analysed the mechanism that allows their inclusion in certification process, it needs to be considered how each of them would be compatible (from a technical point of view) with the different scenarios of products that are already in the market, have a EUCC certification and need to adapt it in order to meet the CRA essential requirements.

If an EUCC-certified product on the market already meets the SFRs and SARs (or equivalent options) that have been identified in this study as necessary in order to meet the CRA essential requirements, then no additional elements need to be added to that certification in general. Then, the existing certification will be potentially suitable to demonstrate that the CRA ESRs are met.

However, if the EUCC-certificate of the product on the market presents some gaps with respect to the necessary SFRs and SARs identified in this study, the manufacturer would need to include the SFRs/SARs in the gap in the scope of the certificate. In order to do so, the factor that impacts the most in the feasibility and complexity of this process from a technical point of view is whether the product is certified using a protection profile.

It is possible to distinguish the following cases:

a) The product in the market is **EUCC-certified doesn’t use Protection Profiles**.
b) The product in the market is **EUCC-certified claiming compliance with one or more Protection Profiles**. Three sub-cases can be distinguished here:
    a. The Protection Profile is claimed with **strict conformance.**
    b. The Protection Profile is claimed with **demonstrable conformance**.
    c. The protection profile is claimed with **exact conformance.**

The compatibility is valued, for each option in terms of compatibility (i.e., if SFRs/SARs can be added to the ST) and complexity (from the perspective of the ST author), describing briefly the implementation process.

Implementation option	**EUCC certification without PP**	**EUCC Certification with PP**		
		Strict conformance	**Demonstrable conformance**	**Exact conformance**
CRA-Tailored Standalone Security Target	**Can add SFRs/SARs:** Yes **Complexity:** Easy **Implementation:** The ST of the EUCC-certified product on the market would be readapted to include the SARs and SFRs required for to meet CRA ESRs, that weren't previously in the ST, and the security problem can be freely reworked.	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST would still claim conformity to the initial PP. The gap between the SFRs/SARs in the PP and those required by CRA are added to the PP compliant-ST, as a superset of the ones existing in the PP. It needs to be reviewed carefully that the security problem in the resulting ST is compatible with that of the PP according to strict conformance rules.	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST would still claim conformity to the initial PP. The gap between the SFRs/SARs in the PP and those required by CRA are added to the PP compliant-ST, with the condition that the resulting SFRs/SARs and SPD are more restrictive than those in the PP.	**Can add SFRs/SARs:** No **Complexity:** N/A **Implementation:** strict conformance doesn't permit that additional SARs or SFRs can be added to those in the PP.
CRA-tailored Protection Profile	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST has to be reworked in order to claim conformance to the CRA-tailored PP. The remaining SARs/SFRs that were in the previous ST but not in the CRA PP need to be added according to the rules of the strict or demonstrable conformance.	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST would claim conformance to both the previous PP and to the CRA PP. The SFRs/SARs and SPDs in both PPs need to be analysed carefully to avoid contradicting statements and ensure compatibility according to strict conformance rules.	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST would claim conformance to both the previous PP and to the CRA PP. The SFRs/SARs and SPDs in both PPs need to be analysed carefully to avoid contradicting statements.	**Can add SFRs/SARs:** No **Complexity:** N/A **Implementation:** strict conformance doesn't permit that additional SARs or SFRs can be added to those in the PP.

PP-Configuration with PP-Modules	**Can add SFRs/SARs: Yes** **Complexity: Medium** **Implementation:** The ST has to be reworked in order to claim conformance to the modular PP and the PP-configurations that are applicable for it. Other SFRs/SARs in the previous ST need to be added according to the rules of the strict or demonstrable conformance, depending on the conformance required by the PP-configuration.	**Can add SFRs/SARs: Dependent** **Complexity: High** Feasibility will depend on whether the existing PP-configurations (combinations of PP-modules contemplated by the PP) contain a configuration that suits to the certified product. **Implementation:** An appropriate PP-configuration needs to be chosen. The ST would claim conformance to both the previous PP and to the modular PP and its chosen applicable configurations. The SFRs/SARs and SPDs in both PPs and PP-configurations need to be analysed carefully to avoid contradicting statements and ensure compatibility according to strict conformance rules.	**Can add SFRs/SARs: Dependent** **Complexity: High** Feasibility will depend on whether the existing PP-configurations (combinations of PP-modules contemplated by the PP) contain a configuration that suits to the certified product. **Implementation:** An appropriate PP-configuration needs to be chosen. The ST would claim conformance to both the previous PP and to the Modular CRA PP and its applicable chosen PP configurations. The SFRs/SARs and SPDs in both PPs need to be analysed carefully to avoid contradicting statements according to demonstrable conformance rules.	**Can add SFRs/SARs: No** **Complexity: N/A** **Implementation:** strict conformance doesn't permit that additional SARs or SFRs can be added to those in the PP.
Standalone Functional and Assurance Packages	**Can add SFRs/SARs: Yes** **Complexity: Easy** **Implementation:** The ST would include the necessary packages. The SFRs/SARs additional to the packages can be added without complexity.	**Can add SFRs/SARs: Yes** **Complexity: Medium** **Implementation:** The ST would claim conformance to the previous PP and will include the necessary packages with SFRs/SARs. The resulting SARs and SPD need to be analysed carefully to avoid contradicting statements and ensure compatibility	**Can add SFRs/SARs: Yes** **Complexity: Medium** **Implementation:** The ST would claim conformance to the previous PP and will include the necessary packages with SFRs/SARs. The resulting SARs and SPD need to be analysed carefully to avoid contradicting statements and ensure compatibility	**Can add SFRs/SARs: No** **Complexity: N/A** **Implementation:** strict conformance doesn't permit that additional SARs or SFRs can be added to those in the PP.

