The Cybersecurity Act: a complement to eIDAS

Introduction

The eIDAS Regulation is the first European regulation that addresses cybersecurity topics from a solution angle. It lays down the conditions for the development of two key solutions, electronic identification (eID) and Trust Services (TS), for the benefit of the Digital Single Market. eIDAS provides legal certainty for the European market and establishes concrete cybersecurity measures for national electronic identification schemes, electronic signatures, electronic seals, time stamping, electronic delivery service and website authentication.

Nowadays, an ever-increasing number of trust solutions are being developed. They all answer different needs depending on the intended use. It is of utmost importance to certify the means of identification and authentication at the adequate security level to increase online trust. However, such diversity creates a risk of market fragmentation as no common European certification scheme applies.

Eurosmart calls on the European Commission to complement the eIDAS Regulation with common cybersecurity certification schemes (high, substantial, basic) as established by the Cybersecurity Act. Such an alignment between the eIDAS Regulation and the Cybersecurity Act would solve the issue of fragmentation, hence simplifying certification for companies.

eIDAS compatibility with the Cybersecurity Act: the case of QSCD

Article 30 of the eIDAS Regulation lays down certification requirements for Qualified Signature Creation Devices (QSCD). The Commission Implementing Decision 2016/650 complements these technical requirements with references to the protection profiles for signature creation device (PP SSCD EN 419 211). Such protection profiles were developed by CEN in the context of the standardisation mandate M/460 given by the European Commission. These protection profiles rely on the evaluation methodology defined by ISO IEC 15408 standards, commonly known as Common Criteria.

In the framework of the Cybersecurity Act, a first certification scheme on Common Criteria is currently being developed by ENISA. This first scheme will rely on ISO IEC 15408 standards. Therefore, eIDAS is the first regulation to be fully in line with the Cybersecurity Act when it comes to the security assessment of QSDC.

In addition, a protection profile for QSDC for Server Signing (SAM PP EN 419 241-2) has been validated and developed by CEN, and fully adopted as European Norm. This standardisation activity has been performed under mandate M/460. This protection profile will also be fully compliant with the first cybersecurity scheme.

Therefore, the European cybersecurity certification scheme on Common Criteria is fully suitable to certify QSCD. This scheme should be referenced in eIDAS secondary legislation.

Aligning assurance levels between the Cybersecurity Act and eIDAS

A link should be created between, on the one hand, the eIDAS levels of assurance (LoA) for identification and authentications and, on the other hand, the three security levels of the Cybersecurity Act. This is the only way to counter market fragmentation and to ensure that the appropriate level of trust is reached.

Eurosmart believes that the formal link should follow this approach:

eIDAS LoA	Cybersecurity Act LoA
High (protected against attackers with high attack potential)	High (penetration testing)
Substantial	Substantial (conformity)
Basic	Basic (self-certification)

The [Commission Implementing Decision 2015/1502](#) lays down technical specifications and procedures for assurance levels low, substantial and high for electronic identification means. For assurance level "high", "[t]he electronic identification means protects against duplication and tampering as well as against attackers with high attack potential". This approach is in line with the level of assurance "high" pursuant to the Cybersecurity Act, where penetration testing is mandatory.

Moreover, eIDAS refers to data protection which constitutes an essential building block of cybersecurity as well. Therefore, eIDAS data protection aspects could be covered by the Cybersecurity Act.

Final note

The Cybersecurity Act was adopted five years after the eIDAS Regulation. As previously demonstrated, the Cybersecurity Act is well-suited for assessing eIDs and trust services by providing existing Protection Profile for local and server based QSCD.

However, it is important to underline that the scope of the Cybersecurity Act is much broader than the scope of eIDAS. eIDAS addresses electronic identification, electronic authentication and trust services for electronic transaction in the European single market. This mainly relates to persons (LOA & QCSD), companies (Seal) and Trusted web services. The Cybersecurity Act covers a broader range of actors such as machines, objects, IOT, suppliers, and even cloud software.

For example, IOT can be considered a key challenge in terms of electronic identification and may have an IoT- **u**nique **id**entity (UID). Electronic identification Platforms are in use in the IoT market and are fragmented, like GS1 with the **E**lectronic **A**rticle **N**umber (EAN) for objects and **L**egal **E**ntity **I**dentifier (LEI) for the financial services. Other technologies are well known, like **B**lock**c**hain (BC), **D**istributed **L**eger **T**echnology (DLT), **S**elf-**S**overeign **I**dentity (SSI), company register and **P**ublic **K**ey **I**nfrastructure (PKI)-infrastructure. Some connected devices have their own unique identity number systems in place, like **I**nternet **P**rotocol (IP)-address in laptops, **I**nternational **M**obile **E**quipment **I**dentity (IMEI) number in smart phones and **U**nique **D**evices **I**dentification (UDI) in medical products. Therefore, the scope of the Cybersecurity Act fully covers eIDAS requirements and much more…

EUROSMART
The Voice of the Digital Security Industry

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei, IDEMIA, IN GROUPE, Infineon Technologies, Inside Secure**, **Linxens**, **Nedcard, NXP Semiconductors, +ID, PayCert, Prove & Run, Qualcomm, Real Casa de la Moneda**, **Samsung, Sanoïa, Sarapis, SGS, STMicroelectronics, Thales, Tiempo Secure, Toshiba, Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com   @Eurosmart_EU   @Eurosmart