EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

GUIDELINES ON CRYPTOGRAPHY

Agreed Cryptographic Mechanisms

Version 0.2, June 2024

DOCUMENT HISTORY

Date	Version	Modification	Author's comments
15 May 2024	0.1	Creation	Version submitted to the ECCG subgroup on cryptography
6 June 2024	0.2	Updates based on the comments made during the ECCG subgroup meeting of June 6, 2024	Endorsed and approved for publication on 16/07/2024 by the ECCG

LEGAL NOTICE

This publication is established in accordance with recital 18 of Commission Implementing Regulation (EU) 2024/482**.**

This guidelines document is established and endorsed by the European Cybersecurity Certification Group (ECCG) in accordance with Article 48 (2-3) of Commission Implementing Regulation (EU) 2024/482.

The document shall be updated where developments and best practices in the field of cryptography require to do so. Updates of this document shall be submitted to the ECCG.

This document shall 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

CONTACT

Constructive feedback or questions related to this document are welcome, please use Cybersecurity Certification (europa.eu)

CONTENTS

1 INTRODUCTION

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.

2 NORMATIVE REFERENCES

- 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)[1]
- 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)[2]

3 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 “SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, further referred to as ACM, available at: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf.

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 to provide the security services evaluated under this scheme.

[1] 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) (OJ L 151, 7.6.2019, p. 15).

[2] 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) (OJ L, 2024/482, 7.2.2024),

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu