ETSI TR 104 071 V1.1.1 (2025-07)

TECHNICAL REPORT

Cyber Security (CYBER); Mapping of the Consumer Mobile Device Protection Profile security requirements to the CRA essential cybersecurity requirements

Reference

DTR/CYBER-00130

Keywords

cyber security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights 4

Foreword....4

Modal verbs terminology....4

Introduction 4

1 Scope 5

2 References 5

2.1 Normative references 5

2.2 Informative references....5

3 Definition of terms, symbols and abbreviations....6

3.1 Terms....6

3.2 Symbols....6

3.3 Abbreviations 6

4 Methodology 7

5 Scope of the assessment 7

6 CRA Annex I Essential Cybersecurity Requirements Part I comparison 8

7 CRA Annex I Essential Cybersecurity Requirements Part II comparison 14

8 Remote data processing....17

9 Gap analysis 18

9.1 Product scope and TOE....18

9.2 Security Functional Requirements 18

9.3 Security Assurance Requirements....18

9.4 Remote Data Processing....19

Annex A: Change history 20

History 21

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The European Commission issued a horizontal legislation, the Cyber Resilience Act (CRA) [i.1], to implement security measures in products with digital elements, throughout the product lifetime. Consumer Mobile Devices fall in the scope of the CRA [i.1] and need to prove their conformity with this legislation. The CRA [i.1] defines several ways to prove conformity and one of these methods is the application of a European cybersecurity certification scheme adopted pursuant to regulation (EU) 2019/881 [i.8].

EUCC [i.9] is a European cybersecurity certification scheme based on Common Criteria ([i.10], [i.11], [i.12], [i.13], [i.14] and [i.15]) and it can be used to provide presumption of conformity to CRA [i.1] assuming that all the essential cybersecurity requirements set out in Annex I of CRA [i.1] are covered.

In the present document the Consumer Mobile Device Protection Profile (CMDPP) ([i.2], [i.3], [i.4], [i.5], [i.6] and [i.7]) security functional requirements and security assurance requirements will be analysed in order to show how they can cover the CRA [i.1] essential cybersecurity requirements; potential gaps will be identified as well as potential solutions to cover such gaps.

1 Scope

The present document provides a mapping between the Consumer Mobile Device Protection Profile (CMDPP) in the ETSI TS 103 732 series ([i.2], [i.3], [i.4], [i.5], [i.6] and [i.7]) security requirements and the essential cybersecurity requirements from the Annexes of the Cyber Resilience Act (CRA) [i.1]. The present document will also analyse the gaps between the CMDPP ([i.2], [i.3], [i.4], [i.5], [i.6] and [i.7]) (if any) and the CRA [i.1], considering how to address them where necessary.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[i.2] ETSI TS 103 732-1 (V2.1.2) (11-2023): "CYBER; Consumer Mobile Device; Part 1: Base Protection Profile".

[i.3] ETSI TS 103 732-2 (V1.1.2) (11-2023): "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

[i.4] ETSI TS 103 932-1 (V1.1.2) (11-2023): "CYBER; Consumer Mobile Devices Base PP-Configuration; Part 1: CMD and Biometric Verification".

[i.5] ETSI TS 103 732-3 (V1.1.1) (10-2023): "CYBER; Consumer Mobile Device; Part 3: Multi-user Protection Profile Module".

[i.6] ETSI TS 103 732-4 (V1.1.1) (06-2024): "CYBER; Consumer Mobile Device; Part 4: Preloaded Applications Protection Profile Module".

[i.7] ETSI TS 103 732-5 (V1.1.1) (07-2024): "Cyber Security (CYBER); Consumer Mobile Device; Part 5: Bootloader & Root of Trust Protection Profile Module".

[i.8] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.9] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[i.10] ISO/IEC 15408-1:2022: "Information security, cybersecurity and privacy protection -Evaluation criteria for IT security — Part 1: Introduction and general model".

[i.11] ISO/IEC 15408-2:2022: "Information security, cybersecurity and privacy protection -Evaluation criteria for IT security — Part 2: Security functional components".

[i.12] ISO/IEC 15408-3:2022: "Information security, cybersecurity and privacy protection -Evaluation criteria for IT security — Part 3: Security assurance components".

[i.13] ISO/IEC 15408-4:2022: "Information security, cybersecurity and privacy protection -Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities".

[i.14] ISO/IEC 15408-5:2022: "Information security, cybersecurity and privacy protection -Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements".

[i.15] ISO/IEC 18045:2022: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security — Methodology for IT security evaluation".

