COMBITECH EUCC SCHEME

Ref. No
CAB-260225-170635-567

Issued by
Anders Staaf

Date
2026-03-11

Issue
1.0

Appoint
Peter Döös

Classification
COMPANY RESTRICTED

Application
EUCC/ISO17065

Combitech EUCC Crypto Policy

Contents

Document History

Date	Ver	Description	Author
2026-02-26	0.1	First draft version	Anders Staaf
2026-03-11	1.0	Updated after review	Anders Staaf

1 Introduction

This document is part of the Combitech certification and evaluation regulations for use with EUCC, defined by its implementing act, *Commission Implementing Regulation (EU) 2024/482 of 31.1.2024*, ref. [EUCC]. EUCC and Combitech's certification and evaluation regulations are below called the Combitech EUCC Certification and Evaluation Scheme or just the Scheme.

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of Information and Communications Technology (ICT) products for which security is a consideration, as well as those already involved with the Scheme, e.g., certifiers, evaluators, customers, contractors, and security consultants.

1.1 Purpose

The purpose of this document is to describe Scheme's requirements on crypto handling.

General information about the Scheme is published in *Combitech EUCC Certification and Evaluation Scheme*, CAB-240701-164858-361, Combitech AB, ref. [Scheme].

1.2 Terminology

The following terms are used to specify requirements:

SHALL	Within normative text, "SHALL" indicates "requirements strictly to be followed in order to conform to the document and from which no deviation is permitted." (ISO/IEC).
SHOULD	Within normative text, "SHOULD" indicates "that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required." (ISO/IEC) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
MAY	Within normative text, "MAY" indicates "a course of action permissible within the limits of the document." (ISO/IEC).
CAN	Within normative text, "CAN" indicates "statements of possibility and capability, whether material, physical or causal." (ISO/IEC).

2 Requirements Specification

2.1 Crypto Primitives

Crypto functionality used by the TOE shall be specified in the PP, PP-Module, functional package, or ST. The crypto functionality shall be specified using Security Functional Requirements, SFRs, from the FCS class in Common Criteria part 2, ref. [CCpart2], or extended components derived from the FCS class. It is recommended but not mandatory to use requirement specifications from the CCDB, Specification of Functional Requirements for Cryptography, ref. [CryptoCatalogue].

Crypto mechanisms should be chosen from ENISA Agreed Cryptographic Mechanisms, ref. [CryptoMechanisms]. A rationale with vulnerability assessment shall be provided in the PP, PP-Module, functional package, or ST if other mechanisms or other key lengths are used.

The [CryptoCatalogue] and [CryptoMechanisms] are partly overlapping. If they are contradictory, [CryptoMechanisms] should be chosen preferentially.

High level SFRs intended to be realized by crypto means, shall be supplemented with SFRs from the FCS class specifying crypto functionality and mechanisms. Example of high level SFRs that can be realized by crypto can be trusted channels and paths according to FTP_ITC, FTP_TRP, FTP_PRO and internal TOE transfer according to FDP_ITT.

2.2 Crypto Protocols

The most commonly used crypto protocols are TLS, IPsec, and SSH. The protocols should be specified by the SFR family FTP_PRO or by extended components.

For TLS the following parameters shall be specified: Supported version and allowed cipher-suites. For IPsec the following parameters shall be specified, key exchange: IKE version, mode, supported integrity and/or authenticated encryption (AEAD) algorithms, encryption primitives, Oakley (Diffie-Hellman) groups, lifetime; data exchange: Protocol, hash, encryption primitives, PFS, lifetime, and extended sequence number.

3 Crypto Library in the Environment

Crypto libraries or modules developed by third party may be used by the TOE. The correctness of the crypto implementation in such third-party components may be exempted from evaluation by defining the component outside of the TOE boundary.

If the TOE developer does not have access to and CM control of the implementation representation of the third-party component, it actually has to be placed outside of the TOE boundary for evaluation at EAL3 and above or when ALC_FLR is claimed.

The crypto functionality used by the TOE shall also in this case be specified according to chapter 2.

The correctness of the crypto implementation put in the TOE environment may be ensured by NIST FIPS 140-2/3 validation, CC certification, or by corresponding developer testing.

It is strongly recommended to use validated or certified crypto libraries.

4 Testing

Regardless of whether the crypto library or module is defined within or outside the TOE boundary, the developer and/or the evaluator shall verify that the crypto requirements specified in the ST are met, i.e., that the crypto functionality is used correctly. This can be done by using a reference implementation. A reference implementation should have a code base that is separate from the crypto implementation used by the TOE. It is also acceptable to use a crypto implementation that has been validated/certified by a trustworthy validation scheme. In this case the implementations do not need to be separate.

All claimed algorithms, key lengths, curves, modes, signature schemes, HMAC variants, cipher suites, etc. used by the TOE and claimed in the ST, are potentially subject for testing. When TOE is using several distinct crypto implementations, each of them should be tested fully. Please note that at lower EALs (EAL1 and EAL2) full coverage may not be required.

5 References

[CCpart1] CCMB-2022-11-001, Common Criteria version CC:2022 revision 1, part 1

[CCpart2] CCMB-2022-11-002, Common Criteria version CC:2022 revision 1, part 2

[CCpart3] CCMB-2022-11-003, Common Criteria version CC:2022 revision 1, part 3

[CCpart4] CCMB-2022-11-004, Common Criteria version CC:2022 revision 1, part 4

[CCpart5] CCMB-2022-11-005, Common Criteria version CC:2022 revision 1, part 5

[CryptoCatalogue] Specification of Functional Requirements for Cryptography, CCDB-018, version 1.0, 2025-01-31, CCDB

[CryptoMechanisms] Agreed Cryptographic Mechanisms, European Cybersecurity Certification Group Sub-group on Cryptography, version 2.0, April 2025, Enisa

[Scheme] Combitech EUCC Certification and Evaluation Scheme, CAB-240701-164858-361, Combitech AB

[EUCC] Commission Implementing Regulation (EU) 2024/482 of 31.1.2024

[EUCCamend] Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation