EUROSMART
The Voice of the Digital Security Industry

Feedback on the revision of the Driving Licence Directive

Introduction

The European Commission will carry out the revision of the current EU Directive on driving licences adopted in 2006[1]. The European Commission lists five key problems to tackle[2]:

1. Excessive number of road crashes with fatalities and serious injuries in which dangerous behaviour plays a role
2. Excessive number of road crashes with fatalities and serious injuries in which insufficient skills, knowledge and/or medical fitness plays a role
3. Lack of recognition of digital or virtual driving licences outside the territory of the issuing Member State
4. Remaining barriers for the citizens to obtain a driving licence or to maintain their driving rights when exchanging/renewing driving licences
5. Possible sub-optimal use of new technologies and mobility concepts for what concerns environmental performance

This paper proposes to answer these challenges in four complementary ways.

First, the revision should strengthen the security features of driving licences and hence reduce the number of forged licences through three key security measures:

1. Mandating a chip in European driving licences
2. High quality of the enrolment of the printed portrait and biometrics of the holder to fight lookalike frauds
3. Harmonisation at a high level of the physical security features to fight document forgery

Secondly, the revision should facilitate usage in another Member State by introducing a chip and a harmonised layout.

Thirdly, digital driving licences are on the rise, and the revision should take them into account.

Fourth and lastly, this revision would not be complete without the update of Commission Regulation 383/2012 to solve its shortcomings.

[1] DIRECTIVE 2006/126/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 December 2006 on driving licences

[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12978-Revision-of-the-Directive-on-Driving-Licences_en

I. Fighting forged driving licences to improve road safety

As explained by the EU Commission in 2013, there is a real relationship between the number of casualties on the road and the number of fake driving licenses: *"Fake driving licences are a licence to kill, that is why we need licences which are easy to read, easy to understand and very difficult to falsify"*.[3]

Thousands of unqualified drivers are putting lives in danger every time they use their vehicles.

They might have never passed any driving test, theory or practical. Many of them have limited knowledge about the Highway Code and little or no driving experience. They cheat either because the test is too hard, either because the test is too expensive -compared to a cheap fake licence- or because they are no longer legally allowed to drive due to a revoked or expired licence.

Once they have their paperwork done and their keys in the ignition, they have a "*licence to kill*". They may even rent and be in charge of buses or trucks.

Many of these illegitimate, dangerous drivers use forged licences. One single fraudster can put many unqualified drivers on the road.

Eurosmart has identified three measures to improve the security of driving licences and hence considerably reduce the possibility for fraudsters to forge licences.

Key security measure 1: mandating a chip in driving licences

A secure microcontroller chip with embedded software is by design protected from unauthorised access and used to store confidential and cryptographic data.

The secure chip brings several advantages, among them:

- Increase the productivity and facilitate automated controls;
- Assist in authenticity and integrity validation;
- Drastically reduce the risk of forgery;
- Allow effective control in any conditions (on a dark country road etc.)

The current Directive has introduced a set of harmonised physical security features and allows Member States to add new security features to enhance security over time. As a result, a heterogeneous mix of security features is used across the different EU Member States. Verifying these physical security features requires knowledge and training on the law enforcement forces across the EU, but also time and good conditions when verifying them (illumination etc.). Consequently, police may be at a disadvantage when verifying a driving licence from another Member State, introducing an opportunity for fraudsters.

Including the chip as a mandatory requirement for all Member States will introduce a shared and well-known advanced security feature, virtually impossible to counterfeit and easy to verify across Member States. Even a smartphone with NFC reader can read such an electronic document. This will reduce the number of fake driving licenses while increasing their ability to detect fake licenses.

In addition to ensuring the authenticity and integrity of the document data, the chip allows for securely storing citizens' biometric data (e.g., fingerprints) in addition to the printed portrait image and protects the access to these sensitive data from unauthorised readers.

[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_13_25

Terminal Authentication is the security mechanism that protects biometric data. It is part of the Extended Access Control[4] (EAC) protocol specified by German BSI. This protocol is used for the European biometric electronic passport and is also defined for the chip of driving licences as it is part of ISO/IEC 18013-3, which is the ISO standard defining the security mechanisms of the Driving Licence application embedded into a chip.

Terminal Authentication relies on a chain of certificates where the document issuer validates and signs the first certificate of the chain. The core mechanism relies on electronic signatures verified by the secure chip to grant access to sensitive data only to authorised inspection systems. At the end of the certificate chain, a dynamic authentication validates that the inspection system is the one identified and authorised by the last certificate of the chain. The security of this protocol is indisputable and widely recognised.