[i.16] ENISA Cyber Resilience Act implementation via EUCC and its applicable technical elements (Final version: 27/01/2025).

[i.17] GSMA™: "SGP.06 GSMA eUICC Security Assurance Principles v2.2".

[i.18] GSMA™: "SGP.07 GSMA eUICC Security Assurance Methodology v2.2".

[i.19] GSMA™: "SGP.25 eUICC for Consumer and IoT Device Protection Profile v2.1".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

embedded UICC: UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the terminal, and enables the secure changing of subscriptions

preloaded application: application provided by the TOE manufacturer as part of the system software that cannot be uninstalled by the user

UICC: smart card that conforms to the specifications written and maintained by the ETSI Secure Element Technologies Technical Body

NOTE: UICC is neither an abbreviation nor an acronym.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADP	Application Distribution Platform
CC	Common Criteria
CEM	Common Evaluation Methodology
CMD	Consumer Mobile Device
CMDPP	Consumer Mobile Device Protection Profile
CRA	Cyber Resilience Act
DoS	Denial of Service

ECR	Essential Cybersecurity Requirement
eSA	eUICC Security Assurance
EUCC	European Union Cybersecurity Certification
GCF	Global Certification Forum
GDPR	General Data Protection Regulation
MNO	Mobile Network Operator
OS	Operating System
PP	Protection Profile
PTCRB	PCS Type Certification Review Board
RDP	Remote Data Processing
SAR	Security Assurance Requirement
SBOM	Software Bill Of Material
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Function

4 Methodology

The present document compares each CRA essential cybersecurity requirements with the SARs and SFRs of the CMDPP documents ([i.2], [i.3], [i.4], [i.5], [i.6] and [i.7]). Two other dimensions are considered in the comparison: the SARs and SFRs defined in the Common Criteria version 2022 ([i.10], [i.11], [i.12], [i.13], [i.14] and [i.15]) than may be used instead of those in the CMDPP due to the fact that CMDPP is based on a previous CC version (i.e. Common Criteria version 3.1R5) and the content of the ENISA document Cyber Resilience Act implementation via EUCC [i.16].

ETSI TS 103 732-1 [i.2], in clause 4.5 claims conformance to CC v3.1 Release 5 and the CC and CEM addenda and it is conformed to the package EAL2 augmented with ALC_DVS_EXT.1 & ALC_FLR.3.

As per EUCC [i.9] the CMDPP ([i.2], [i.3], [i.4], [i.5], [i.6] and [i.7]), which implement AVA_VAN.2 vulnerability assessment, is considered at assurance level 'substantial'.

5 Scope of the assessment

The CMDPP TOE is a subset of the Consumer Mobile Device (CMD) seen as product with digital elements in the context of the CRA [i.1]. Although the CMDPP TOE includes hardware, the Operating System and the preloaded apps (see clause 4.1 of ETSI TS 103 732-1 [i.2]), the radio interface of the CMD including its security functionality (UICC/SIM) related to the cellular mobile communication are not included in the TOE.

The cellular mobile communication functions are out of the scope of the CMDPP.

However, as suggested in [i.16], the PP owner can justify the difference between the CMDPP TOE and the CMD on the basis of the risk analysis linked to the CMDPP Security Problem Definition. If a gap still remain it has to be covered with an extension of the CMDPP or other means.

The security of the mobile communication credentials is delegated to the secure element which stores them. Depending on the secure element form factor there are two scenarios:

a) The secure element is a UICC. In this case the UICC is not provided by the CMD manufacturer but from the MNO chosen by the user purchasing the CMD. The UICC is therefore not part of the CMD but it is itself a different product with digital elements. The UICC manufacturer is therefore responsible of the CRA conformity of the UICC.

b) The secure element is an embedded UICC (eUICC) or an integrated eUICC. In this case the secure element is a component included by the CMD manufacturer in the CMD. The eUICC and the integrated eUICC have their own Protection Profile and moreover they are products with digital elements that need to be supplied to the CMD manufacturer with proof of CRA conformity (i.e. CE mark). It is a duty of the CMD manufacturer to verify that the eUICC or the integrated eUICC is conform to CRA.

In both cases the secure element which stores the mobile communication credentials may be certified independently by dedicated security assessment schemes and is not introducing a gap.

The other component involved in the CMD cellular mobile communication functions is the cellular modem. The modem interacts with the (e)UICC and provides the cellular mobile connectivity with the mobile network implementing the 3GPP standards. The implementation of such standard is guaranteed by the certification provided by Global Certification Forum (GCF) and PCS Type Certification Review Board (PTCRB). The functional compliance to the 3GPP standards is therefore granted.

