EUROSMART
The Voice of the Digital Security Industry

The new paradigm of security certification of chip-based identity documents

Guidance in the context of the Cybersecurity Act

Executive summary

- There are growing concerns regarding the security erosion of embedded software nested in the chip of identity documents. Some national authorities want to maintain the security of the software on the field.
- Long-lasting identity documents and security erosion are two contradictory trends.
- The future EU Common Criteria certification scheme – developed in the framework of the Cybersecurity Act (CSA)- will bring continuous monitoring. This will be an improvement compared to the current SOG-IS.
- This monitoring should feed a risk management implemented by national authorities. This risk management should take into account the output of the monitoring (security surveillance) and the risks stemming from the usage of the embedded software.
- Correction of security flaws may be done via software upgrade, but this is not always possible.
- Limiting the validity period of identity documents is a complementary or alternative approach to software upgrade.
- Technical solutions should be as transparent and as smooth as possible for the final holder.

Introduction

Within Europe, the three main types of chip-based identity document, namely electronic passport, European resident permit and identity card have a long validity period (usually ten years for passport and identity cards). These identity documents are instrumental as they (1) support free circulation of citizen within Europe, (2) secure crossing of external European borders, and (3) also provide digital identity and electronic services to citizen, providing them secure access to private and public digital services.

For each of these three functions, the security of the identity document is paramount, and for each of them, the security of the embedded software nested in the chip of the identity document is also key. The security of embedded software used in chip-based identity document is demonstrated through a security certification pursuant to the Common Criteria methodology under the SOG-IS Mutual Recognition Agreement (MRA). The minimum security level required by the various national and European regulatory and legislative acts is EAL4 enhanced with AVA_VAN.5. The latter component being key to demonstrate it is not possible to tamper with the embedded software using state of art methods, skills and equipment.

Currently the Common Criteria security certificates delivered under the SOG-IS Mutual Recognition Agreement (MRA) have a limitation as they only demonstrate that the embedded software met the security requirements at the time of certification, but don't provide any guarantee with regards to this compliance later in time.

Several trends currently at stake will change this situation in the near future.

-**Part I** describes how the transformation of the Common Criteria security certification scheme will lead to the inclusion of a continuous monitoring of the Common Criteria security certificate. This will provide better confidence in the effective security of certified products over time, but will also entail enhancement of the process of initial Common Criteria security certification through a continuous security monitoring thanks to regular security surveillance (pursuant to Common Criteria methodology).

-**Part II** analyses the market trends pertaining to identity documents that have impacts on the expectations vis à vis the security of embedded software contained in chip based identity documents. In particular, it analyses the growing concern for security erosion of embedded software on the one hand – which meets to some extent the transformation of the Common Criteria security certification scheme, and the need for very long lasting lifetime of embedded software on the other hand, which are conflicting trends.

-**Part III** looks into the measures to put in place to (1) meet the new requirements resulting from the transformation of the Common Criteria security certification scheme, and (2) address the two conflicting market trends identified in part II.

I-The new context established by the CSA for security certification of embedded software

The CSA[1], approved by the European Parliament and the Council of the European Union in 2019, defines a generic framework for security certification schemes providing EU wide recognition.

To benefit from the recognition brought by this regulation, a security certification scheme shall meet the key principles defined in article 54. In particular, it shall meet the principle enacted in article 54 (j).

> *(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity,* ***including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements.***

This principle is important as it entails that any security certification scheme shall ensure a continuous monitoring of compliance with the applicable cybersecurity requirements of any product which has been granted a security certificate. Should a product cease to meet the applicable cybersecurity requirements – for instance because of a security flaw – the monitoring procedure put in place by the security certification scheme shall ensure that (1) the issue is detected and (2) the security certificate is withdrawn. Furthermore, pursuant to article 58.7(a) of the CSA, it is the responsibility of the National Cybersecurity Certification Authority (NCCA) – appointed by each Member State – to enforce the fulfillment of the principles enacted in article 54, including (j).

The principle enacted in article 54(j) will harmonize and clarify the meaning of a security certificate issued by a National Cybersecurity Certification Authority (NCCA) under the framework of the CSA. As long as the security certificate is valid, the product is considered as meeting the expected security requirements. Conversely, as soon as the National Cybersecurity Certification Authority (NCCA) notices a product does not meet anymore the expected security requirements, the security certificate shall be withdrawn, if the issue cannot be solved within a short timeframe during which the certificate is suspended. As such, this principle will ensure higher trust when using security certified products, as the security certificate will not only ensure that they met the security criteria at the time of certification, but also that they still meet them as long as the security certificate is valid. This is a major breakthrough and a new paradigm for security certification.

Following a direct request from the European Commission to ENISA[2] mid-2019, security certification based on Common Criteria methodology under the SOG-IS Mutual Recognition Agreement (MRA) will be transformed into a security certification scheme compliant to the provisions of CSA. While it will not fundamentally change the assessment methodology, it will bring major improvements compared to the current SOG-IS Mutual Recognition Agreement (MRA) with regards to the monitoring of certified products. This transformation is of direct interest for embedded software – used among other in identity documents to protect sensitive data (biometry, authentication keys…) – which are all security certified using Common Criteria methodology under the SOG-IS Mutual Recognition Agreement (MRA), as they will benefit from these improvements.

Currently, Common Criteria security certificates delivered under the SOG-IS Mutual Recognition Agreement (MRA) only demonstrate that a product met the security requirements at the time when

---

[1] **C**yber**S**ecurity **A**ct - 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).

[2] European Union Agency for Cybersecurity.

the certificate was granted. It does not bring any insurance with regards to the effective security of the product after certification, as the monitoring of the effective security of products after their certification is not required by the agreement. Furthermore, depending on (1) the certification scheme (country of issuance), and (2) the decision of the developer, some kind of continuous monitoring of Common Criteria security certificate may be put in place, however it is difficult to sort out if and how, and the approaches are diverse between Member States. This national fragmentation, combined with the limited scope of the SOG-IS Mutual Recognition Agreement (MRA) with regards to the continuous monitoring of security certified products, leads to a limited significance of security certificates delivered under this agreement. Therefore, these Common Criteria security certificates only demonstrate that a product met the security requirements at the time of certification, but do not have any meaning with respect to their effective security later in time.

The transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA will bring major harmonization and clarity when it comes to the meaning of a Common Criteria security certificate with regards to the effective security of a certified product at any time. As long as a product will benefit from a valid Common Criteria security certificate, it entails an effective security meeting the requirements set for initial security certification. As such, it will support a higher level of trust and better visibility when using a Common Criteria security certified product.

Unlike Common Criteria security certificates delivered under the SOG-IS Mutual Recognition Agreement (MRA), the certificates that will be delivered under the new security certification scheme will be continuously monitored by the National Cybersecurity Certification Authority (NCCA) over time. It entails that any security certified products will have to go through security surveillance on a regular basis, so that the National Cybersecurity Certification Authority (NCCA) could verify the security certificate is still valid. Should the security surveillance demonstrate that the product on the field (already issued) does not meet the security requirements anymore, it would be up to the National Cybersecurity Certification Authority (NCCA) to decide whether or not to withdraw the security certificate.

Resulting from the requirement of monitoring of certified products, and as required by article 54 (r) security certificates issued under a security certification scheme compliant with the CSA shall have a limited lifetime.

r) maximum period of validity of European cybersecurity certificates issued under the scheme.

Technical highlight

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA (EU CC scheme). The ad hoc group has proposed that security certificates have a limited lifetime of 5 years, that could however be extended upon successful security surveillance.

More details can be found in "§20. PERIOD OF VALIDITY OF CERTIFICATES" of the report prepared by the ad hoc group.[3]

[3] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/at_download/fullReport.

Also, the transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA will provide for handling of vulnerabilities not detected previously, as required by article 54 (m) of CSA:

> *(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;*

The purpose is to make sure that appropriate rules are put in place to report and handle any vulnerabilities detected on a product previously certified and thus potentially on the field. In particular, it aims at making sure these vulnerabilities (1) are reported in a responsible manner to avoid exploitation by malicious actors, and (2) are handled and processed with the utmost confidentiality and care.

Technical highlight

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA (EU CC scheme). The ad hoc group has identified that following standards shall be used to meet this provision from the CSA:

- "ISO/IEC 30111 - Information technology — Security techniques — Vulnerability handling processes" for the handling of vulnerabilities;
- "ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure" for the vulnerability disclosure.

More details can be found in "§14. RULES RELATED TO HANDLING VULNERABILITIES" of the report prepared by the ad hoc group.[4]

II-Market expectations vis à vis security of embedded software contained in chip-based identity document

Some trends of the market of identity documents also have impacts on expectations vis à vis the security of the embedded software.

Growing concerns for security erosion of embedded software

In 2017, the ROCA issue, impacting some embedded softwares contained in chip-based identity documents, highlighted that the product security may erode over time. It really acted as a revelation. Despite the negative consequences that had to be handled, it had nevertheless positive consequences, as it increased the global awareness of issuing authorities of security erosion over

[4] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/at_download/fullReport.

time of embedded software. Ever since, more and more issuing authorities are concerned with the erosion of security of embedded software over time.

Managing security erosion of embedded software requires continuous monitoring of its effective security over time. It may be achieved thanks to the security surveillance procedure. In that respect, the concerns from issuing authority meet the future improvement of the Common Criteria security certification scheme resulting from its transformation into a security certification scheme compliant with the provisions of CSA. The continuous monitoring of the validity of Common Criteria security certificates ensured by the National Cybersecurity Certification Authority (NCCA) will support the issuing authority. However, this is not sufficient. This monitoring shall feed a risk management taking into account the output of the monitoring (security surveillance) and the risks stemming from the usage of the embedded software. It is the responsibility of the issuing authority to manage the risks.

Some issuing authorities have even decided to go far beyond, by also requiring to maintain over time the effective security of embedded software contained in chip-based identity documents **on the field (meaning delivered to their final holder)**. It means that potential or identified security flaws on embedded software shall be corrected on the identity documents on the field **(meaning delivered to their final holder)** so that their security is maintained.

Long lasting identity document

Embedded software contained in chip-based identity document are security certified before the issuance of identity document, in order to make sure that only trustable documents are delivered. However, a substantial delay may happen between the date when the security certification is granted, and the date of first issuance of identity document. In some cases, the security certification is required not only for the issuance of identity document to the final holder, but prior to the production of blank document, which may take place a year ahead of the beginning of document issuance. Furthermore, once industrially qualified, a given version of embedded software is used for production of identity documents for several years.

On the other hand, the identity document is made to be used for a long validity period, usually ten years.

These major considerations entail that the lifetime of an embedded software, defined as the time between the date of its security certification and the date when the last identity document where it is included is removed from the field, is very long. This lifetime covers (1) the period between the security certification of the embedded software and the date of issuance of the first identity document containing it (leadtime for introduction of the embedded software on the field), (2) the period during which the embedded software is used for the production of identity document (several years), and (3) the validity period of the identity document (time needed before the last identity document containing the embedded software is removed from the field).

> **Example**
>
> In the case of a passport with a validity period of 10 years, whose embedded software has been used for production for 3 years, and has been introduced on the field 1 year after its security certification, the lifetime of the embedded software is 1+3+10 = 14 years.

It entails that the lifetime of the embedded software is large, longer than the validity period of the identity document itself.

These two trends of identity documents market are conflicting from the perspective of security of embedded software: very long lifetime of embedded software (well above 10 years) and growing concern for its effective security all along its lifetime. They are contradictory as the larger the lifetime of the embedded software is, the higher is the likelihood of its security erosion and apparition of security flaws due to the progresses of hacking capacities and expertise of malicious entities. Therefore, because of its long lifetime, the effective security of the embedded software contained in chip-based identity document all over its lifetime, especially towards the end of its lifetime is seriously questioned. Furthermore, as explained above, the Common Criteria security certificate of the embedded software does not provide any help. It only demonstrates it was secure at the time of security certification, but does not provide any assurance with regards to its effective security all along its lifetime.

In order to reconcile these two contradictory trends, supplemental measures going beyond the initial security certification of the embedded software are needed.

III-Which impacts on chip-based identity documents?

Issuing authorities shall bear in mind the operational consequences drawn from (1) the transformation of the Common Criteria security certification scheme into a security certification compliant with the provisions of the CSA, and (2) the consequences of the market trends. The initial Common Criteria security certification of the embedded software - regardless its level - is not sufficient anymore to meet these goals, unless it is completed by the following supplemental measures:

- Providing a monitoring of the effective security of the embedded software all along its lifetime;
- If required by the issuing authority, putting in place measures allowing to maintain the effective security of the embedded software all along its lifetime.

Monitoring of effective security over time

At minimum, the erosion of the security of the embedded software contained in the chip-based identity document shall be monitored on a regular basis to help the issuing authority to manage risks and possibly take actions. This new paradigm is also acknowledged by the transformation to come of the Common Criteria security certification scheme under the CSA, where security certificate will remain valid as long as the continuous monitoring ensured by the National Cybersecurity Certification Authority (NCCA) demonstrates the security requirements are still met.

This entails regular security surveillance of (1) the underlying IC, (2) the operating system (e.g. javacard platform) and (3) the applet/application all along the lifetime of the identity document. This task consists in assessing periodically within a duly qualified ITSEF the strength of each of these items with regards to the state-of-the-art hacking methods. It requires highly skilled experts and specific cutting-edge equipment.

Technical highlight

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA (EU CC scheme). The ad hoc group has proposed that security surveillance of certified

product be carried out in accordance with the re-assessment procedure defined in assurance continuity process.[5]

More details can be found in "§11.RULES FOR MONITORING COMPLIANCE" of the report prepared by the ad hoc group.[6]

This step allows (1) the National Cybersecurity Certification Authority (NCCA) to assess the erosion of security of the embedded software - and thus its effective security - and to decide whether the security certificate still applies or not, and above all (2) the issuing authority to have an overview of the effective security of the embedded software. However, it does not guarantee that the effective security of the embedded software still meets the one required at time of certification.

Regular security surveillance is not an end in itself but shall feed a **risk management** operated by the issuing authority. Should the effective security be considered as insufficient, leading to the withdrawal of the security certificate, the corresponding risks shall be managed by the issuing authority. In particular, the issuing authority shall (1) understand the risks, and (2) assess them with regards to the usage of the embedded software contained in the chip-based identity document to decide which action(s) to initiate (mitigation measures, limitation of usages, anticipated replacement…). It requires from the issuing authority a sharp expertise but above all the ability to manage a risk. While this is common in the payment sector (with banking cards), such approach may not be well perceived by issuing authorities, which are governmental entities usually reluctant to risks.

In order to support the necessary risk management, **issuing authority should define a contingency plan** detailing the different mitigation measures and scenarios to apply depending on the level of the security erosion. The contingency plan may for instance provide for:

- Regularly introducing newer, more recent and more secure embedded software for the production of identity documents;
- Using several embedded softwares' source for the production of identity documents to mitigate potential impacts resulting from their security erosion;
- the limitation of uses for impacted identity documents (if the security erosion requires it);
- replacing embedded software used for production of identity document by a new one (if the security erosion requires it);
- replacing identity documents on the field by new ones (if the security erosion requires it).

Maintenance or restoration of effective security

Beyond the monitoring of the effective security of embedded software contained in chip-based identity document, issuing authority may also require this effective security to be maintained all along its lifetime, so that (1) it reaches the same level as the one met at the time of initial security certification, and (2) thus its security certificate remains valid all along its lifetime.

[5] https://www.sogis.eu/documents/mra/JIL-Assurance-continuity-v1.0.pdf.
[6] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/at_download/fullReport.

One possibility consists in upgrading the embedded software contained in chip-based identity document as soon as a security flaw is identified, to curb it. This is achieved by applying a patch. To ensure the upgrade of the embedded software is performed in a fully secure manner, the patch management feature shall be security certified.

Technical highlight

The methodology for security evaluation of embedded software supporting upgrade features (patch) has been first defined by the SOG-IS, which proposed a comprehensive approach in a dedicated application note.[7] The latter has been inspired by ANSSI's application note.[8] Also, standardization activities are currently ongoing to standardize methodology for security evaluation of ICT products (not limited to embedded software) supporting upgrade features (patch). Within ISO/IEC JTC1/SC27/WG3, the Technical Report "Extension for Patch Management for 15408 and 18045" is being prepared. Also, the ISCI/WG1 is preparing new SAR components and Packages in Common Criteria for Patch Management.

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act, ENISA has set up an Ad Hoc Working Group to support the transformation of the SOG-IS Mutual Recognition Agreement (MRA) into a security certification scheme compliant to the provisions of CSA (EU CC scheme). Pursuant to the work of this ad hoc group, if one of these evaluation methodologies are applied during the initial certification of the product, new possibilities emerge for the correction of the vulnerabilities found in the already certified product. The report[9] prepared by this ad hoc group defines 4 levels of patch in "§15. PATCH MANAGEMENT ":

-Patch Level 1 applies where the TOE (Target Of Evaluation i.e. certified product) is part of a bigger ICT product, and product parts not affecting the TOE may be patched whenever required. The initial Common Criteria evaluation needs to clearly define the TOE scope and demonstrate that changes outside the TOE scope cannot affect the security of the certified TOE as stated above.

