GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

The EU Cybersecurity Certification Scheme

White Paper

Mapping misalignment with industry security levels and understanding the impact

September 2022

Table of Contents

ABOUT US

GlobalPlatform is a technical standards organization that enables the efficient launch and management of innovative, secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity, and convenience to users. It achieves this by providing standardized technologies and certifications that empower technology and service providers to develop, certify, deploy, and manage digital services and devices in line with their business, security, regulatory, and data protection needs. Key offerings include secure component specifications; the Device Trust Architecture for accessing secure services within a device; the IoTopia Framework for secure launch and management of connected devices; and the SESIP Methodology for IoT device certification.

GlobalPlatform technologies are used in billions of smart cards, smartphones, wearables, and other connected and IoT devices to enable convenient and trusted digital services across market sectors, including healthcare, government and enterprise ID, payments, smart cities, industrial automation, smart home, telecoms, transportation, utilities, and OEMs.

GlobalPlatform standardized technologies and certifications are developed through effective industry-driven collaboration, led by multiple diverse member companies working in partnership with industry and regulatory bodies and other interested parties from around the world.

SECTION 1: THE STATE OF PLAY – USE CASES, RISKS & REQUIREMENTS

Our lives rely heavily on smart connected devices: we now use them to manage our professional, private, financial, and other affairs. While this personal technology offers obvious benefits, these devices store huge amounts of code and data susceptible to attacks by hackers and other bad actors. What's more, the sheer number of applications available for download represent an even larger opportunity for fraudsters, and the sophistication of threats is also evolving at a staggering pace.

Meanwhile, our offices, factories, cities, cars, and other environments are also becoming increasingly connected; providing more capabilities than their original core functionality. Additionally, users interact with these devices and environments in new ways. From organizing a trip from one's TV to automating a factory infrastructure, these expanded practices create new security vulnerabilities. This, in turn, emphasizes the need for technology that increases the security of devices and applications, ways to validate that security, and clear frameworks to help industry stakeholders and end-users to understand the security capabilities of their devices.

Different use cases demand differing approaches to cybersecurity

This increased need for security is driven by the evolving characteristics of these smart connected devices and their ever-broadening use cases. A few such features, and their related security concerns, include:

- **Identity and Authentication**: The traditional method of authenticating a user involves requesting a username and password. However, security experts increasingly deem this method inadequate due to weak or reused passwords that provide hackers with relatively easy access to accounts. Moreover, because application or service providers often maintain stores of personally identifiable and sensitive information on their servers, such hacks make headlines, upset consumers, and undermine business confidence. Accordingly, there is a need for improved authentication mechanisms that protect consumers while still allowing application developers flexibility.

  On top of this, different types of identification documents, like ID cards, ePassports, and health insurance cards, store increasing amounts of personal information, including credentials, passwords, medical data, etc. To prevent exposure of this information in the event of loss, theft, malware, or another adverse event, sufficient security is needed to store, process, and distribute such personal data.

  Consider one example of an organization that is working to improve authentication: Fast Identity Online (FIDO), which aims to "move beyond passwords" and proposes a "password-less" authentication experience for devices that have been certified according to its specifications. More simply, FIDO authentication becomes a two-stage process wherein the user first authenticates themselves to the device (perhaps using a biometric or trusted user interface), followed next by an authentication scheme between the device and the relying parties. This process uses a public key on the server and a private key on the device. For maximum effectiveness, FIDO's key material and cryptographic algorithms will need to be protected from attack. It should be noted that, with FIDO and other organizations seeking to address authentication concerns, a mechanism is required to offer certifiable security for trusted providers while preventing hackers from gaining access.

- **Financial Risks**: The use of connected, mobile devices to conduct financial transactions has become commonplace. These transactions already include ticketing, remote payment, proximity payment, and financial e-transactions. The use of mobile devices to make purchases at retail locations is growing rapidly. Furthermore, there are an increasing number of use cases where the mobile device becomes the point of sale (POS) terminal, particularly for highly mobile points of sale. These devices require substantial to high security to resist attacks and breed consumer confidence.

  Financial risk can also extend beyond the loss of money, to the loss of physical items. Financial implications would be considerable if a car can be stolen using a compromised digital key or house broken into through a compromised smart lock.

- **Corporate Data Access and Industrial Automation**: Enterprise company IT professionals are often wary of enabling access to their internal networks, fearing that the endpoint devices could carry malware, be stolen, or create attacks from within the internal network when used outside of company premises. To protect against these possibilities, IT departments frequently establish green-lists and red-lists of devices based on their security capabilities. Additionally, the always-on nature of these devices and the enforcement of password protection and device locking when not actively in use further concern IT security professionals.

  In industrial automation, we are seeing previously closed factory networks being connected, for example, and new connected machinery installed. This increases the security requirements of both the networks and the devices installed in the connected environment.

- **Child-Specific Devices**: Very few regulations exist currently related to child-specific devices. Even so, privacy is paramount for both the protection of minors and for parents' peace of mind. Security certification offers a minimum level of assurance to parents that devices used to monitor, entertain, or educate children are not easily susceptible to attack by bad actors.

  EU initiatives are progressing to address child-specific devices, like the Radio Equipment Directive (RED), improving device security but studying the targeted levels of assurance.

- **Telecommunications Capabilities**: As more and more devices and 'things' are connected, a broader spectrum of devices need an agreed baseline of security and enhanced security features based on the capabilities of the specific device or thing. Initiatives like the RED, EU 5G, and other schemes in Europe are offering a basis for device requirements, like technical features for the protection of privacy and personal data and against fraud. Additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software. All of these rely on access to clear security levels.

Each of these factors and sets of use cases present security concerns that must be addressed for the technology to function appropriately and securely in the markets they serve. This white paper explores the current industry approach to platform and component security, and the device and application security these assurances enable, as well as the security levels and certification programs already widely adopted in the global technology industry. The paper will then map this existing work against the approach outlined in the European Union’s Cybersecurity Act (CSA) and the correlating Cybersecurity Certification Scheme developed by the European Union Agency for Cybersecurity (ENISA) in line with the requirements set out in EU CSA. Finally, it will explore the need for greater alignment between the current cybersecurity certification frameworks in play and ENISA’s new scheme, and the almost-certain challenges that misalignment will bring.

SECTION 2: ADDRESSING THE CYBERSECURITY NEEDS OF THE GLOBAL TECHNOLOGY MARKET

The rapid evolution of technology and connectivity has created, and is creating, numerous challenges for the cybersecurity industry, including:

- Growth in the number and types of devices.
- Increasing connectivity of devices, both to networks and each other.
- Expanding utility of devices and services.
- Demand for security solutions that support different business models and risk profiles.
- Increasing sensitivity of data captured, stored, processed, and communicated via connected devices.
- The need to control or reduce the connectivity of devices and what they do when connected.
- Expanding fragmentation of cybersecurity and privacy regulations and requirements.
- The need to demonstrate the security and privacy features of components and devices.
- The need to protect intellectual property and brands.
- A desire to foster confidence in the IoT.

To address these challenges, the industry has collaborated through industry bodies and forums on a number of initiatives, including:

- Working to map and define the threat landscape that devices and services needed to be protected against.
- Orienting around a common approach to security levels which meet the needs of different implementations, vertical markets, and business models.
- Standardizing security technologies and techniques which align with these security levels and market requirements.
- Establishing certification and labeling programs for vendors to demonstrate the security and robustness of their products.
- Fostering close collaboration and alignment between industry bodies on standardization initiatives and certification programs.
- Optimizing the certification process to bring about time and cost efficiencies by ensuring mutual recognition of certificates across different countries, regions and industries.

Today, several certification and labeling schemes and initiatives have emerged from the security and vertical industries in response to these challenges. Each scheme has its own scope and value both to the greater ecosystem and to their respective stakeholders. Collaboration between organizations, both within and across industries, has resulted in broad alignment around security standards and robustness levels. Though terminology differs slightly from one organization to the next, generally speaking, each framework or standard characterizes security robustness levels as high, enhanced/substantial, and basic – and the robustness of each level translates from one body to the next.