The cellular modem is however part of the CMDPP TOE because the later includes all the CMD hardware; it is therefore subject to the vulnerability management of the CMDPP TOE.

Based on the above consideration it appears that the gaps in the scope of the CMDPP TOE are covered by the (e)UICC certification and the modem functional compliance provided by the GCF or PTCRB.

6 CRA Annex I Essential Cybersecurity Requirements Part I comparison

This clause compares the Essential Cybersecurity Requirements set out in CRA Annex I Part I "Cybersecurity requirements relating to the properties of products with digital elements" with the CMDPP SFR/SAR.

The CRA ECR in Table 1 below are provisions defined in the Cyber Resilience Act [i.1].

Table 1: Mapping of CMDPP SFRs and SARs versus CRA ECR Annex I Part I

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion

(1) 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;	-	ASE_SPD.1 Security problem definition;
		ASE_OBJ.2 Security objectives;
		ASE_REQ.2 Derived security requirements.
			ENISA request:
			ASE_SPD.1 Security problem definition;
			ASE_OBJ.1 Security objectives;
			ASE_REQ.1 Direct rationale security requirements.
				Covered

(2) 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;	-	AVA_VAN.2 Vulnerability analysis	ENISA request minimum: AVA_VAN.1 Vulnerability survey	Covered

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(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;	FPT_RCV.2 Automated recovery	ADV_ARC.1 Security architecture description	The CMD is provided with the possibility to reset it to the factory configuration. The factory configuration implements the security architecture described in ADV_ARC.1. This is not the case where the CMD is deliberately provided in a non-secure configuration. FPT_RCV.2 mandate the TOE to return to a secure state using automated procedures.	Covered
I 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;	FDP_UPF_EXT.1: Update check frequency; FMT_SMF.1/APP_ Update Specification of Management Functions FMT_SMF.1/SSW_ Update Specification of Management Functions	-	The FDP_UPF_EXT.1 defines requirements for the frequency the TOE checks for updates of apps, system software and actions if an update is available. This ensures that security updates are installed within an appropriate timeframe (e.g. "an interval of no more than 1 month"). FMT_SMF.1/APP_Update and FMT_SMF.1/SSW_Update defines requirements for the TSF to specify if the software update (application or system software) is automatically installed, or the user is notified after the download, or the user is notified about the software update without the download. Several further actions are specified after the user selection.	Covered

(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;	FIA_UAU.1 Timing of authentication;
	FIA_UAU.1 Timing of authentication;
	FDP_ACC.1/UserDataAsset Subset access control;
	FDP_ACF.1/UserDataAsset Security attribute based access control;
	FIA_AFL.1 Authentication failure handling
		-	Authentication and access control requirements are fulfilled by the CMDPP.
			FIA_AFL.1 the allowed threshold of authentication attempts and the actions when the final attempt fails.
				Covered

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion

I 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;	Stored data confidentiality: FDP_ACF.1/UserDataAsset Security attribute based access control;
	Confidentiality of communication:
	FTP_ITC_EXT.1/BT Inter-TSF trusted channel;
	FTP_ITC_EXT.1/HTTPS Inter-TSF trusted channel;
	FTP_ITC_EXT.1/TLS Inter-TSF trusted channel;
	FTP_ITC_EXT.1/WLAN Inter-TSF trusted channel;
	Cryptographic mechanisms:
	FCS_RNG_EXT.1 Random number generation;
	FCS_CKM.1/Asymmetric Cryptographic key generation;
	FCS_CKM.1/Symmetric Cryptographic key generation;
	FCS_COP.1/SigGen Cryptographic operation;
	FCS_COP.1/KeyEst Cryptographic operation;
	FCS_COP.1/Symmetric Cryptographic operation;
	FCS_COP.1/Derivation Cryptographic operation;
	FCS_COP.1/Hash Cryptographic operation;
	FCS_COP.1/Keyed Hash Cryptographic operation
		-	FDP_ACF.1 defines the conditions under which the CMD decrypt the User Data Assets based on their classification; this assumes that the User Data Assets are encrypted on the CMD.
			The confidentiality of the communication is defined within the TOE scope for Bluetooth, HTTPS, TLS and WLAN.
			Other supported TSF trusted channel might be added by the manufacturer in its ST, but this is out of the scope of the present TOE.
			Cryptographic mechanisms are covering the state of the art.
				Covered

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion

(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;	Integrity of communication:
	FTP_ITC_EXT.1/BT Inter-TSF trusted channel;
	FTP_ITC_EXT.1/HTTPS Inter-TSF trusted channel;
	FTP_ITC_EXT.1/TLS Inter-TSF trusted channel;
	FTP_ITC_EXT.1/WLAN Inter-TSF trusted channel;
	Cryptographic mechanisms:
	FCS_RNG_EXT.1 Random number generation;
	FCS_CKM.1/Asymmetric Cryptographic key generation;
	FCS_CKM.1/Symmetric Cryptographic key generation;
	FCS_COP.1/SigGen Cryptographic operation;
	FCS_COP.1/KeyEst Cryptographic operation;
	FCS_COP.1/Symmetric Cryptographic operation;
	FCS_COP.1/Derivation Cryptographic operation;
	FCS_COP.1/Hash Cryptographic operation;
	FCS_COP.1/Keyed Hash Cryptographic operation
			The Integrity of the communication is defined within the TOE scope for Bluetooth, HTTPS, TLS and WLAN.
			Other supported TSF trusted channel might be added by the manufacturer in its ST, but this is out of the scope of the present TOE.
			Cryptographic mechanisms are covering the state of the art.
			The integrity of the stored data is not clearly mentioned in ETSI TS 103 732-1 [i.2]. A possible way forward is to require in FCS_CKH_EXT.1 an explanation about the algorithm used to grant the data integrity. Alternatively, to use a new SFR from CC2022 like FDP_SDI.
			The report of the data corruption is not applicable to Consumer Mobile Device scenario. The user will not be able to use the data if they are corrupted and most likely the application of service affected by the problem will not work.
				Possible gap

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(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 (data minimisation);			ENISA defined an extended SAR for this purpose: ADV_PDM.1: Processed Data Minimisation (Extended). However, as described in section 8 for RDP, the CMD is expecting that the preloaded application will demonstrate their conformity to CRA separately from the CMD. This means that the data minimisation concept applies only to the CMD main OS and system services (e.g. ADP).	Possible gap
(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;	FPT_FLS.1 Failure with preservation of secure state FPT_RCV.2 Automated recovery	-	The TSF preserves a secure state in case of failures due to software update. The secure state can be the state before the update is executed or a state for recovery as defined in FPT_RCV.2 Automated recovery. FPT_RCV.2 mandate the TOE to return to a secure state using automated procedures. The TSF checks its integrity running a suite of self-tests at the initial start-up to demonstrate its correct operation. Incidents at that stage are countered with FPT_RCV.2. However, the DoS attacks are considered to be network attacks (or network-based, anyway), and these two SFRs are not applicable to that scenario. They are considered only to handle the case where there is a failure in the system software. The scenario where the CMD is used to perform DdoS attack against a network is protected by the authentication and authorization SFRs.	Covered or NA

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;	The TSF protects itself trough: FPT_PHP.3 Resistance to physical attack FPT_TST.1 TSF testing		The attacks scenarios are local, physical attacks, not relevant to network services. This is not really relevant for the mobile device as it is not providing services to other devices.	NA

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;	-	AVA_VAN.2 Vulnerability analysis;
		ADV_TDS.1 Basic design;
		ADV_FSP.2 Security-enforcing functional specification;
		ADV_ARC.1 Security architecture description.
			ENISA request:
			AVA_VAN.1 Vulnerability survey;
			ADV_TDS.1 Basic design;
			ADV_FSP.1 Basic functional specification;
			ADV_ARC.1 Security architecture description.
				Covered

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	FPT_FLS.1 Failure with preservation of secure state
	FPT_RCV.2 Automated recovery
		ADV_ARC.1 Security architecture description;
		ADV_TDS.1 Basic design;
		ADV_FSP.2 Security-enforcing functional specification.
			ENISA request:
			FPT_FLS.1 Failure with preservation of secure state;
			FPT_RCV.1 Manual recovery;
			ADV_ARC.1 Security architecture description;
			ADV_TDS.1 Basic Design;
			ADV_FSP.1 Basic functional specification.
				Covered

(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;			ENISA request: FMT_SMR.1 Security roles. In FAU_GEN.1 Audit data generation it is necessary to indicate which events are logged. In FMT_SMF.1, the opt-out mechanism (enable/disable audit function) needs to be included.	Possible Gap

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(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.	FCS_CKM.4 Cryptographic key destruction	-	The permanent removal of the user data is one of the CMDPP Security Objectives: O.SECURE_WIPE The TOE is able to make user data assets permanently unreadable. This objective is achieved by FCS_CKM.4 specifying that keys from the key hierarchy for each class of data can be deleted on request of the user, making the data unreadable. The user data included in the User Data Assets are transferred in a secure manner using the mechanisms listed for ESR 2I. The ENISA requested SFRs are not applicable as user data are neither exported nor transmitted. The SFR FDP_RIP.1 subset residual information protection is replaced with the alternative FCS_CKM.4 achieving the equal result.	Covered

7 CRA Annex I Essential Cybersecurity Requirements Part II comparison

This clause compares the Essential Cybersecurity Requirements set out in CRA Annex I Part II "Vulnerability handling requirements" with the CMDPP SFR/SAR.

The CRA ECR in Table 2 below are provisions defined in the Cyber Resilience Act [i.1].

Table 2: Mapping of CMDPP SFRs and SARs versus CRA ECR Annex I Part II

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
Manufacturers of products with digital elements shall:	-	-	-	-
(1) identify and document vulnerabilities and components contained in products 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 products;	-	ALC_FLR.3 Systematic flaw remediation	ALC_FLR.3 covers the first part of the ESR. The second part related to a software bill of materials is not currently covered. ENISA is defining an extended SAR: ALC_SBM.1: Software bill of materials (Extended), but it would be useful to evaluate if this can be achieved with alternative SARs defined in CC2022.	Possible Gap
(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;	-	ALC_FLR.3 Systematic flaw remediation	ENISA request at minimum ALC_FLR.1 Basic flaw remediation. The extended component defined by ENISA about the distinction between security and functional updates is not applicable for the CMD scenario where in several cases the way to remediate a vulnerability is a mix between a security and a functional update.	Covered
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	-	-	ENISA is defining an extended SAR: ALC_PSR.1 Periodic security review and testing. However, the EUCC surveillance mechanism implicitly fulfil the requirement. The EUCC scheme itself is covering the requirement.	Covered

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(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;	-	ALC_FLR.3 Systematic flaw remediation	ENISA request at minimum ALC_FLR.1 Basic flaw remediation.	Covered
(5) put in place and enforce a policy on coordinated vulnerability disclosure;	-	-	This is not applicable to the product certification.	NA
(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;	-	ALC_FLR.3 Systematic flaw remediation	ENISA request at minimum ALC_FLR.2 Flaw reporting procedures.	Covered
(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;	-	ALC_FLR.3 Systematic flaw remediation	ENISA request at minimum ALC_FLR.3 Systematic flaw remediation. The extended component defined by ENISA about the distinction between security and functional updates is not applicable for the CMD scenario where in several cases the way to remediate a vulnerability is a mix between a security and a functional update.	Covered

CRA ECR	CMDPP SFRs	CMDPP SARs	Rationale	Conclusion
(8) ensure that, where security 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.	-	ALC_FLR.3 Systematic flaw remediation	ENISA request at minimum ALC_FLR.3 Systematic flaw remediation. The extended component defined by ENISA about the distinction between security and functional updates is not applicable for the CMD scenario where in several cases the way to remediate a vulnerability is a mix between a security and a functional update. The commercial aspects of the ESR is not applicable to the CMDPP.	Covered

8 Remote data processing

The remote data processing service is defined in the Cyber Resilience Act [i.1] as a data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions.

In the context of the CMDPP it is necessary to make some assumptions on the TOE defined in ETSI TS 103 732-1 [i.2] concerning the CMD functionalities that involve a remote data processing:

- The functionalities related to cellular mobile communication (that are actually out of the scope of CMDPP) have their counterpart in the cellular mobile network that performs a remote data processing to allow the cellular mobile communication service. However, the cellular mobile network is not designed and developed by the CMD manufacturer and it is under the responsibility of the Mobile Network Operators (MNOs), therefore this remote data processing cannot be considered as part of the CMD intended as product with digital element.

- The preloaded application are part of the TOE and their SFR/SAR are described in the base PP ETSI TS 103 732-1 [i.2] and the PP Module ETSI TS 103 732-4 [i.6]. The scope of the preloaded applications SFR/SAR is to grant they are not negatively affecting the main OS and the CMD user data. The functionalities of each preloaded application are not considered as part of the TOE and it is expected they are separately tested or certified (whatever will be the scheme used). This means that in the context of the CRA [i.1] the preloaded application remote data processing, if any, is to be handled within the preloaded application CRA conformity and not in the CMD CRA conformity. Moreover, some preloaded applications, even if they are included in the CMD by the CMD manufacturer, are designed and developed by a third party that design, develop and operate the remote data processing; therefore, in these cases, this remote data processing cannot be considered as part of the CMD intended as product with digital element.

- The remote services provided to the CMD in order to perform its functionalities are described in clause 4 of ETSI TS 103 732-1 [i.2]. The CMD uses and Application Distribution Platform (ADP) to allow the user to download the mobile device applications. Such ADP is usually provided by the CMD manufacturer and provides also the functionality to install the mobile application on the device. When the ADP is designed, developed and operated by the CMD manufacturer the related remote data processing is considered part of the CMD intended as product with digital element. The actual version of the CMDPP is not covering this part therefore there is a gap to cover for this functionality. The case where the user decides to use a third party ADPs is out of the scope of the CMDPP and it is also not in the scope of the CRA [i.1] due to the fact these ADPs are not under the control of the manufacturer.

- Other remote servers may be present in the CMD ecosystem; one on them is the trustworthy update server which provides secure update to the CMD system software. This server is fully under the control of the CMD manufacturer therefore the remote data processing is considered part of the CMD intended as product with digital element. The actual version of the CMDPP is not covering this part therefore there is a gap to cover for this functionality. Other servers, if any, has to be handled case by case.

The concern with the Remote data processing being included within the direct boundary of the CMDPP is that it is difficult to properly scope the requirements between both the client and remote server into a single set of requirements. This will have to be discussed as to the best way to cover these requirements.

9 Gap analysis

9.1 Product scope and TOE

The parts that are today out of the scope of the CMDPP have to be handled to cover the entire Consumer Mobile Device products in light of the CRA conformity. In particular the two aspects to cover are:

- eUICC: the eUICC is part of the CMD and the CMD manufacturer has to grant its conformity. This can be achieved reusing the eUICC Common Criteria certification based on the related protection profile [i.19] or considering the GSMA eSA eUICC certification scheme [i.17] and [i.18].
- Cellular modem: the 3GPP functionalities of the cellular modem are out of the scope of the CMDPP. This has to be handled even due to the fact that the modem is an important product in the CRA context. There are some potential solutions that can be considered to fill this gap in the scope:
  - Re-use GCF and/or PTCRB certification.
  - Consider the CRA compliancy of the modem (e.g. using the vertical harmonised standard for the routers, modems intended for the connection to the internet, and switches [i.1]).
  - A combination of both.

  These ways forward could be part of the CMDPP Assumption section.

9.2 Security Functional Requirements

There are some gaps to be filled in the next version of the CMDPP:

1) CRA ECR Annex I Part I article 2(f) related to the integrity of the stored data; this is not explicitly covered by the CMDPP. This could be solved with the CC2022 FDP_SDI or with an application note of the existing FCS_CKH_EXT.1.
2) CRA ECR Annex I Part I article 2(g) related to data minimization. It is important to clarify that the CMDPP data minimization is not covering the mobile application behaviours This means that the data minimization concept applies only to the CMD main OS and system services (e.g. ADP).
3) CRA ECR Annex I Part I article 2(l) related to recording and monitoring relevant internal activity; there could be a gap because today the CMDPP does not provide any SFR/SAR on this topic. However further investigation is needed to understand which level of monitoring is needed also considering the monitoring done by online services linked to the user accounts. The opt-out mechanism for the user is not relevant in the Consumer Mobile Device case because it assumes a specific knowledge of the logged information. Lastly GDPR implication needs to be considered.

9.3 Security Assurance Requirements

The main gap identifies in the SAR section is related to the CRA ECR Annex I Part II article 1 related to the SBOM requirement. This gap can be filled with an extended SAR or with a combination of existing SAR in CC2022.

9.4 Remote Data Processing

Accordingly, with the analysis did in clause 8 of the present document, the remote data processing solution to be considered a part of the CMDPP are the ADP provided by the CMD manufacturer and the remote server used to provide secure update of the system software when this involve the processing of the user data.

Annex A:
Change history

Date	Version	Information about changes
September 2024	V0.0.1	Introduction, Scope, References and skeleton of the present document
April 2025	V0.0.7	Stable draft
April 2025	V0.0.9	Stable draft after the rapporteur call
May 2025	V0.0.11	Final draft for approval
May 2025	V0.0.12	Answer to TO comments
May 2025	V0.0.13	Solved the last editorial comments

History

Document history		
V1.1.1	July 2025	Publication