Once an authorised inspection system gains the right to access a citizen's sensitive data, it reads the biometric data from the chip and verifies the match between data from the chip and live data from the citizen. Biometry considerably increases the level of security by ensuring the citizen's indisputable authentication, therefore reducing the fraud and indirectly increasing road safety.

It is worth noting here that there is no need to store the biometric data in a database with such an implementation. In all cases, biometrics should always be introduced in full respect of applicable European laws, including data protection rules and the right to privacy.

The mandatory introduction of a chip (containing biometrics) would also bring the following advantages:

Security level alignment with national identity cards, travel documents and European residence permits

A driving licence equipped with a chip containing the holder's portrait and sensitive biometric data (e.g., fingerprints) would be aligned in terms of security with national identity cards, travel documents (e.g., passports) and European residence permits that are currently issued in Europe. As a result, a chip-based driving licence, aligned with other documents, would provide the same level of trust. All these documents contain a chip holding the holder's portrait and sensitive biometric data, as mandated by EU legislation.

As a driving licence can be used as an identification means, it must provide the same level of confidence as a national identity card, a passport, or a residence permit. Otherwise, driving licences remain the easiest target for fraudsters, who find it easier to counterfeit them than, for example, a national identity card. Reaching a consistent and high level of security across all identity documents in the EU is a priority.

This alignment is of the utmost importance because driving licences can also be used to prove identity for financial operations. For this reason, as well, driving licences are attractive to fraudsters. Driving licences with weaker security than national identity cards, travel documents (e.g., passports), and European residence permits may be an enabler for money laundering.

Protection of citizen's biometric data and offline verification

As described above, the Terminal Authentication protects the sensitive biometric data (e.g., fingerprints) against unauthorised access, and grants read access only to inspection systems approved by the issuing country or by authorities approved by the issuing country. This protocol ensures the privacy of citizens' sensitive biometric data.

[4] https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/SecurityMechanisms/securEAC/eac_node.html

In addition, relying on a microcontroller chip storage avoids the security threats with sensitive biometric data used online and stored in a central database or the cloud. In this respect, it also guarantees digital sovereignty over sensitive biometric data[5]. It also annihilates legal constraints associated with personal data registries.

Finally, the chip allows offline verifications, a must-have feature considering that some country roads can be without communication network coverage.

What kind of chip should be mandated for the driving licence?

The Directive should mandate a microcontroller chip and software compliant with ISO/IEC 18013.

ISO/IEC 18013 series defines a set of standards for an "ISO compliant Driving Licence" (IDL). It is made up of the following parts:

ISO/IEC 18013 Parts	Description
1	Physical characteristics and basic data set
2	Logical data structure, encoding rules and minimum mandatory set of features for the machine readable technologies
3	Security mechanisms of the Driving Licence application embedded into the chip: access control, document authentication and data integrity validation
4	Requirements to test the compliance of an ISO Driving Licence with regard to ISO/IEC 18013 part 2 and 3
5	Mobile driving licence (mDL) application

ISO/IEC 18013-5 specifies the mobile Driving Licence (mDL) application in ISO 18013-5. More details on this point are given in section III on digitalisation.

Mandatory compliance with ISO/IEC 18013-2, 3 and 4

Only ISO/IEC 18013-2, 3 and 4 are relevant for a driving licence, including the support of a chip.

ISO/IEC 18013-2 and ISO/IEC 18013-3 features are similar to ICAO doc 9303[6] electronic passport ones. There are some differences in the data encoding and information stored (defined in ISO/IEC 18013-2) as an electronic passport does not have data related to driving.

One of the main reasons to mandate a chip compliant with ISO/IEC 18013-3 is that it enables leveraging existing infrastructure and fostering interoperability in the EU. There are many similarities between ISO/IEC 18013-3 and ICAO doc 9303. In particular, the ISO driving licence uses the same security mechanisms[7] as the European electronic travel document (e.g., passport), European resident permit or national electronic identity card according to EU Regulation 2019/1157. Therefore, relying on ISO/IEC 18013-3 allows easily reusing and leveraging of infrastructures already deployed, not only for the inspection but also for the issuance. It will drastically reduce the investment for ministries of transport. Thus, as an international and recognised standard, ISO/IEC 18013-3 is the best choice to foster interoperability and recognition inside and outside the borders of the European Union.

[5] https://www.eurosmart.com/eidas-digital-europe-recommendations-to-strengthen-sovereignty-and-security/

[6] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[7] ISO/IEC 18013 part 3 specifies all security mechanisms of the ISO Driving Licence

Eurosmart recommends the revised Directive on driving licence to require the chip of the driving licence to comply with ISO/IEC 18013-2 and ISO/IEC 18013-3.