		according to strict conformance rules.	according to demonstrable conformance rules.	
PP with functional packages	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST has to be reworked in order to claim conformance to the PP with functional packages. Other SFRs/SARs in the previous ST need to be added according to the rules of the strict or demonstrable conformance, depending on the conformance required by the PP with functional packages and the packages.	**Can add SFRs/SARs:** Yes **Complexity:** High **Implementation:** The ST would claim conformance to both the previous PP and to the CRA PP and its applicable functional packages. The SFRs/SARs and SPDs resulting in applying both the initial PP and the functional packages need to be analysed carefully to avoid contradicting statements and ensure compatibility according to strict conformance rules.	**Can add SFRs/SARs:** Yes **Complexity:** Medium **Implementation:** The ST would claim conformance to both the previous PP and to the CRA PP and its applicable functional packages. The SFRs/SARs and SPDs resulting in applying both the initial PP and the functional packages need to be analysed carefully to avoid contradicting statements and ensure compatibility according to demonstrable conformance rules.	**Can add SFRs/SARs:** No **Complexity:** N/A **Implementation:** strict conformance doesn't permit that additional SARs or SFRs can be added to those in the PP.

Table 1: Analysis of feasibility for interoperability options

The analysis performed in this table reveals that, on the technical level:

i. EUCC-certified products that don’t claim conformance with a PP in the EUCC certificate can be updated with the gap of required CRA SFRs/SARs in a smooth way, no matter which implementation option among the ones in this study is chosen.
ii. EUCC-certified products claiming conformance with PPs in the EUCC make the addition of additional SFRs and SARs more complex, depending on the type of conformance. In the case of exact conformance, there is a limitation to add these technical elements.

3. Annex III. Template: CRA conformance claims for EUCC certified products

This section proposes a template that manufacturers of EUCC certified products can use to claim conformance with CRA through summarization of the EUCC technical aspects explored in this study.

This template can be incorporated as an annex to the Security Targets (recommended option) or be provided separately to CRA Notified Bodies.

EUCC Protection Profiles that aim to meeting the CRA essential requirements for the products certified claiming conformance to those PPs should provide this template in their certification process. ST authors that later instantiate the PP should reuse that filled template, filling the certification-specific fields in their particular product certification processes.

Note: this template is different from the declaration of conformity mentioned in Annex VII Requirement 7 of CRA.

Template for CRA conformance claim					
Identification					
Doc No.		Version		Date	
EUCC certification ID					
Reference to EUCC Security Target or Protection Profile					
TOE reference					
Applicability *(subsection)*					
Product type. Product category / CRA (e.g. Network management system – CRA, Annex IV)					
Coverage of the product with digital elements by the EUCC certificate *(subsection)*					
Components of the product (e.g., full solution) covered by the EUCC certification					
Components of the product **not covered by the EUCC certification**	If any, reference to harmonised standard, common specification or European cybersecurity certification schemes are applied to parts of the product not included in the scope of the EUCC certification that are **not** considered as remote data processing solutions (*for each component outside the EUCC certification covered by them)*.				
Remote data processing solutions necessary for the operation of the product **not covered by the EUCC certification**	If any, reference to harmonised standard, common specification or European cybersecurity certification schemes are applied to the remote data processing solution				
	Which SFRs in the Security Target and/or assumptions in the SPD ensure a secure communication channel between the TOE and the remote data processing solution.				
If the scope of the TOE is smaller than the scope of the product with digital elements, justification than the TOE boundary is sufficient	*Rationale based in PP/STs SFRs, Security Problem Definition or design details, or reference to the part of the technical documentation containing the justification*				
Applicability of CRA Essential Security Requirements in Annex I, part I (subsection)					
Requirement	Applicable (Yes/No)		If the ESR in Annex I, part I is applicable to the TOE: SFRs in the ST/PP covering the CRA ESR If the ESR in Annex I, part I is not applicable to the TOE: rationale with reference to the Security Problem Definition relevant elements in the ST/PP that justifies why the requirement is not applicable		
A I.1 (1)					
A I.1 (2) (a)					
A I.1 (2) (b)					
A I.1 (2) (c)					
A I.1 (2) (d)					
A I.1 (2) (e)					
A I.1 (2) (f)					
A I.1 (2) (g)					
A I.1 (2) (h)					

A I.1 (2) (i)		
A I.1 (2) (j)		
A I.1 (2) (k)		
A I.1 (2) (l)		
A I.1 (2) (m)		
CRA Essential Security Requirements in Annex I, part II (subsection)		
Requirement	Technical specification used to cover the ESR / SARs/SFRs in the ST/PP covering that CRA ESR	
A I.2 (1)		
A I.2 (2)		
A I.2 (3)		
A I.2 (4)		
A I.2 (5)		
A I.2 (6)		
A I.2 (7)		
A I.2 (8)		
Reference to elements in the SPD of the ST/PP that taken into account the foreseen support period		
Optional: If the manufacturer chosen to make the SBOM publicly available, where the software bill of materials can be accessed by the user (i.e. public URL). **Note:** It can be provided as a separate deliverable or inside a ST annex.		

Table 2 Template for CRA conformance claims in EUCC certified products