Different industries have different approaches to security standards and schemes depending on the requirements of the market, their business models and requirements for appropriate security. For example, payment and identity cards require Secure Elements (SEs) that demonstrate high levels of security robustness. Smartphones can largely rely on enhanced levels of security as the capabilities of the device enable additional layered security measures to be in place. As a final example, while privacy is key for a simple children's device, it does not require gold-standard security. The following horizontal and vertical security initiatives map to these high, enhanced, and basic security levels:

2.1 THE HORIZONTAL APPROACH TO SECURITY

GlobalPlatform's Security Certification program verifies that secure components meet the assurance levels outlined in Common Criteria-recognized protection profiles through independent security evaluation. It ensures that secure components meet the required levels of security defined for a particular service, enabling service providers to confidently and effectively manage risk and comply with industry requirements. To assist the market in managing varying security requirements, GlobalPlatform has structured the program under three security levels. Each level denotes the ranked levels of threats and attacks that the security certified secure component will defend against. They are:

- High (Secure Element products)
- Enhanced (Trusted Execution Environment products)
- Basic

This simple framework allows future technologies and solutions to be added under these levels. In addition, device manufacturers can select the most appropriate accredited component for meeting their particular requirements, while allowing service providers to mandate a particular level of security to protect their digital services on devices.

The **Security Evaluation Standard for IoT Platforms (SESIP)** methodology supports IoT device makers and certification bodies as they establish their own IoT device security certification schemes. The SESIP methodology provides a common and optimized approach for evaluating the security of connected products that meets the specific compliance, security, privacy, and scalability challenges of the evolving IoT ecosystem. A feature of the methodology includes reusability of certification that can extend to new devices and implementations.

The **PSA Certified** scheme takes a layered approach to IoT security and offers certifications for all components of a connected device, ensuring that each element has built-in security. Certifications are consumable so that device manufacturers can leverage expertise from the value chain and build on certified silicon and software. PSA Certified status can also be reused with other security frameworks and evaluation schemes. For example, device manufacturers can reuse their certificates to show mappings to regulations and silicon vendors can use their certificates to demonstrate they have a secure Root of Trust suitable for other certification schemes.

PSA Certified currently provides three levels of silicon security assurance to ensure 'right size' security can be built into products. PSA Certified Level 1 is available for silicon, system software, and endpoint device manufacturers, while PSA Certified Level 2 and PSA Certified Level 3 evaluate the silicon Root of Trust.

Synergy between PSA Certified & SESIP

PSA Certified supports the use of the SESIP methodology by publishing SESIP profiles for PSA Certified Level 2 and at PSA Certified Level 3.

PSA Certified also enables chip vendors to use composition by allowing their trusted subsystems to be certified using SESIP and the PSA Certified RoT Component flow.

This 'better together' proposition is the market recognition of PSA Certified together with the opportunity to use composition via SESIP. Chip vendors can do one evaluation and achieve two certificates.

Eurosmart has launched a pilot project: the *Eurosmart IoT device certification scheme* at the level "substantial" (eIoT SCS), designed to be fully compliant with the European Cybersecurity Certification Framework. This framework, as defined by the European Cybersecurity Act, enables their users to ascertain the level of security assurance (basic, substantial, and high), and ensures that these security features are independently verified. Eurosmart has been developing its own certification scheme for IoT devices with a focus on the substantial security assurance level, based on this regulation.