ISO/IEC 18013-4 are test methods meant to confirm the compliance of a product with ISO/IEC 18013-2 and ISO/IEC 18013-3. As such, it is crucial to eliminate any risks of incompatibility when reading a driving licence claiming compliance with these two standards. Therefore, the revised Directive on driving licence shall require the chip of the driving licence to comply with ISO/IEC 18013-4.

Mandatory security certification at level EAL4+AVA_VAN.5 pursuant to the Common Criteria

The Common Criteria certification scheme is very rigorous, has strong international recognition and offers one of the highest assurance levels (when the Evaluation Assurance Level is higher or equal to EAL4+AVA_VAN.5) for both the chip and the embedded software. Besides, mandatory security certification of chip and embedded software pursuant to the Common Criteria at level EAL4+AVA_VAN.5 (at least) is already required for other documents ruled by European legislation, such as electronic passport, national identity card, European resident permit, or Qualified Signature Creation Device (QSCD). Likewise, the revised Directive on driving licence shall mandate the chip and the embedded software used in driving licence to be security certified pursuant to the Common Criteria at level EAL4+AVA_VAN.5 (at least).

Last but not least, the new context stemming from the Cybersecurity Act (Regulation 2019/881) should be considered, whereby a European-wide recognition for Common Criteria security certification will be set up: the EUCC scheme. Therefore, it should be required that this security certification be performed in accordance with the EUCC scheme.

Relying on similar security mechanisms and protocols as ICAO doc 9303 also offers the possibility of reusing the same framework and supporting documents for the security certification of driving licences as those used for electronic passports. Therefore, the security certification of the chip and the embedded software used in driving licences shall be performed according to the same security models – called protection profiles - like the ones used for travel documents: BSI-CC-PP-0056-V2[8] or BSI-CC-PP-0068-V2[9].

Provide for pragmatic management of security certification of driving licence on the field

The revised Directive on driving licence should require chips (and embedded software) to be security certified **only at the time of issuance**. Requiring security certification of driving licences after issuance would create substantial legal issues for issuing authorities. Because of natural security erosion, vulnerability may appear over time, causing driving licences on the field to not meet the security level they met at issuance. Therefore, requiring security certification on the field would oblige issuing authorities to remove and/or replace overnight all issued driving licences as soon as a vulnerability appears, despite pragmatic measures that could be put in place to manage the possible risks.

The right approach consists in introducing specific provisions in the revised Directive to allow keeping on using the chip (and embedded software) in the driving licence on the field after a vulnerability has been detected, provided the issuing authority agrees to do so and adequate risk management and mitigation measures are put in place. It is essential to avoid making thousands or millions of driving licences on the field useless overnight because of a minor vulnerability.

[8] https://www.commoncriteriaportal.org/files/ppfiles/pp0056_V2b_pdf.pdf

[9] https://www.commoncriteriaportal.org/files/ppfiles/pp0068_V2b_pdf.pdf

Regulation (EU) N° 165/2014[10] ruling 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 on the field (or on the market):

Product to be put on the market

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 on the field (or on the market)

When a vulnerability is discovered on a product on 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 on the field when an exploitable vulnerability is detected.

Eurosmart recommends adopting the very same approach for managing the situation where a vulnerability is discovered on driving licences on the field.

Mandatory support of NFC

The driving licence should support NFC communication to ensure easy verification by a police officer or another official agent. NFC provides the best verification experience on a dark country road. Therefore, chips should be mandatorily equipped with a Near Field Communication (NFC) interface. In addition, NFC also provides a communication channel between the driving licence and a smartphone. It would allow easy importing of the licence data within the future European Digital Identity Wallet application.

Key security measure 2: high quality of the enrolment of the printed portrait and biometrics of the holder to fight lookalike frauds

On top of mandating a chip fulfilling the above-mentioned conditions, the revision of the Directive should set high-quality requirements for the enrolment of the (printed) portrait and biometrics of the holder. These requirements are currently missing, which entails, in particular, divergences across the EU in the quality of the holder's portrait printed on the driving licence. Fraudsters exploit portraits of low quality to impersonate someone else's driving licence, as it is hard to tell the difference between the printed portrait and the holder. Such fraud is called lookalike, where someone else tries to use someone else's document.

In order to fight these frauds, a portrait with high quality is needed to avoid impersonation. Such quality requirements will help better identification, either manually or using biometric authentication (e.g., for remote identity proofing), thus reducing the risk of lookalike frauds. In that regard, the CEN/TS 17661 -European enrolment guide for biometric ID documents (EEG) - should be mandated.

