EUROSMART
The Voice of the Digital Security Industry

Managing the risk for chip-based documents

Introduction

In a previous paper[1], Eurosmart highlighted the challenge of ensuring that software embedded in the chip of documents keeps its initial security level all over its lifetime. Such documents may be, for instance, identity cards, electronic passports, but also tachograph cards, health cards, or tokens used to create qualified signatures. This difficulty stems from two factors. Firstly, the lifetime of documents may be very long (the typical lifetime of a passport or a national identity card is ten years). Secondly, throughout this period, the expertise of fraudsters will substantially rise, and the range of materials available to them will broaden. This situation leads to the erosion of the security of the software embedded in the chip of documents. Therefore, the risk of successful compromising attempts by malicious actors increases over time.

The previous paper identified and described several solutions to avert this risk. Furthermore, it placed a particular emphasis on the concept of risk management which is instrumental to successfully managing the security erosion of software embedded in the chip of documents over its lifetime.

The present document builds on this work. After reviewing the management of security erosion of certified products under the EUCC certification scheme (Section 1), it proposes novel solutions to address the problem. In particular, it gives recommendations on three aspects:

1. Update the current legal framework to align it with the "reality principle" (Section 2);
2. Improvement of the EUCC certification scheme to take into consideration products already in the field (Section 3);
3. Guidelines for issuing authorities to manage the risk of exploitable vulnerability occurrence (Section 4).

[1] The new paradigm of security certification of chip based identity documents – Guidance in the context of the Cybersecurity Act (https://www.eurosmart.com/eurosmart-advocates-for-a-new-paradigm-of-security-certification-of-chip-based-identity-documents/).

1. Management of the security erosion of certified products under the EUCC certification scheme[2]

Current situation

As described in our previous paper, applicable EU provisions require that software embedded in the chip of documents is security certified using the Common Criteria methodology at a certain level, usually at least at level EAL4+ AVA_VAN.5. In Europe, the recognition of such security certificates is ruled by the SOG-IS agreement[3] that provides a common understanding and methodology for the evaluation and, in particular, penetration testing. Soon, the EUCC certification scheme will replace this agreement. It will be the first security certification scheme established under the Cybersecurity Act (Regulation 2019/881). Pursuant to the rules set forth for the EUCC certification scheme, the maximum validity period of the security certificates will be five years.

However, because of the long-lasting lifecycle of documents, spanning from (1) development, (2) period of issuance, and (3) validity period (usually ten years), providers must renew the security certificate of their products several times, as summarised below:

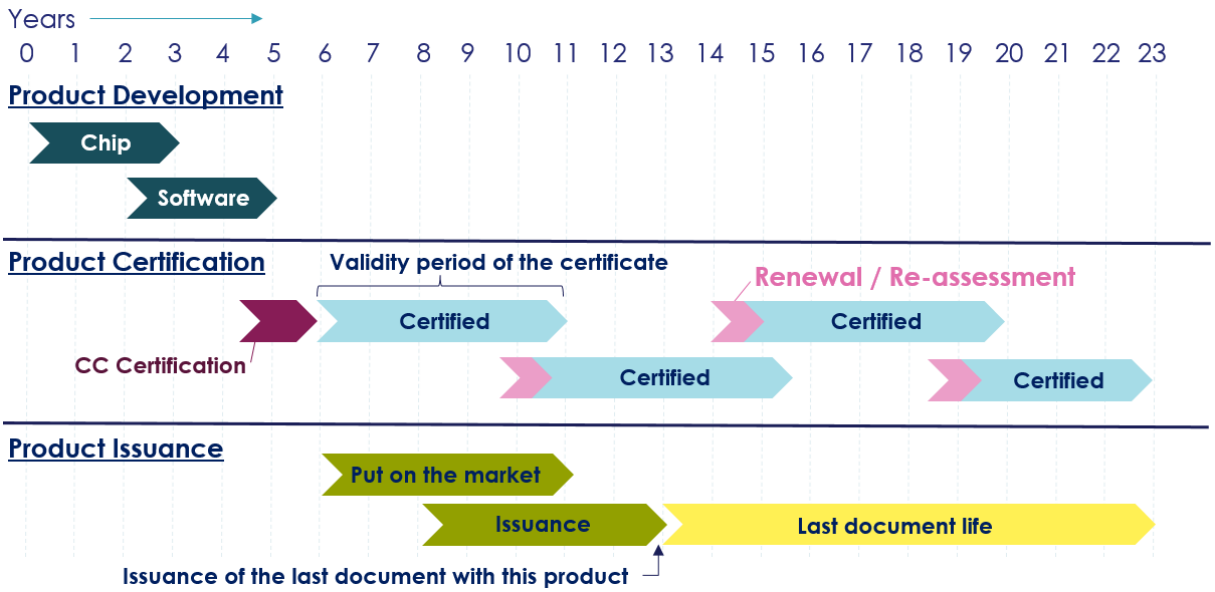

Figure 1 – CC Renewals during the product life

The process for the monitoring of the security certificate of a product (reflecting its effective security level) is described in the EUCC certification scheme "ANNEX 11: ASSURANCE CONTINUITY », "§2.4.4. Reassessment". Furthermore, this section clarifies the status of a security certificate after the detection of a security flaw. Pursuant to table 1, in case of a flaw, (1) the previous certificate shall be

[2] Cybersecurity certification - EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS - v1.1.1 - May 2021 (https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1).

[3] Senior Officials Group Information Systems Security (SOG-IS) - https://www.sogis.eu/index_en.html.

archived, and (2) the certificate shall be re-issued with the updated AVA_VAN[4] level (reflecting the effective resistance to vulnerability) or with a reduced scope of the Target Of Evaluation (TOE).

Shortcomings of this approach for chip-based documents in the field

The approach proposed by the EUCC certification scheme is perfectly suitable for monitoring the security certificate of embedded software to be placed on the market. This approach confirms the software meets the required security level before production and issuance. However, it does not provide a fully satisfying answer for software embedded in the chip of documents in the field.

The main reason is that legal obligations (resulting from laws and regulations), as well as contractual agreements with the supplier,[5] impose security certificates to keep their validity – including the AVA_VAN.5 level (resistance to vulnerability) and EAL[6]- so that the document could remain in the field. However, as a document generally stays in the field for a very long time (e.g., usually ten-year validity for a passport or an identity card), the security erosion of the software embedded in the chip is inevitable.

This security erosion of software embedded in the chip over time usually results from new exploitable vulnerabilities found either in the underlying integrated chip (IC) or in the software itself, in the course of the regular security monitoring. When a new exploitable vulnerability is found on the IC, the security recommendations to be applied by the developer of the embedded software running on the said IC are updated in order to counter the new potential risks. Embedded software not implementing such new security recommendations may therefore be at risk - as they do not implement the countermeasures required to counter the new exploitable vulnerabilities from the underlying IC.

Furthermore, it is hardly possible to have documents replaced in case of security erosion of the embedded software because of (1) the large number of documents in the field and (2) the inconveniences it would create for their holders (giving back the identity document, apply for another one, revert to a counter etc.).

Ways to mitigate this challenge

The monitoring of the security certificate of software embedded in the chip of documents already in the field shall rely on the approach proposed by the EUCC certification scheme. It is instrumental to provide the issuing authority with a comprehensive view of effective security throughout its lifetime. At the same time, the principle of reality also imposes finding ways so that software embedded in the chip of document already in the field could still be used, provided appropriate risk management is put in place. **Otherwise, it would lead to inextricable situations where users would have in their hands documents with embedded software that would not meet legal obligations anymore, and thus that would not be usable anymore. At the same time, issuing authorities would not be in a position to have them replaced.**

In order to address this issue, the present document provides:

- **Proposals to update legal texts** so that the reality principle described above is duly considered.
- **Proposals to improve the EUCC certification scheme** so that the EUCC certification scheme better takes into consideration the case of products in the field.