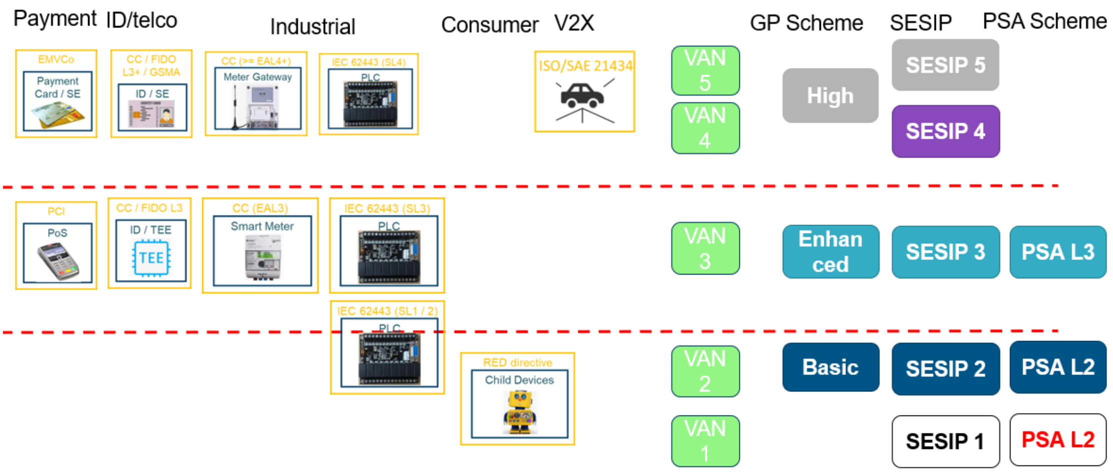

Figure 1: Mapping use cases with industry security levels. The vertical and use case approach to security.

EMVCo is working to make the global payments infrastructure more secure by issuing specifications and technologies for payment cards and the devices used for storing, processing, and transmitting payment cardholder data. These standards apply not only to merchants and payment processors, but also to the software developers and manufacturers of applications and devices used in those transactions. The technologies and specifications apply to a number of payment methods which have different security and assurance requirements, including contact, contactless, mobile, tokenization, QR codes, secure remote commerce, and EMV 3-D secure.

The **FIDO Alliance** is an open industry association that seeks to create authentication standards to help create more secure authentication than passwords provide. FIDO promotes the development of, use of, and compliance with standards for authentication and device attestation and seeks to fulfill this mission by: “operating industry certification programs to help ensure successful worldwide adoption of the specifications” and “submitting mature technical specification(s) to recognized standards development organization(s) for formal standardization.” FIDO’s certified authenticator levels, for example, rely on the presence of hardware and security software measures present in devices.

In the telecommunications sector, **GSMA** participates in setting standards by following process AA.35 which requires the organization to “establish structural, procedural, and reporting mechanisms that are specifically created to serve the creation of and maintenance of multi-stakeholder Industry Specifications.” Initiatives like the Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and GSMA, provide an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP defined security test cases for the security evaluation of network equipment.

The **Trusted Connectivity Alliance (TCA)** seeks to foster trust in a connected future by acting as leaders within the Tamper Resistant Element (TRE) ecosystem and working to advance and advocate the trust and security credentials of TREs, standardize and enhance the TRE ecosystem to support the evolution of cellular connectivity (e.g. 5G and IoT), and promote innovation and growth opportunities the TRE offers across markets where security is paramount, such as connected cars, wearables, smart utilities, industry 4.0, and healthcare. To accomplish this mission, TCA works with industry partners outlined above, including Eurosmart, GlobalPlatform, and GSMA to support the continued standardization of the TRE ecosystem alongside other technical industry associations and standards bodies.

Finally, The **Trusted Computing Group (TCG)** works to maintain the integrity and sustainability of the global ICT infrastructure by promoting the open, interoperable, and internationally vetted security standards that are critical for the success of trusted computing. The organization believes a multilateral approach to creating these standards is most effective and works within the international standards community, fostering working group relationships with the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC). The organization’s Trusted Platform Module is defined by an ISO/IEC international standard and The TCG Certification Program leverages established and recognized security evaluation standards, including certification by laboratories operating under the supervision of National Schemes of Common Criteria members.

--

Each of these organizations serves different objectives, stakeholders, technologies and end-users. The commonality of the industry approach to cybersecurity – whether it be horizontal or vertical – is the coalescence around a structured set of aligned security levels; basic, substantial, and high.

SECTION 3: EUROPE'S RESPONSE: EU CYBERSECURITY ACT & EU CYBERSECURITY CERTIFICATION SCHEME (EUCC)

In response to the growing threat landscape, on March 12, 2019, the Members of the European Parliament adopted the Cybersecurity Act (CSA) as "the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g., Internet of Things) and services." The Cybersecurity Act also seeks to further strengthen the EU Agency for Cybersecurity (ENISA) and grants the agency a permanent mandate to develop and maintain the framework for cybersecurity certification themes.

ENISA recognizes that certification plays a crucial role in increasing trust and security in important products and services for the digital world, and as discussed above, that several different security certification schemes for ICT products currently exist in the EU. Yet, without a common framework for EU-wide valid cybersecurity certificates, there is an increasing risk of fragmentation and barriers between Member States. Therefore, under the new EU-wide cybersecurity certification for ICT products, processes, and services created by CSA, companies doing business in the EU can benefit by certifying ICT products, processes, and services only once. Furthermore, the cybersecurity certificate would be recognized across the entire European Union.

In line with CSA, several schemes are being defined including the EUCC, EU Cloud Services (EUCS), EU Artificial Intelligence (EUAI), and EU Internet of Things (IoT).

On 1 July 2020, ENISA delivered the first certification scheme to the EU. This work was done in conjunction with: an Ad Hoc Working Group composed of cybersecurity certification experts; members of the European Cybersecurity Certification Group (ECCG) composed of representatives from EU Member States; and with input from the EU Stakeholders Cybersecurity Certification Group (SCCG) which includes representatives from consumer organizations, conformity assessment bodies, standard developing organizations, and trade associations. This scheme, which was made available for consultation and feedback, covers the certification of ICT products using the Common Criteria ISO/IEC 15408.

According to *Cybersecurity Certification: EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS,* the new certification framework builds on the framework agreed upon under the Senior Officials Group Information Systems Security (SOG-IS), and seeks "to improve the Internal Market conditions, and to enhance the level of security of ICT products dedicated to security (e.g., firewalls, encryption devices, gateways, electronic signature devices, means of identification such as passports, …) as well as of any ICT product embedding a security functionality (i.e., routers, smartphones, banking cards, medical devices, tachographs for lorries, …)."

The framework achieves this aim by offering security assurance levels which inform users of the cybersecurity risk of a product. The CSA designates three levels: basic, substantial, and high. These three levels are intended to be commensurate with the level of risk associated with the intended use of the product, service, or process, in terms of probability and impact of an accident. A high assurance level would mean that the certified product passed the highest security tests. The EUCC, however, only describes substantial and high, as there are minimal requirements to achieving a basic level security certification.

In addition to addressing the requirements of substantial and high cybersecurity certification, the framework sets out the following:

- The scheme includes specific measures to allow the prompt recognition of certified ICT products as it includes rules for the implementation and use of a dedicated labeling framework. Such framework has been designed to foster the placement of certified products both within and beyond the EU single market.
- Flexible set of evaluation assurance levels: Multiple levels of assurance are defined in the EUCC and have been mapped with two assurance levels of the CSA. This allows covering the security assurance needs of a large number of different markets, as the higher the level of assurance the product has, the more proof there is for its security with an increasingly rigorous method of testing.
- Certification under this scheme at 'high' assurance levels stems from the authorization of a Governmental agency.
- The EUCC enables consumers to have an impartial assessment of an ICT product: such an assessment is also a security evaluation, as the EUCC includes an analysis and testing of the product for conformance to specific security requirements. This increases the consumer's level of confidence in and reliance on the security of the certified ICT product.
- The EUCC enables patch management and vulnerability handling.

SECTION 4: Analyzing the EUCC's approach

4.1 The value of certification

Certification demonstrates that a device, component, or application adheres to a level of cybersecurity conformance, interoperability, and robustness. The certification level designation enables stakeholders to maximize the potential of existing opportunities and break into new markets. It also confirms alignment with business, security, regulatory, and data protection requirements laid out by national, regional, and global entities. By obtaining cybersecurity level certification, private companies can differentiate and market their products against competitor solutions. Moreover, obtaining cybersecurity certification allows companies to build and protect their own brand by protecting the products and/or services that they offer, and the ever-growing volume of sensitive personal data collected and stored on, and communicated by, connected devices.

Furthermore, cybersecurity certification helps decrease fraud and improve public safety by safeguarding privacy and preventing access to sensitive data and critical systems by bad actors. For example, undergoing cybersecurity certification ensures that components in an automobile's computer system are resistant to hacks, particularly important while the vehicle is on the road. Similarly, certifying the security of traffic light devices in a smart city offers assurance that the infrastructure will not be breached, causing city-wide delays or even accidents.