Key security measure 3: harmonisation at a high level of the physical security features to fight document forgery

Finally, the revised Directive should also harmonise the physical security features of driving licences at a high level. Such harmonisation would facilitate the work of police forces or private actors (e.g., car

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

rental companies) when they manually control driving licences while ensuring a high level of protection against document forgery and counterfeiting.

Making use of harmonised physical security features for European driving licences could help identify forged ones more easily, particularly when controlled by the private sector. Last but not least, it is important to make sure the physical security features of the European driving licence are commensurate with the ones of the other documents: national identity cards, European travel documents and European residence permits. European driving licence shall not become a loophole that all fraudsters would forge because its physical security features are less secure than those of other documents. Therefore, it is instrumental to harmonise the security features at a high level.

For this purpose, EU driving licences should comply with ISO/IEC 18013-1 Annex C "Document Security and Security Features".

II. Easing usage outside the issuing Member State

Facilitating use and renewal in another Member State through the chip

Introducing a chip in driving licences is not only an effective way of fighting forged licences but also a concrete measure to facilitate the usage of driving licences outside the issuing Member State. Thanks to robust security protocols, any Member State can easily ensure that an ISO-compliant driving licence is genuine and issued by another Member State. Furthermore, biometric data stored in the chip provides an indisputable authentication of the citizen. Therefore, the chip and biometric data facilitate the acceptance and trust of a driving licence from another Member State. In the case of passports, the introduction of the chip was instrumental in supporting easy inspection by other countries while maintaining a high level of trust and ultimately streamlining border crossing.

Moreover, the chip eases the creation of the new driving licence by importing the licence data from the chip issued by the Member State of origin. An ISO-compliant driving licence with a chip and biometric data facilitates the renewal when a citizen establishes his normal residence in another Member State by providing indisputable authentication and driving licence data.

Beyond the renewal of driving licences, the chip enables streamlining police control and eases usage in the private sector. The chip could be accessed to retrieve the data and the portrait in all these use cases. Such functionality would not only facilitate the rental of a car but also increase the security level of verification by private operators.

Harmonising the layout and visual aspect of driving licences

The revision of the Directive on driving licences is also a clear opportunity to harmonise further the layout and visual aspect of driving licences issued in the EU. Currently, the layout and visual aspects of driving licences issued by Member States are quite diverse, which impedes the ability to detect fantasy or counterfeited driving licences at first glance. In the same way as for European residence permits, the layout and visual should be further harmonised so that driving licences issued by each Member States look the same.

Such harmonisation would facilitate cross border usage. For instance, using a driving licence for car rentals or for proving identity could be smoother due to a harmonised layout. Besides, it would help fight fraud as genuine European driving licences could be easily identified at first glimpse, which is not the case today.

For this purpose, the European Commission should further clarify the content of Annex I of Directive 2006/126 to set a clear layout for the document. More particularly, Annex I should define the size and the location of each document area and align it with the layout defined by ICAO. The size and location

of the portrait (zone V) should be the one defined by ICAO. The colour to be used should also be better harmonised, in particular the pantone reference of the pink colour. At the moment, the colour scheme significantly diverges among Member States.

III. Supporting digitalisation of driving licences

The revision of the Directive on driving licences should also consider current evolutions towards digital driving licences and mobile driving licences according to ISO/IEC 18013-5. More and more, citizens have driving licences on connected devices (e.g., smartphones). Those digital and mobile driving licences should be usable in any Member State, as long as they comply with EU requirements.

An enabler toward the digital world

Remote identity proofing is an essential step in digitalisation, as it allows securely linking a physical person and its identity information. It is largely used in many different sectors as soon as a remote transaction is at stake: financial sector to fulfil the KYC[11] or anti-money laundering legal requirements, registration for a qualified signature service, enrolment for digital identity, etc.

By adding a chip, the driving licence would become a supplemental means to prove its identity online alongside an electronic identity card, electronic passport, or European resident permit through remote identity proofing. It would increase the outreach of remote identity proofing within the population by extending the number of people who could use it and ultimately enlarge access to the digital world.

Digital driving licences and eIDAS 2 go hand in hand

The revision of the eIDAS Regulation introduces the concept of the European Digital Identity Wallet. Every Member State will issue or recognise a European Digital Identity Wallet that will run on mobile devices. Concretely, citizens will be able to store in this Wallet their identity data but also attributes, attestations of attribute and credentials. The driving licence could be one of these attestations of attribute or credentials. Thus, citizens would have a digital version of their driving licence in their European Digital Identity Wallet.