---

[4] The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

[5] For more details, refer to Annex 1.

[6] Assurance Level - set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package (definition Evaluation drawn from CC part 1).

- **Guidelines for managing the risks of exploitable vulnerability occurrence in software embedded in the chip of documents** so that issuing authorities could (1) limit consequences of an exploitable vulnerability and (2) handle it if it happens.

2. Proposals to update legal texts

Anticipate in legal texts the possibility of exploitable vulnerabilities and security certificate withdrawal

Suppose a legal text mandates a valid security certificate for a product. In that case, it shall also specifically consider the case of a product in the field when a vulnerability can be exploited. Specific provisions in the legal text shall allow the issuing authority to keep using a product in the field when a vulnerability has been detected, or the security certificate has been withdrawn, provided the issuing authority agrees to do so and adequate risk management and mitigation measures are put in place. It is essential to avoid any disruption in the provision and access to the service and avoid thousands or millions of documents in the field becoming useless overnight because of security certificate withdrawal.

When such an undesired event happens, the certification body, the evaluator of the product (SW and HW), the issuing authority and the product manufacturer should perform a risk assessment considering the exploitable vulnerability properties, the configuration and the environment of the product. Thus, they would identify mitigation measures that could be put in place to reconcile both the need for a high level of security but also the reality and the provision of the service.

Regulation (EU) N° 165/2014[7] ruling on tachograph cards is an excellent example of how a legal act shall handle such a topic. This Regulation makes the necessary distinction between products to be put on the market and products already in the field (or on the market):

Product to be put on the market

In order to be put on the market, tachograph cards have to get a type approval which implies a security certificate pursuant to Common Criteria (Article 2(u)). Should an exploitable vulnerability be discovered, Article 20(4) – first sentence - states that the product shall not be put on the market.

Product in the field (or on the market)

When a vulnerability is discovered on a product in the field, Article 20(4) – second sentence and next ones - clearly indicates how the manufacturer and competent authorities shall behave. In particular, this provision allows putting in place pragmatic risk management for the products in the field when an exploitable vulnerability is detected.

Article 20

Security

1. Manufacturers shall design, test and review vehicle units, motion sensors and tachograph cards put into production so as to detect vulnerabilities arising in all phases of the product life- cycle, and shall prevent or mitigate their possible exploitation. The frequency of tests shall be laid down by the Member State which granted the approval certificate, within a limit which shall not exceed two years.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0165.

2. For this purpose, manufacturers shall submit the documentation necessary for vulnerability analysis to the certification body referred to in Article 12(3). 3. For the purposes of paragraph 1, the certification body referred in Article 12(3) shall conduct tests on vehicle units, motion sensors and tachograph cards to confirm that known vulnerabilities cannot be exploited by individuals in possession of publicly available knowledge. **4. If, in the course of the tests referred to in paragraph 1, vulnerabilities in system elements (vehicle units, motion sensors and tachograph cards) are detected, those elements shall not be put on the market. If vulnerabilities are detected in the course of the tests referred to in paragraph 3 for elements already on the market, the manufacturer or the certification body shall inform the competent authorities of the Member State which granted the type-approval. Those competent authorities shall take all measures necessary to ensure that the problem is addressed, in particular by the manufacturer, and shall inform the Commission without delay of the vulnerabilities detected and of the measures envisaged or taken, including where necessary the withdrawal of type-approval in accordance with Article 16(2).**

Table 1- Extract from Regulation (EU) N°165/2014

Eurosmart calls on the European Commission and Member States to replicate such an approach in any legal text requiring security certification of products. In particular, the legal texts identified in Annex 1 should be considered.

The particular case of QSCD pursuant to eIDAS Regulation

Pursuant to Articles 30 and 39 of the eIDAS Regulation[8], a product shall be certified as QSCD[9] by a designated national authority based on a security certificate. For QSCD relying on secure element technology, security certification pursuant to Common Criteria at least at level EAL4+AVA_VAN.5 according to the protection profiles listed in Implementing Decision 2016/650[10] shall be performed.

QSCD certification is mandatory so that a product can create a qualified signature, i.e. a signature having the same legal value in court as a handwritten signature. On the other hand, as soon as the QSCD certification is lost, any subsequent signature that is created is not qualified anymore and loses its legal value.

The eIDAS Regulation does not differentiate between products to be placed on the market and products in the field. National authorities in charge of QSCD certification may interpret these articles in an exclusive way, where the QSCD certificate shall be withdrawn as soon as the underlying security certificate is withdrawn. While this interpretation is right for products to be put on the market, it is more disputable when it comes to products in the field. However, the wording of Articles 30 and 39 does not mandate to withdraw the QSCD certificate of a product in the field if its security certificate is withdrawn. Instead, a more pragmatic interpretation of these articles could be adopted, where a QSCD certificate could be maintained if suitable mitigation measures are implemented. This would help handle the case of QSCD in the field for which exploitable vulnerabilities occur.

Eurosmart supports the interpretation of Articles 30 and 39 whereby the QSCD certification of products to be put on the market requires a valid security certificate pursuant to Common Criteria at least at level EAL4+AVA_VAN.5. In addition, Eurosmart recommends national authorities in charge of QSCD certification adopt a more pragmatic interpretation of Articles 30 and 39 with regards to QSCD certificate for products in the field. In particular, it should be possible to keep the QSCD certificate of

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[9] Qualified Signature Creation Device.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650.

products in the field when vulnerabilities are exploited, provided suitable mitigation measures are implemented.

3. Improve the EUCC certification scheme[11]

Once an exploitable vulnerability is discovered on a certified product, following the monitoring of its security certificate (also called reassessment), the EUCC certification scheme provides for the following management of the security certificate[12]:

- The current security certificate shall be archived, meaning it is not valid anymore;
- The security certificate shall be re-issued to reflect the effective security level (AVA_VAN[13] and/or EAL[14]) following the outcome of the reassessment.

However, this transition may have substantial impacts on products in the field. The security erosion may lead to a situation where products in the field have their initial security certificate archived – and thus not valid anymore and updated with a lower effective security level (AVA_VAN and/or EAL), so much that they do not meet anymore the applicable legal and/or contractual obligations (in particular with regards to the AVA_VAN level and/or EAL). This situation is of particular importance for software embedded in the chip of documents which are meant to be long lasting, as highlighted in the figure below:

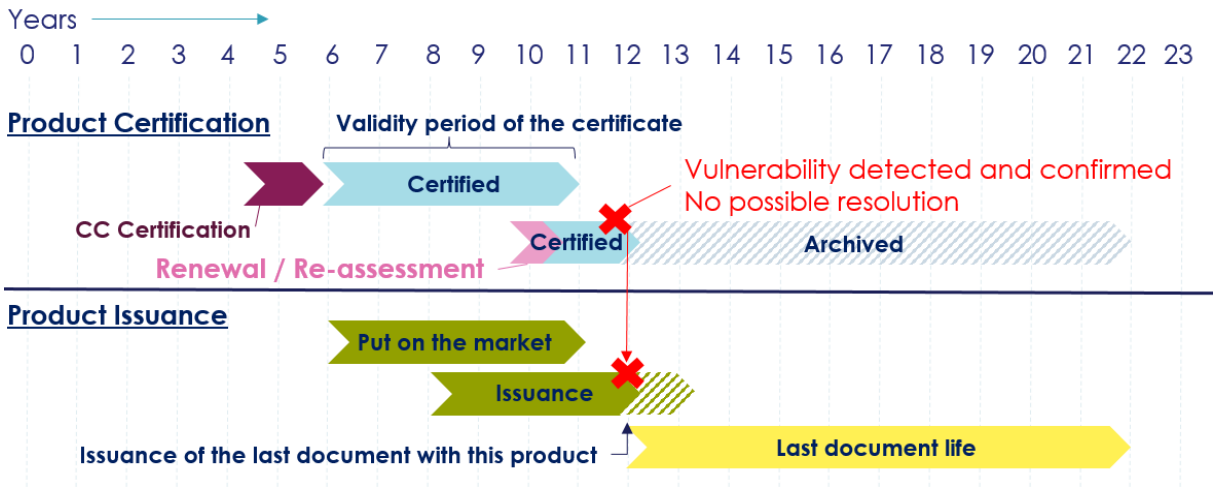

Figure 2 – EUCC Scheme – certificate vulnerability management

In its current shape, the EUCC certification scheme misses pragmatic solutions to manage the situation of products in the field for which exploitable vulnerabilities have been discovered and "to provide (…) a comprehensive view of effective security during its whole lifetime » (see previous Eurosmart paper[15]).

---

[11] Cybersecurity certification - EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS - v1.1.1 - May 2021 (https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1).

[12] ANNEX 11: ASSURANCE CONTINUITY, §2.4.4. Re-Assessment, table 1.

[13] The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

[14] Assurance Level - set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package (definition Evaluation drawn from CC part 1).

[15] https://www.eurosmart.com/eurosmart-advocates-for-a-new-paradigm-of-security-certification-of-chip-based-identity-documents/.

The ultimate goal is to avoid the situation where many products in the field must be replaced overnight because the security certificate that is legally/contractually required is lost, independent of the actual vulnerability status of the product and despite any risk mitigation plan that issuing authorities may put in place. The remedies to this are threefold:

- First, the issuing authorities should get all necessary information to assess the risks stemming from exploitable vulnerabilities of products in the field and to make the appropriate decisions, possibly including the implementation of external mitigation measures. The EUCC certification scheme does not provide tools to convey such information. Therefore, Eurosmart recommends formalising the outcome of the security monitoring activities of certified products into a new type of report one could name "vulnerability assessment report", independent of the certification decision.
- Second, identity documents may be used in the field even though their security certificates have been withdrawn (or AVA_VAN level and/or EAL decreased) or expired[16]. To assist issuing authorities in their risk management and conformity tasks, the information related to the security certificates should remain available without limitation. Therefore, Eurosmart recommends creating a permanent public repository of all security certificates with their status (valid, expired, withdrawn) and the list of the relevant documentation (e.g. security target(s), certification report(s), maintenance report(s), vulnerability assessment report(s)).
- Third, as the lifetime of identity documents usually exceed the validity of certificates, the EUCC scheme should also provide voluntary tools to maintain up-to-date security/vulnerability information of products which were certified but do not hold a valid certificate anymore.

Moreover, Eurosmart would support investigating the feasibility of a new type of certificate based upon a vulnerability assessment report, and that leads to the withdrawal of the initial certificate.

One approach consists in differentiating between products in the field and products put on the market in case an exploitable vulnerability is discovered:

- For products put on the market (not yet in the field), the security certificate should be withdrawn or updated in accordance with the EUCC certification scheme. The products would have to be removed from the market and thus not deployed;
- For products in the field, a different type of certificate would be granted to comply with legal/contractual obligations. This type of certificate would be bound to a vulnerability assessment report as proposed above.

However, as of today, it appears very complicated to introduce such differentiated management of security certificates within the EUCC certification scheme.

Eurosmart strongly recommends updating legal texts, such as regulations, directives and national laws, and contractual obligations so that (1) security certificates of products in the field could evolve and even lose strict conformity with the initial requirements, and (2) pragmatic risk management could be applied to the products in the field.

[16] In the EUCC certification scheme, a security certificate expires after 5 years.

4. Guidelines for managing the risks of exploitable vulnerability occurrence in software embedded in the chip of documents

This section provides guidance and recommendations for issuing authorities to manage the risks of exploitable vulnerability occurrence when procuring or purchasing software embedded in the chip of a document.

1/ Software embedded in the chip of document to be procured or purchased

The procurement or purchase of the product shall stop as soon as:

(1) the reassessment of the security certificate is not positive, i.e., additional restrictions of uses are added, or it shows security erosion, including decreasing of its AVA_VAN level,

or

(2) the security certificate has expired.