-Patch level 2 is to be applied for minor changes. According to this level, the evaluation laboratory (ITSEF) needs to determine, whether the patch complies with the applied patch management methodology, and whether it can be deployed on the field. The patch, if deemed appropriate can be deployed before the certification body reviews the evaluation documentation, thus providing an opportunity to speed up the process. The certification body will review the results, and if there is any problem with the process, can make a decision based on the certification process.

-Patch level 3 is the application of the already existing Assurance Continuity process[10].

-The fourth level is called Critical update flow, for changes where an attack is already possible to be exploited or update is critical and needs to be released urgently. Critical Update Flow process shall not replace Patch Level 2 or 3, and shall be used as a way for the manufacturer or provider to deploy or release a critical update quickly and then follow Patch Level 2 or 3 at a later date. This is the only case where the patch is deployed or released prior to review, but

[7] https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-note-on-security-requirements-on-code-loading-v1.0.pdf.
[8] https://www.ssi.gouv.fr/uploads/2014/11/ANSSI-CC-NOTE-06.2.0-Exigences-de-s%C3%A9curit%C3%A9-pour-un-chargement-de-code-en-phase-dutilisation-EN.pdf.
[9] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/at_download/fullReport.
[10] https://www.sogis.eu/documents/mra/JIL-Assurance-continuity-v1.0.pdf.

of course, here the initial certification process already ascertained the methods to be followed by the manufacturer.

With these applicable patch management levels, the EU CC Scheme might offer a solution to the problem of how to handle effectively vulnerabilities found in already certified product while continuously offering a certified state of the product.

In addition, the upgraded embedded software shall also be security certified each time an upgrade is released, to ensure a continuous trust all along its lifetime. However, this approach has some limitations described below.

First, **it may not always be technically possible to maintain the effective security**, especially when the security flaw relates to the physical characteristics of the embedded software (hardware design, new methods to exploit ancillary channel…) which cannot be corrected through software means.

Secondly, where the upgrade of the embedded software leads to the erasure of the data it contains, specific issues may arise. In the case of personal data (portrait, biographic data…), it may be necessary to temporarily safeguard them in an external repository, so that they could be reloaded later in the embedded software after completion of the upgrade. Such situation would require to ensure and demonstrate compliancy of these processes with the provisions of GDPR (regulation 2016/679), in particular with regards to **the confidentiality and privacy of personal data**. In the case of "technical data" used for the provision of digital identity or trust services (private keys, certificates, holder PIN codes) to ensure the binding between the embedded software, the holder and the issuer, i.e.:

- **Authentication/trust service private key(s) and corresponding certificate(s)** binding the embedded software (and thus the chip-based identity document) to the issuing authority;
- **PIN code(s)** binding the embedded software (and thus the chip-based identity document) to the holder.

A form of re enrollment should be carried out after completion of the upgrade to securely restore the binding of the embedded software (and thus the chip based identity document) with (1) the issuing authority (through a new authentication/trust service private key(s) and certificate(s) securely provisioned in the embedded software), and (2) the holder (through the secure loading of the PIN code(s)).

Nevertheless, this approach remains very interesting to ensure a long-lasting security of embedded software, as it allows a continuous maintenance of its security and correction of security flaws. However, issuing authority shall bear in mind that it requires (1) specific mechanisms to be implemented in the embedded software, and also (2) to deploy and operate the corresponding management infrastructure (server…). Last but not least, it is of the highest importance that the technical implementation be transparent and as smooth as possible for the final holder. In particular, upgrade of the embedded software should not be perceived as cumbersome by the identity document holder. It is instrumental to make sure this solution is effectively implemented on the field.

A complementary or alternative approach consists in avoiding the risk of security erosion of the embedded software by limiting the validity period of the chip-based identity document to reduce the lifetime of the embedded software. The underlying idea is to reduce the validity of the identity document, so that the risk of security erosion of the embedded software over its lifetime can be estimated, controlled and ultimately reasonably excluded. For instance, issuing

authority could consider reducing the validity period of identity card from 10 to 5 years to exclude the risk of security erosion of the embedded software it contains. Where the same version of embedded software is used for production of identity cards during three years, and the leadtime for introduction of the embedded software on the field is one year, it could reduce the lifetime of the embedded software from 14 to 9 years.

Glossary

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CC	Common Criteria
CSA	Cyber Security Act
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ITSEF	Information Technology Security Evaluation facility
MRA	Mutual Recognition Agreement
NCCA	National Cybersecurity Certification Authority
SOG-IS	Senior Officials Group Information Systems Security

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

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com