Stringent certification standards benefit corporates and consumers, increasing confidence in the technology and its application. When applied globally and recognized across borders, standards help decrease disparities and fragmentation easily and efficiently, promoting trade and economic development.

The EU should be commended for its proactive approach to responding to today's threat landscape and the increasingly complex relationship between technology, security, commerce, and data. The Cyber Security Act (CSA) provides a solid starting place from which to improve the general security level of the market and the products and services that it comprises.

There are challenges with the approach laid out by ENISA, however, that may create confusion in the marketplace and ultimately undermine the aims of the CSA.

4.2 The challenges of misalignment: Comparing public & private certification schemes

Though the CSA seeks to provide stakeholders and European citizens with a method for clearly identifying and evaluating the security of their products, implementation of the EUCC scheme, as proposed by ENISA, may in fact introduce additional confusion.

Citizens need clarity and confidence to adopt technology. If a device is certified at the highest level of security, that achievement should clearly equate to the robustness of the device's security and the functionality it can therefore support.

The EUCC has potentially introduced confusion in how it has established its security levels. According to the EUCC's current framework, only public schemes operated by national bodies can certify that an applicant meets the highest level of cybersecurity.

By extension, certifications from established security certification schemes, such as those advanced by GlobalPlatform, EMVCo, and FIDO Alliance which represent today's best practices for cybersecurity across many different industries, can only be recognized as substantial under the EUCC.

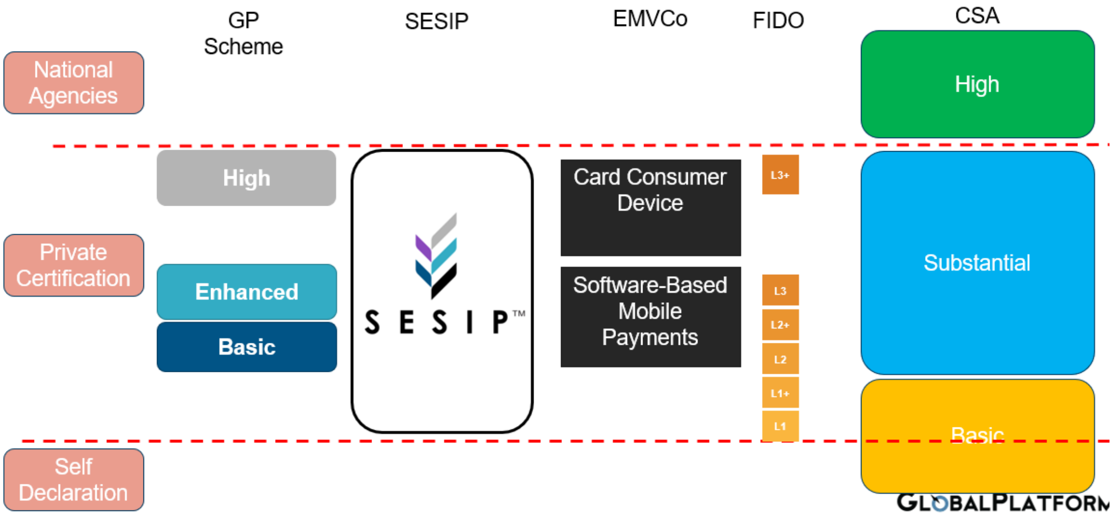

Figure 2: EUCC security levels, based on certifying bodies

This approach confuses robustness with assurance, highlighting to end users that the entity that certified the device is more important than the robustness of the device's security. To put this in context, a product with a AVA.VAN.5 robustness (highest security) under GlobalPlatform's private scheme would be labeled "EU substantial" while a product with a AVA.VAN.3 robustness (moderate security) under the EUCC scheme could be labeled "EU high." In cases like these, mixing security robustness with the certifying body only serves to increase confusion instead of confidence.