This implies that the procuring or purchasing entity shall organise the introduction of another product (or version) beforehand, meeting the expected security level (AVA_VAN.5), to have it ready and available.

Providers of software embedded in the chip of documents frequently renew their products to offer a new generation every few years. Issuing authorities should not hesitate to migrate to a more recent product whenever available. Such migration reduces the overall product lifetime and then risks attached to old products. Products being procured and purchased should be regularly renewed so that they are always recent and thus meet the expected security level (AVA_VAN.5). This renewal should be planned ahead of time, and the right frequency for the introduction of a new generation of products is typically three years, but it can be more. This timeframe corresponds to the time needed for the industry to introduce a new generation of products.

2/ Software embedded in the chip of documents that have been procured, purchased or that are being used in the field

As soon as the re assessment of the security certificate shows that the product does not meet the AVA_VAN level (resistance to vulnerability) identified in the initial security certificate, or when a vulnerability is exploited, the issuing authority shall carry out a comprehensive risk analysis. Based on it, the issuing authority shall set up a mitigation plan to fully thwart the identified risks or reach a situation where remaining risks are acceptable. This mitigation plan shall ensure the product's overall security is equivalent to the AVA_VAN level (resistance to vulnerability) provided in its initial security certificate, considering its effective usages, or maintain the remaining risks at an acceptable level.

a) Risk assessment

The risk assessment shall appraise the risks posed by the exploitable vulnerabilities identified by the reassessment of the product. This risk assessment shall be performed in the light of the effective usages of the product, which are only known to the issuing authority. Indeed, the risk assessment shall also rely on the inputs of the ITSEF[17] that has carried out the reassessment of the product.

[17] Information Technology Security Evaluation Facility.

The risk assessment shall help the issuing authority decide whether the risk(s) is(are) acceptable and can be managed. However, it may not always be the case, and sometimes the risk assessment may conclude that the remaining risk is not acceptable, and the product shall be withdrawn.

b) Mitigation plan

Based on the risk assessment, the issuing authority shall set up a mitigation plan to keep the product's overall security equivalent to the AVA_VAN level (resistance to vulnerability) provided in its initial security certificate. If not possible, it shall aim at reducing the risk to a level it deems acceptable and manageable. However, it may not always be the case, and sometimes the mitigation plan cannot reduce risks enough, making it necessary to withdraw the product.

The mitigation plan shall be built on the risk assessment, taking into consideration the effective usages of the product, which are only known to the issuing authority, and the inputs of the ITSEF that has carried out the reassessment of the product. For instance, if the risk assessment concludes that a functionality not being used is affected, a mitigation plan is not needed as the effective usages of the products are unaffected.

The purpose of the mitigation plan is to compensate for the security flaws that have been identified in the product considering its effective usage. This rebalancing may be achieved in several ways (which may be combined): using the product differently, restricting some usages, or applying use recommendations.

3/ Leverage on patching mechanism of chip-based documents

Some products may support a patching mechanism allowing to upgrade the software embedded in the chip of the document. It may be very useful to correct exploitable vulnerabilities in the software embedded in the chip of documents that have been procured, purchased or that are being used in the field. As such, a patching mechanism could help maintain their security level all along their lifetime. However, it may not always be technically possible to fix any vulnerability, especially when it relates to the physical characteristics of the embedded software (hardware design, new methods to exploit ancillary channels etc.), which cannot be corrected through software means.

Besides, the very long lifetime of identity documents (as shown in figure 1) raises very specific challenges, as a version of software embedded in the chip of identity documents may be in the field for much more than 12 years. Obviously, the risk of exploitable vulnerability occurrence increases with the age of the product and gets higher as it becomes old.

Reducing the validity period of the identity documents directly yields to suppress this highly sensitive period of the software embedded in the chip of identity document lifetime where exploitable vulnerabilities are likely to occur. Therefore, Eurosmart recommends reducing the validity of identity documents to five years to reduce the risk of exploitable vulnerability occurrence. This is particularly relevant for sensitive use cases such as QSCDs, authentication (inclusion provision of digital identity). For instance, this is acknowledged in the particular case of digital tachograph cards, as the maximum validity period is set to five years (Regulation 2014/165, Article 26(6)).