However, because of the sensitivity of a driving licence, safeguard measures shall be defined to avoid any risks of fraud when issuing a digital version. First, only national authorities should be allowed to issue such digital versions. Secondly, the revision of the Directive shall also identify the specific requirements – stemming from the driving licence context and governance - to which the entities in charge of issuing such digital version should be subject. For instance, these requirements may encompass security aspects, governance aspects (e.g., service operated by a non-commercial entity) or technical aspects (e.g., storage and processing of data in the EU).

Accompanying the uptake of mobile driving licence (ISO/IEC 18013-5)

Being able to store a copy of its driving licence and use it from its mobile phone is more and more required by citizens. Many attempts have been carried out worldwide. The revision of the Directive on driving licences shall accompany this trend to avoid diverse implementations that would cause fragmentation within the EU and ultimately impede cross border usage.

ISO/IEC 18013-5 provides the technical specifications for the implementation of a driving licence in association with a mobile device. This standard is largely recognised worldwide for mobile driving licence implementation.

[11] Know Your Customer.

The revision of the Directive on driving licences should refer to this worldwide recognised standard, either in the Directive itself or in a supporting implementing act. The revision should also clearly state that mobile driving licences should be issued only by national authorities.

Digital and mobile driving licences as a companion to physical driving licences

It is worth underlining that digital and mobile driving licences should be the digital companion of physical driving licences, not their substitute. Thus, the use of digital and mobile driving licences should be voluntary, just like the use of the European Digital Identity Wallet, and the possession of a physical driving licence should remain the rule.

There are two good reasons to keep physical driving licences. The first one is inclusiveness. There are various levels of digitalisation across society, some citizens being less digitised due to a lack of skills or by choice. They should still be able to use physical driving licences. The second reason is resilience. There might be situations where the digital or mobile driving licence might not be usable, for instance, if there is a cyber-attack or if the holder's mobile phone is not available (no battery, lost or stolen, etc.). In this case, having the physical driving licence still in place provides resilience in the society and ensures holders can always show their driving licence.

VI. Fixing the discrepancies and shortcomings from Commission Regulation 383/2012

Correction of the contradictions in the standard referencing

Commission Regulation 383/2012 establishes technical requirements with regard to driving licences which include a storage medium (microchip). Unfortunately, this Regulation contains many shortcomings and would benefit from a revision.

Commission Regulation 383/2012 refers to ISO/IEC 18013 but actually (1) redefines many of its aspects and (2) mandates a patchwork of standards that ends up contradicting ISO/IEC 18013. In short, although this was not the initial spirit of the Regulation, chip-equipped driving licences compliant with Regulation 383/2012 are not compliant with ISO/IEC 18013!

The problem can easily be solved by directly referring to ISO/IEC 18013-2 and 3, instead of the current mix of standards.

Introduction of functional certification requirements

The revision of Commission Regulation 383/2012 would also be the opportunity to require chips to be functionally tested and certified in accordance with ISO/IEC 18013-4. This standard covers test methods meant to confirm the compliance of a product with ISO/IEC 18013-2 and ISO/IEC 18013-3. Such a new requirement is crucial as it would ensure the chip effectively complies with the applicable standards (ISO/IEC 18013-2 and ISO/IEC 18013-3). It would eliminate any risks of incompatibility when reading a chip in the course of cross border usage.

Security certification requirements

One aspect of Commission Regulation 383/2012 is worth maintaining; the security certification of the chip and embedded software should indeed be kept at Common Criteria level EAL4+AVA_VAN.5. However, it should be updated to take into account the recommendations described in the section "What kind of chip should be mandated for the driving licence?".

Conclusion

Eurosmart recommends that the European Commission bring driving licences into the 21st century by proposing an ambitious revision of the Directive. New security requirements, including incorporating a chip containing the holder's portrait and sensitive biometric data (e.g., fingerprints) and harmonisation at a high level of security features, would reduce the number of forged licences and considerably improve road safety. Combined with a harmonised layout, the chip would also facilitate cross-border usage of driving licences, including the renewal in another Member State. Finally, the revision cannot ignore the current trends toward digital and mobile driving licences -as a companion to the physical document, but also the consequences of the eIDAS 2 Regulation that will introduce a digital wallet.

The envisaged revision is ambitious and yet simple as the technical standards already exist: they can be found in the ISO/IEC 18013 series. Relying on these standards would not only ensure interoperability but also reduce the costs of implementation and ensure a high level of security. Last but not least, synergies with existing infrastructures for other types of documents (e.g., electronic passports, national identity cards or European residence permits) are possible. As a result, the implementation will be simplified, with limited financial impacts.

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**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, TrustSEC, 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