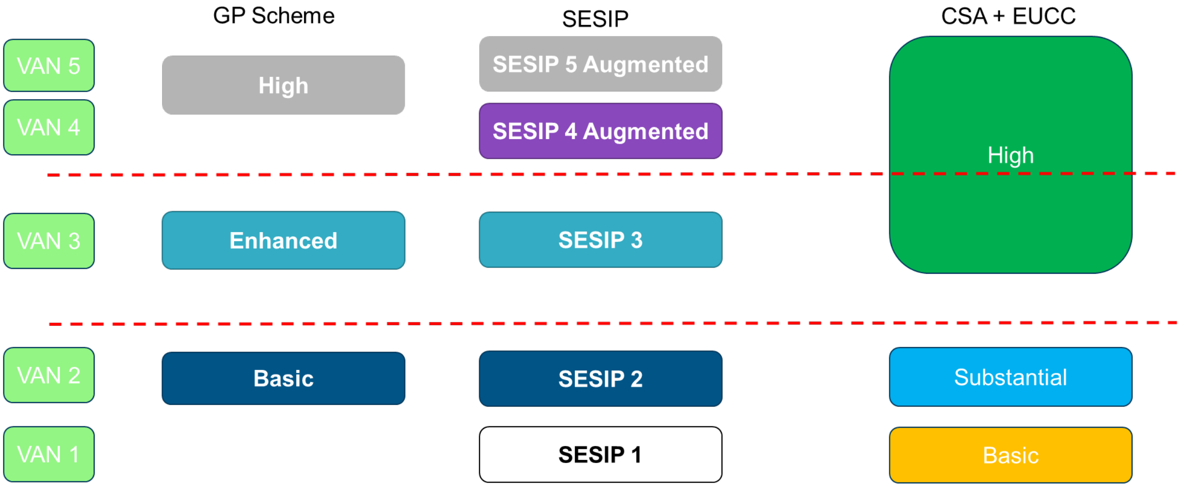

Figure 3: Comparison based on attack potential

Compounding this, the EUCC also groups several AVA.VAN assurance levels together. In practice, this might mean that two separate countries for their eID process may require vendors to achieve a “high” certification. However, by grouping AVA.VAN levels into the high category, the first country could require AVA.VAN.5 security while the second country’s high certification could only meet AVA.VAN.3. To truly understand the security robustness, the end user must know the difference between AVA.VAN.3 and AVA.VAN.5 and understand that the high-level security designation can reflect either, depending on the country in which the device is certified. Furthermore, defining AVA_VAN.3 in the “High” category is not coherent with the approach of industry security schemes. The CSA’s framework will therefore not necessarily reflect the security reality. ENISA’s framework disrupts the market already governed by a security mindset that relies more on robustness than assurance and adds unnecessary complexity to the ecosystem. GlobalPlatform’s suggestion is to adopt the following approach, that will better reflect the market.

