Skadden

Cybersecurity and Data Privacy Update

March 27, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

22 Bishopsgate
London, EC2N 4BQ
44.20.7519.7000

TaunusTurm, Taunustor 1
60310 Frankfurt am Main, Germany
49.69.742200

EU Adopts First of a Series of Voluntary Cybersecurity Certification Schemes

Key Points

On January 31, 2024, the European Commission (EC) adopted the first of a series of initiatives to harmonize cybersecurity certification across the EU: the European Cybersecurity Scheme on Common Criteria (EUCC).

UCC certification is voluntary, it may be vital in demonstrating cybersecurity compliance under other EU laws such as the Network and Information Systems Security Directive (NIS 2), the Digital Operational Resilience Act (DORA) and the Cyber Resilience Act, and may provide commercial advantages.

From January 31, 2025, businesses will be able to apply for EUCC certification of their information and communication technology (ICT) products (*e.g.*, software, hardware and technological components, including chips and smart cards) with a "substantial" or "high" assurance level. Producers of ICT products that are EUCC-certified may affix a mark and label on the products.[1]

As an alternative to product-by-product certification, businesses may apply to certify multiple related ICT products covered by a "protection profile."

With adoption of the EUCC, businesses will want to consider:

- Whether to include EUCC certification as part of their selection process and contractual framework when choosing third-party vendors.
- Whether to apply for EUCC certification of their products, which may be required by some customers and give a market advantage. However, there are reputational and commercial risks of non-compliance with the EUCC framework.

EUCC Background

The EUCC framework for ICT products will be followed by a series of certification schemes covering cloud services,[2] 5G mobile communications and artificial intelligence that are being developed by the EU Agency for Cybersecurity (ENISA), all aimed at harmonizing cybersecurity certification across the EU.

[1] EUCC, Article 11. The mark and label will be accompanied by a QR code with a link to a website containing additional certification information.

[2] See our November 30, 2023 client alert, "Latest Draft of the European Cybersecurity Certification Scheme for Cloud Services – Updates for Non-EU Cloud Service Providers".

EU Adopts First of a Series of Voluntary Cybersecurity Certification Schemes

Importantly, the EUCC provides for mutual recognition agreements with non-EU countries which, when agreed, will acknowledge the adequacy of certain non-EU certified ICT products' cybersecurity when sold in the EU.[3] The U.S., for instance, recently established a voluntary certification process for certain technology products. See our March 21, 2024, client alert "FCC Approves Voluntary Internet-of-Things Cybersecurity Labeling Program").

The EUCC arose from the EU Cybersecurity Act, which called for ENISA to develop an EU-wide cybersecurity certification scheme to regulate ICT products, ultimately for adoption by the EC. The EUCC is part of the EC's broader strategy of ensuring that individuals and businesses benefit from secure digital technologies. This is an area of particular focus for the EC, which is seeking to drive digital transformation while recognizing that the EU relies on foreign countries for over 80% of digital products, services and infrastructure.[4]

The EUCC standards will be familiar to ICT product providers as they are based on the internationally recognized Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) (Common Criteria). The Common Criteria framework has proven popular in Europe over the past 30 years, with businesses in France and Germany at the forefront of Common Criteria certifications. Under the EUCC, ICT product producers will benefit from a one-stop, pan-European certification and can avoid any national specificities.

As part of the EUCC, ENISA has shared annexes, which are supplemented by state-of-the-art documents and guidance on ENISA's website. Further, ENISA has published guidelines on best practices for cyber crisis management, which are primarily aimed at member states.

What Are the Key Considerations for Businesses?

When considering whether to adopt the EUCC for its own ICT products, or require that its vendors adopt the EUCC, businesses should weigh the following factors:

The EUCC covers ICT products and protection profiles. Businesses can apply to certify single ICT products or, alternatively, to certify multiple related ICT products covered by a protection profile, *i.e.*, a set of Common Criteria technical standards or configurations developed for specific technology types, such as smart cards and similar devices[5] and hardware devices with security boxes, each of which are areas of technical focus under the EUCC and are expected to have particular security requirements.[6] In 2022, 74% of Common Criteria certifications were made using a protection profile, particularly for network devices.[7] Approved protection profiles provide businesses with operational certainty and provide the opportunity to maximize the scope of the certification.

Certification requires third-party assessment. Unlike "CE" certification in Europe for safety, health or environmental requirements, the EUCC is not a self-certification process. Instead, products must be evaluated and certified by external assessment bodies. These are laboratories referred to as "Information Technology Security Evaluation Facilities" (ITSEFs) for calibration and testing activities of the ICT product and an accredited certification body for certification and inspection activities.

EUCC certification for an ICT product lasts for up to five years unless prior approval is obtained from the relevant national cybersecurity certification authority. The duration of certification will take into account the characteristics of the certified ICT product.[8] However, a certification of a protection profile may last for a period up to the lifetime of the protection profile concerned, which the EUCC notes will be a minimum of five years. The EUCC encourages the use of protection profiles, as demonstrated by the removal of the requirement for regular recertification.[9]

Certification holders must report any identified vulnerabilities in their certified ICT products. For their EUCC-certified ICT products, businesses must establish and maintain vulnerability management processes and any vulnerabilities identified must be reported to the certification body and/or the relevant national cybersecurity certification authority without undue delay.[10] This report should contain all elements necessary to understand the impact of the vulnerability on the ICT product, possible risks associated with the proximity or availability of an attack, whether the vulnerability can be remedied and, where it can, the possible resolutions. If the vulnerability cannot be remedied, this could potentially lead to the suspension, or even withdrawal, of the EUCC certificate. Sanctions for the violation of the

[3] EUCC, Article 44.

[4] European Commission, 2023 Report on the State of the Digital Decade.

[5] For example, smart card hardware, integrated circuits, smart card composite products, trusted platform modules as used in trusted computing, or digital tachograph cards.

[6] For example, payment terminals, tachograph vehicle units, smart meters, access control terminals and hardware security modules.

[7] jtsec, 2022 Common Criteria Statistic Report.

[8] EUCC, Article 12(1).

[9] EUCC, Recital 7.

[10] EUCC, Article 35.

EU Adopts First of a Series of Voluntary Cybersecurity Certification Schemes

obligation to report vulnerabilities are laid down in EU member state law.[11]

There are both reputational and commercial risks to non-compliance. The EU's Cybersecurity Act allows each EU member state to set the rules on penalties applicable to infringements of European cybersecurity certification schemes, including the EUCC. Additionally, in case of non-compliance, EUCC allows for the suspension (for up to 42 days and, in justified cases, up to one year), or even withdrawal, of the EUCC certificate. This may cause reputational or commercial harm to the ICT product producer:

- *Suspension or withdrawal:* The national cybersecurity certification authority will inform ENISA, which will publish the updated status of the EUCC certificate and the business must immediately stop any promotion of the ICT product as being EUCC certified.
- *Suspension:* The business must inform any purchasers of the ICT product about the suspension, including any reasons provided by the certification body that are not sensitive and would not constitute a security risk. This information must also be made publicly available by the business.
- *Withdrawal:* The business must disclose and register any publicly known and remediated vulnerability on the European vulnerability database, hosted by ENISA.

[11] EU Cybersecurity Act, Article 65. In Germany, for example, the national cybersecurity certification authority can impose an administrative fine of up to €500,000 in case of the infringement by a EUCC certificate holder of its obligation to report detected vulnerabilities or irregularities concerning the security of the EUCC-certified ICT product (Sec. 14 (4) No. 2 of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*)).

The EUCC contemplates mutual recognition agreements. As mentioned, the EU is open to recognizing non-EU cybersecurity certification schemes that are equivalent to the requirements of the EUCC under mutual recognition agreements. These may include other countries, *e.g.*, the UK's Cyber Essentials, whose cybersecurity schemes are influenced by international standards.

EUCC certification: mandatory or voluntary? Although EUCC certification is voluntary, recent and incoming European legislation makes the EUCC a pivotal business tool to evidence future cybersecurity compliance in Europe for DORA[12] and the Cyber Resilience Act.[13]

Moreover, use of EUCC-certified ICT products may be mandatory for regulated businesses falling within the scope of the NIS 2.[14] Under NIS 2, EU member states may require essential and important entities to use only EUCC-certified ICT products.

Customers may insist on EUCC compliance. Additionally, individual and business customers are increasingly requiring that their vendors implement good industry cybersecurity practices, and avoidable cyber incidents can damage vendors' reputations and result in huge amounts in compensation and resultant litigation, in addition to the internal cost of the cyber incident itself.

[12] Under DORA, which goes into effect on January 17, 2025, European supervisory authorities examining critical third-party ICT providers will consider their certifications.

[13] The Cyber Resilience Act was approved by the European Parliament on 12 March 2024 and is now subject to formal approval by the Council.

[14] The Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, set a deadline of October 2024 for implementation of its terms by member states.

Contacts

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Kata Éles
Associate / Frankfurt
49.69.74220.143
kata.eles@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Jonathan Stephenson
Associate / London
44.20.7519.7038
jonathan.stephenson@skadden.com

Trainee solicitor **Imad Mohammed Nazar** contributed to this article.