



EUCC SCHEME

GUIDELINES ON CRYPTOGRAPHY

Agreed Cryptographic Mechanisms

Version 2, May 2025

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
15/05/24	0.1	Creation	Version submitted to the ECCG
06/06/24	0.2	Updates based on the comments made during the ECCG subgroup on cryptography meeting of 06/06/24	Endorsed and approved for publication on 16/07/24 by the ECCG
05/05/25	v2	Addition of PQC mechanisms	Endorsed and approved for publication by the ECCG subgroup on cryptography



LEGAL NOTICE

LEGAL NOTICE

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

This document is established under the responsibility of the European Cybersecurity Certification Group (ECCG) and may be updated whenever needed to reflect the developments and best practices in the field of Agreed Cryptographic Mechanisms.

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

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

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

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025



This publication is licensed under CC-BY-ND 4.0 DEED. Making copies and redistributing this document is permitted. (<https://creativecommons.org/licenses/by-nd/4.0/>)

CONTACT

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



TABLE OF CONTENTS

1. INTRODUCTION	4
1.1 OBJECTIVE	4
1.2 NORMATIVE REFERENCES	4
2. RECOMMENDATIONS ON CRYPTOGRAPHIC MECHANISMS	5



1. INTRODUCTION

1.1 OBJECTIVE

This document supporting the EUCC scheme (the European Cybersecurity Certification Scheme on Common Criteria) provides guidelines regarding the cryptographic mechanisms that should preferably be used in ICT products submitted to certification.

This document is primarily addressed to developers and evaluators.

1.2 NORMATIVE REFERENCES

Regulations

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

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)¹, as amended by Implementing Regulation 2024/3144.

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



2. RECOMMENDATIONS ON CRYPTOGRAPHIC MECHANISMS

When deciding which cryptographic mechanisms should cover their need for cryptographic protection, e.g.: confidentiality, integrity, data origin authentication, and authentication, in their protection profiles and ICT products submitted to EUCC certification, developers of protection profiles and developers of ICT products should consider using the agreed cryptographic mechanisms as defined in ECCG Agreed Cryptographic Mechanisms version 2, further referred to as ACM v2, available at [EUCC Certification Scheme - EU Cybersecurity Certification](#)

When evaluating protection profiles and ICT products under the EUCC scheme, evaluators should verify that these protection profiles and ICT products preferably rely on agreed cryptographic mechanisms as defined in ACM v2 to provide the security services evaluated under this scheme.



ABOUT ENISA

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

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium



enisa.europa.eu