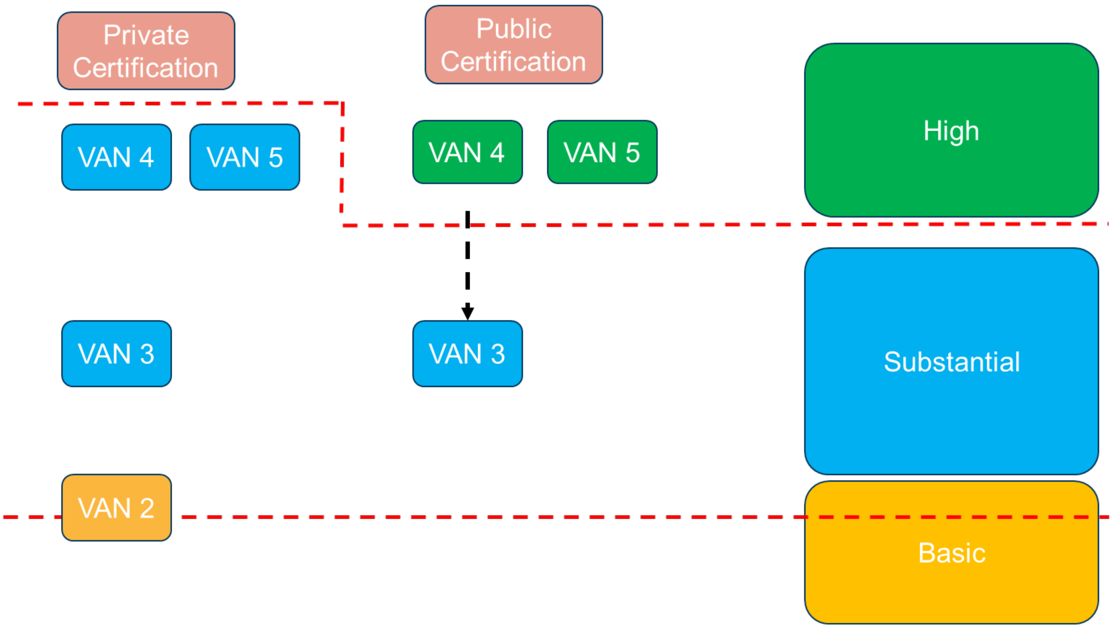

Figure 4: Proposal for EUCC coherence with the market

4.3 ADDRESSING FRAGMENTATION

Initiatives like this should also decrease fragmentation, rather than foster it. Defining differing regulatory approaches by country or region is not productive and does not effectively communicate to consumers the robustness of the security certification, particularly in cases where device makers want to develop and launch products to be deployed globally. The objective is the same everywhere: secure devices that function effectively as designed while still protecting the involved stakeholders’ privacy. If each region’s process for standards certification diverges, device makers will need to spend unnecessary time, money, and effort to achieve the same outcome. From an economic standpoint, it’s essential for the sake of global trade to avoid fragmentation between countries and regions. The EU must align with the U.S. and both Europe and North American must align with other markets like China to provide device makers with a global view of cybersecurity standard requirements.

--

Ultimately, some markets require mandatory Industry Security Certification that focuses on security robustness and is recognized worldwide. As such, to maintain relevance, the EU's certification scheme must come into alignment with the schemes already in place in private industry. As it stands, established global industry and private schemes will never be compliant with the EUCC and existing schemes are already tailored to address the needs of the industry and the complexity of the ecosystem.

SECTION 5: CONCLUSION

Security is critically important and security levels help bring alignment to the global ecosystem. The certification process allows the industry to validate and demonstrate security robustness. A clear approach to security certification and robustness helps stakeholders, end users, and consumers understand and compare the security features of components and devices.

> *“The implementation of CSA by ENISA using the proposed EUCC scheme will result in misalignment and confusion. For a time, only security experts will be able to differentiate between the security robustness and assurance offered by the EUCC. We will need to live for a while with this reality and it may not be pleasant. End users expect and rely on the fact that devices meet the requirements for high or substantial security. If the robustness of the security does not meet the expectation of the consumer, brands may be exposed and damaged. End users will not have accurate information to make educated choices.”*
>
> *Olivier Van Nieuwenhuyze, Chair of the GlobalPlatform Security Task Force*

If the EU’s true aim is to enhance cybersecurity, the misalignment of the CSA created by ENISA’s adoption of the EUCC as it stands can be rectified through collaboration and alignment between private and public certification bodies and schemes, and placing more emphasis on soliciting input from the industry through organizations like the SCCG. The goal of this collaboration must be a cybersecurity certification scheme that is transparent, aligned with industry, and accessible to the end user.

Countries and regions are already motivated to avoid fragmentation in the certification ecosystem to promote streamlined, efficient cross-border trade. Similarly, governments and multinational corporations are recognizing and adopting certification methodologies like SESIP to facilitate secure product development and innovation, and to reduce time to market and the need to seek out multiple certifications for the same product. In the US, the National Institute of Standards and Technology (NIST) already recognizes the SESIP methodology, and its certification scheme maps to SESIP so that the assurance levels are mutually recognizable, easily scalable, and can be reused across multiple market-specific schemes.

As more European countries and multi-national corporations in Europe align their cybersecurity certification schemes with SESIP and other private industry-initiated frameworks outlined above, fragmentation will dissipate, clarity around security assurances will increase and certifications will be understood and recognized across borders, and the overall level of cybersecurity will increase.

The EU CSA, ENISA, and the EUCC have a fundamental role to play in the future of cybersecurity on both the European and global stages. Alignment with existing cybersecurity initiatives and security levels will help the ecosystem to demonstrate the capabilities of products, foster confidence and adoption, and provide greater end-to-end security, privacy, simplicity, and convenience for everyone.

SECTION 6: TABLE OF FIGURES