Conclusions

Legal texts mandating to use products having a security certificate must consider the particular case of products in the field having their security certificate withdrawn. If this case is not adequately addressed, it may result in major disruption of services and inextricable situations that the industry may face. eIDAS Regulation provides an example of such an inextricable situation when a product in the field – QSCD certified based on a security certificate – loses the latter.

Yet, it may be solved if national authorities in charge of QSCD certification adopt a pragmatic interpretation of Articles 30 and 39. Nevertheless, the way Regulation (EU) N° 165/2014 on tachograph cards is written should be followed as it clearly differentiates between products put on the market and products in the field. As of today, it is the only way to address this crucial issue.

Unfortunately, it appears very complicated to update the EUCC certification scheme to ensure that security certificates of products in the field remain formally compliant with the applicable legal and/or contractual obligations (in particular with regards to the AVA_VAN level and/or EAL) when a certificate should be withdrawn or is expired. Therefore, the security certification framework cannot help solving this issue. It must be absolutely handled through the applicable legal – including regulations, directives, national laws etc. - and/or contractual obligations.

The EUCC certification scheme should be updated at least so that issuing authorities have all necessary information (1) to correctly assess the risks stemming from an exploitable vulnerability of products in the field, and (2) when the latter could be managed, to put in place suitable mitigation measures. This could be achieved through a new type of Evaluation Technical Report (ETR), that one could name "vulnerability assessment report". In addition, expired and withdrawn security certificates should remain available at any time in a repository to support issuing authorities in their risk management and conformity tasks.

Simple measures can be applied by issuing authorities to (1) limit as much as possible the probability of having software embedded in the chip of documents in the field facing exploitable vulnerability occurrence and (2) handle it if it happens. Eurosmart proposes guidelines to achieve these goals, which recommends – amongst other measures – to regularly renew the embedded software (and the chip) used to produce documents. Besides, for the specific case of identity documents used for sensitive use cases, Eurosmart recommends limiting their validity period to five years.

Last but not least, risk assessment, risk management, and mitigation measures for software embedded in the chip of documents in the field are instrumental. Eurosmart proposes to work with NCCA[18] to set up a clear methodology for risk assessment and risk mitigation for that purpose.

[18] National Cybersecurity Certification Agency – pursuant to Regulation 2019/881.

Annex I
Landscape of legal obligations requiring security certification of chip-based documents

This Annex identifies the legal obligations requiring security certification of chip-based documents. In particular, it investigates whether these legal obligations mandate chip-based documents to have a valid security certificate at the time of issuance or usage (meaning at any time, and thus all along its lifetime).

1/ Legal obligations stemming from European laws

Security certification of chip-based documents is ruled by European regulations and directives as follows:

Document	Security certificate shall be valid at	Legal instrument
European Residence Permit	Issuance	REGULATION (EC) No 1030/2002
European passport & travel document	Issuance	REGULATION (EC) No 2252/2004
Identity card	Issuance	REGULATION (EU) 2019/1157
Driving license	Usage	DIRECTIVE 2006/126/EC
Digital Tachograph card	Issuance	REGULATION (EU) No 165/2014
QSCD	Issuance	REGULATION (EU) No 910/2014

2/ Legal obligations stemming from national laws

Some national laws provide for supplemental obligations regarding security certification of chip-based documents and mandate the security certificate to be valid at time of usage (meaning at any time, and thus all along its lifetime).

3/ Legal obligations stemming from contractual agreements

Some contractual agreements imposed by issuing authorities to their suppliers may also provide for security certificate of chip-based documents to be valid at any time (meaning at any time, and thus all along its lifetime).

About us

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

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, Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight, CCLab, CEA-Leti, Jtsec**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), 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 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, ECIL, ETSI, ECSO, 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