EUROSMART
The Voice of the Digital Security Industry

European Digital Identity Wallet: Why do we need level "high" (eIDAS) & level "high" (Cybersecurity Act)?

The discussion around assurance level "high" is rightfully confusing for many following the revision of the eIDAS Regulation. What is meant by assurance level "high"? Does it mean resistance to skilled attackers, so a high level of cybersecurity for a given product? Does it mean that an electronic identification means needs to be entirely trustworthy, including the process of issuing identity credentials? Does it mean both?

In this paper, Eurosmart would like to take on the ambitious task of bringing clarity to the debate. The needed starting point is to understand that there are two meanings of assurance levels "high":

- assurance level "high" in the meaning of the eIDAS Regulation
- assurance level "high" in the meaning of the Cybersecurity Act (CSA)

In the first section, Eurosmart explains the difference between the two concepts (eIDAS assurance level "high" and CSA assurance level "high") as well as how they overlap. In a second section, Eurosmart presents why the new eIDAS 2 regulation needs to rely on both assurance levels "high".

Section 1: eIDAS assurance level "high" and CSA assurance level "high": What is what?

Two distinct concepts stemming from two distinct legislations

eIDAS assurance levels

The digital identity community often calls the eIDAS levels of assurance " LoA ". These eIDAS assurance levels refer to Article 8 of the eIDAS Regulation[1]. This article defines assurance levels for electronic identification means. The purpose here is to see where a national electronic identification means stands in terms of trustworthiness. Such a common EU reference is essential as these means must be recognised and trustable cross-border.

Article 8(2)c of the eIDAS Regulation defines level of assurance “high” as follows:

> *Assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to* ***prevent misuse or alteration of the identity****.*

Member States shall take several criteria into account to assess the trustworthiness of their electronic identification means or those of other Member States. Commission Implementing Regulation 2015/1502[2] describes these criteria. For each of these criteria, this legal act lays down a series of requirements to fulfil in order to comply with a specific level ("low", "substantial", or "high"). The higher the level, the stricter the requirements.

Eurosmart identified two types of requirements:

- Requirements that relate to procedures (e.g., procedure to enrol the applicant, procedures to revoke and renew the electronic identification means) and do not directly relate to the electronic identification means. Those represent the majority of requirements to reach a specific eIDAS assurance level.
- Requirements that directly relate to the electronic identification means, in particular requirements on how the electronic identification means is managed and authentication. For instance, for level "high", the electronic identification means shall protect against duplication and tampering as well as against attackers with high attack potential. Special security measures shall also be in place for the authentication mechanism.

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN

[2] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

Any potential overlap with the CSA can only concern this second category of requirements.

Since the adoption of eIDAS 1, Member States have been notifying their electronic identification means, each time specifying their assurance level. A Member State typically pre-notify an electronic identity card (equipped with a chip) at an assurance level "high". Following pre-notification, other Member States verify whether the claimed assurance level is fulfilled. This is the peer review process.

CSA assurance level high

Article 52 of the CSA Regulation[3] defines its own assurance levels, a distinct concept from the eIDAS levels. The CSA assurance level applies to European cybersecurity certification at large. The CSA assurance level indicates the confidence one can have in a product fulfilling pre-determined security requirements and the level at which this product was evaluated.

Article 52 defines level "high" as follows:

> *A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state-of-the-art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.*

In addition, Article 52 item 1 clarifies the scope of assurance level:

> *A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process in terms of the probability and impact of an incident.*

In other words, each certification scheme will specify the assurance level associated with level 'high' for a specific domain or category of products certified through that scheme. For example, EUCC maps EU CSA "substantial" to Common Criteria assurance levels AVA_VAN.1 and AVA_VAN.2 and maps EU CSA "high" to Common Criteria assurance levels AVA_VAN.3 to AVA_VAN.5.

Is there a bridge between both concepts?

In a short and simplified manner, the CSA assurance level belongs to the cybersecurity world. A manufacturer wants to demonstrate that a product complies with pre-defined cybersecurity requirements; this is when the European cybersecurity certification and the CSA assurance level come into play.

The eIDAS assurance level belongs to the digital identity world. A Member State wants to notify an electronic notification means and needs to indicate the strength of the identity proofing, authentication mechanism etc. This is when the eIDAS assurance level comes into play.

---

[3] 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): https://eur-lex.europa.eu/eli/reg/2019/881/oj

However, looking at the requirements to fulfil the eIDAS level "high", one notices a clear overlap with the CSA. First, Article 8 of the eIDAS Regulation states that the technical specifications, standards, and procedures related to the electronic identification means shall "prevent misuse or alteration of the identity". Such a legal requirement entails the implementation of cybersecurity measures to avoid theft and misuse of (identity) data.

- Secondly, the electronic identification means must resist "attackers with high attack potential" (Implementing Regulation 2015/1502). This concept of resistance against attackers with high attack potential provides for the highest level of security as it ensures resistance to the most skilled attackers. Naturally, such a level of evaluation of electronic identification means requires very skilled and equipped laboratories. In order to be meaningful and recognised by other parties, the security evaluation of electronic identification means at that level shall be organised within a mutual recognition agreement. Each party shall (1) share the same understanding of what is meant by "attackers with high attack potential" and (2) trust the capacities and skills of the laboratory in charge of carrying out such an evaluation. These requirements orientate naturally towards the CSA definition of assurance level "high" as it provides for a mutual recognition between parties at the highest level of security through peer reviews;
- the level of security evaluation required for the electronic identification means implies that it shall resist to "skilled attackers, using penetration testing" which is a key criteria defining the level of certification "high";

However, the electronic identification means shall resist to "attackers with high attack potential", which may go a step beyond the CSA definition of assurance level "high". For instance, in the case of the EUCC scheme[4], a certification pursuant to CSA level 'high" is mapped to a vulnerability assessment assurance starting from AVA_VAN.3 as defined by the Common Criteria methodology for security evaluation, while the one for electronic identification means shall be AVA_VAN.5.

Therefore, very logically, one can deduce that if an electronic identification means is certified at CSA assurance level "high" to demonstrate its resistance to "attackers with high attack potential", it complies with one of the requirements for the eIDAS level "high" (cybersecurity requirement). Eurosmart would even argue that this is the most effective way of complying with the eIDAS requirement of cybersecurity. To give a concrete example, if the chip of an electronic identity card is certified level "high" (CSA) using the EUCC scheme with a level of vulnerability assessment of AVA_VAN.5, then it already demonstrates that it can resist "attackers with high attack potential". Therefore, it fulfils one of the eIDAS level "high" requirements.

However, arguably, a CSA certificate level "high" also ensuring resistance to "attackers with high attack potential" is not sufficient to demonstrate that an electronic identification means complies with all the eIDAS requirements for level "high". Implementing Regulation 2015/1502 mentions other requirements, including the way enrolment was performed (identity proofing etc.). Resistance against "attackers with high attack potential" is only one requirement among others that an electronic identification means must fulfil to comply with eIDAS level "high"

[4] The EUCC scheme is the first European cybersecurity certification scheme, prepared in the context of the CSA. It is based on the Common Criteria methodology for security evaluation.

Section 2: eIDAS 2 needs eIDAS assurance level "high" and CSA assurance level "high"

On-boarding onto the Wallet with the eIDAS assurance level "high"

With eIDAS 2, every Member State will provide a European Digital Identity Wallet to its citizens. Users should be able to use it cross-border to identify and authenticate themselves and present attestations of attributes. There is currently an ongoing discussion around the eIDAS assurance level that the Wallet should meet.

Eurosmart believes that the Wallet should fulfil the requirements of the eIDAS assurance level "high" for the enrolment and on-boarding process[5]. ALL the criteria of the level of assurance relating to enrolment and on-boarding (identity proofing and verification, eID means management and authentication etc.) SHALL be carried out in accordance with the level of assurance "high" so that the Wallet could be used for identification and authentication at a level of assurance "substantial" or "high". If on-boarding at the level of assurance "substantial" is allowed, it will lead to the situation where there would be two types of Wallets on the field:

- Wallet where on-boarding was carried out pursuant to the level of assurance "substantial", and that could be used only up to the level of assurance "substantial"
- Wallet where on-boarding was carried out pursuant to the level of assurance "high", and that could be used up to the level of assurance "high" (including "substantial")

To avoid fragmentation, Eurosmart favours a level of assurance “high” for the on-boarding of the European Digital Identity Wallet. Users can use it for a wide range of use cases -requiring level of assurance “high” or “substantial”. Allowing level of assurance “substantial” for enrolment and on-boarding would hinder large-scale interoperability and impede Wallet uptake in Europe.

From a technical standpoint, Eurosmart strongly believes that meeting the eIDAS level "high" requires relying on the secure element of the smartphone or the user's identity card. Secure elements provide the safest place for cryptographic keys.

[5] Enrolment consists in verifying and confirming the identity of someone and creating and populating the corresponding record with all the necessary information. Once enrolled, the application is ready to be processed by the issuing authority so that digital identity credentials could be issued to that person (adjudication). Identity proofing is part of enrolment and only provides confidence in the link between a claimed identity and an applicant. Digital identity credentials are issued to a citizen by national authorities. However, enrolment does not give any guarantee on the device that will be used to store the credentials. How to ensure that the issued credentials will be stored and used in a device that belongs to the legitimate holder? The on-boarding encompasses the enrolment but also addresses the measures to guarantee that the issued credentials are transferred and stored in a device and Wallet compliant with the issuing authority requirements (technical, security etc.) and under the sole control of the rightful holder. For instance, it may take the shape of a link sent to the user through a SMS where the user would be prompted to enter a code, to ensure that the device belongs to the legitimate holder of the credentials.

Cybersecurity certification of the Wallet with an assurance level "high"

The Wallet should be very resistant to cyber-attacks. The first reason for this is that it will contain very valuable and sensitive data, namely cryptographic keys, person identification data and all kinds of attributes that represent a person in society. Identity theft is here the main risk, as well as all the problems that this could entail in terms of privacy violation.

Another reason, a legal one, calls for this high level of resistance to cyber-attacks. Suppose the Wallet must comply with the eIDAS assurance level "high" for enrolment and on-boarding. In that case, that also means it must fulfil the requirement of resistance against "attackers with high attack potential".

As explained above, the best way to comply with such requirement is to carry out a cybersecurity certification of the Wallet pursuant to the CSA with a level of assurance “high” which also demonstrates resistance against "attackers with high attack potential". The technical requirements to assess the resistance of a product to "attackers with high attack potential" within a CSA certification scheme at level “high” is defined by the security certification scheme itself. For example, when using EUCC scheme, the Wallet shall be security certified with a level of vulnerability assessment of AVA_VAN.5 pursuant to the Common Criteria, to ensure its resistance to "attackers with high attack potential".

Thus, Eurosmart calls for mandatory certification of the European Digital Identity Wallet (1) pursuant to a CSA cybersecurity certification scheme level "high" and (2) demonstrating its resistance to "attackers with high attack potential" or, if such a scheme is unavailable, using a national scheme that provides an equivalent security level. In particular, when using EUCC scheme, the Wallet shall be security certified with a level of vulnerability assessment of AVA_VAN.5 pursuant to the Common Criteria, to ensure its resistance to "attackers with high attack potential.

The importance of technical standards for eIDAS assurance level “high”

In the previous paragraphs, the link between eIDAS assurance level « high » and CSA assurance level « high » was clarified. In particular, it appears that the demonstration of compliancy of electronic identification means - including the Wallet - with the requirements of eIDAS assurance level « high » could leverage cybersecurity certification at assurance level « high » under the CSA.

A harmonised security approach is beneficial for product development, evaluation and certification. It brings clear risk management to the issuer and demonstrable trust to the final user that the product is secure and protects its data.

The harmonised security approach shall include a threat analysis of the Wallet that covers the whole system: the secure components that stores the sensitive information, the device (s) and the operating environment.

The harmonised security approach shall rely on dedicated « security profiles » to address the specific security features of each component of the system. For the component that protects the key security features of an electronic identification means (cryptography, random number, firewall…), Eurosmart recommends using the above listed Protection Profiles (PPs) to demonstrate conformity of electronic identification means with the level of assurance “high” pursuant to eIDAS. These already existing PPs have indeed brought security harmonization towards level high and represent a proven track:

- Security IC Platform Protection Profile - BSI-CC-PP 0035
  https://www.commoncriteriaportal.org/files/ppfiles/pp0035a.pdf

- Security IC Platform Protection Profile with Augmentation Packages - BSI-CC-PP-0084 https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf
- Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile - BSI-CC-PP-0117 https://www.commoncriteriaportal.org/files/ppfiles/pp0117a_pdf.pdf

Besides, as the wallet shall also allow the user to create qualified signature, the corresponding protection profiles for Secure Signature creation Device should also be considered:

- PP for a Secure Signature Creation Device - Part 2: Device with Key Generation https://www.sogis.eu/documents/cc/pp/sc/sscd/pp0059_ma2b.pdf
- PP for a Secure Signature Creation Device - Part 3: Device with key import https://www.sogis.eu/documents/cc/pp/sc/sscd/pp0075_ma1b.pdf
- PP for a Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication with certificate generation application https://www.sogis.eu/documents/cc/pp/sc/sscd/pp0071_ma1b.pdf
- PP for a Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted communication with signature creation application https://www.sogis.eu/documents/cc/pp/sc/sscd/pp0072_ma1b.pdf
- PP for a Secure Signature Creation Device - Part 6: Extension for device with key import and trusted communication with signature creation application https://www.sogis.eu/documents/cc/pp/sc/sscd/pp0076_ma1b.pdf

About Eurosmart

Eurosmart, the Voice of the Digital Security Industry, is a **European 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 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 is a 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, ETSI, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com