

**Opinion of the European Cybersecurity Certification Group (ECCG)
on the ENISA EUCC Scheme Guidance on Cryptography**

“Agreed Cryptographic Mechanisms”, version 0.2, June 2024

Adopted via written procedure on 5 July 2024

The Cybersecurity Act¹ in its Article 62(4), point (e), sets the task for the European Cybersecurity Certification Group (ECCG) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes. Moreover, the European Common Criteria-based cybersecurity certification scheme (EUCC Scheme)² in its Article 48(1) and (2) tasks the ECCG with adopting opinions in view of maintaining the EUCC Scheme and to undertake the necessary preparatory works, as well as with adopting opinions endorsing state-of-the-art documents.

ENISA has drafted the EUCC Scheme Guidance on Cryptography “Agreed Cryptographic Mechanisms” (Version 0.2, June 2024). The guidance document supports the EUCC Scheme by providing recommendations regarding the cryptographic mechanisms that should preferably be used in ICT products submitted to certification, in particular in relation to the use of the agreed cryptographic mechanisms as defined in “SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, further referred to as ACM.

The ECCG subgroup on cryptography, composed of representatives of Member States, has been closely involved in developing the guidance, therefore the referred guidance document reflects the opinion of the group. At the 21st ECCG meeting of 15 April 2024, the ECCG took note of the recommendations of the sub-group as included in the “Assessment of ACM possibly becoming a SoA document supporting certification schemes Version 0.3, 25-03-2024”. The conclusion of the subgroup stresses that the ACM could be considered as a possible state-of-the-art document when a suitable derogation mechanism and necessary guidance have been developed and that such elements could be available within one year. In the meantime, the ACM should be used as guidance.

In line with the recommendation of the sub-group, the ECCG herewith endorses the document ENISA EUCC Scheme Guidance on Cryptography “Agreed Cryptographic Mechanisms”, version 0.2, in view of working further on a possible state-of-the-art document on cryptographic mechanisms.

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. 15–69.

² Commission Implementing Regulation (EU) 2024/482 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.