EUROSMART

The Voice of the Digital Security Industry

The future of European national electronic identity cards regarding to regulation proposal from the European Commission

"On strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement"

EUROSMART, OCTOBER 2018

Foreword

On the 17th of April, The European Commission tabled a proposal for a regulation to improve the security features of EU citizens' identity cards and residence cards with the aim at curbing document fraud.

Eurosmart and its members are fully committed in achieving the highest level of trust and security in particular in the fields of physical and digital ID documents. The Digital Security Industry welcomes the European Commission's proposal to set common security standards across the EU in the line with the ICAO requirements, and stresses the fact that facial and fingerprints data stored on a certified secure element, remains the best option to prevent bad uses and falsifications.

National ID cards and electronic passports are likewise used in Europe to travel, by embedding a harmonised contactless secure element storing the face and fingerprint biometrics will help to increase security within the Union

The proposal will contribute to reduce the space in which terrorists and criminals are able to operate by creating an interoperability between the different national ID cards, so that all the EU citizens can exercise their free movement rights in a harmonized and highly secure way.

We are pleased to see European Commission promoting technologies that are certified under the SOGIS MRA scheme in a such highly sensible use case.

The use of this secure technology opens the door to a wide spectrum of new features that could help both business and citizens in everyday life such as electronic identification, e-signature and trust services for electronic transactions in the internal market as set out by the 2014 eIDAS regulation.

The Following document presents the view of the Digital Security Industry on the future of electronic documents issued by national authorities in Europe. As part of the European Commission proposal on "Strengthening the security of identity cards of Union citizens", Eurosmart is pleased to address some technical points and to contribute to the debate.

Stefane MOUILLE
President of Eurosmart

Eurosmart's position

Eurosmart welcomes this proposal of regulation and in particular:

- The proposal to include the holder's portrait in the chip of the national identity card;
- The compliance of the national identity card and its chip with ICAO specification (ICAO Doc 9303);

Eurosmart calls upon:

- Not to over-regulate e-Government applications whose interoperability and interconnection issue has already been solved by the current implementation of eIDAS.
- Standardizing a secure 2D barcode, much easier and user friendly for the holder to capture with the camera of a smartphone than a MRZ, and add it on identity card, together with the MRZ.

Eurosmart fully supports the provisions related to security harmonization of national identity cards

Eurosmart considers that the content of the proposal is a good trade-off between (1) the need for a harmonized security level of national identity card throughout Europe, and (2) necessary subsidiarity allowing Member State to design their own identity cards.

No security is everlasting and Eurosmart calls upon a continuous improvement of identity cards' security against new frauds.

Eurosmart highlights that the biggest risk of fraud remains the lookalike in which a fraudsters uses the identity card of a genuine holder having the same face as him, leading to an impersonation. The proposal to include the holder's portrait in the chip of the identity card is instrumental to help fighting this fraud by allowing biometric authentication in case of doubt.

Last but not least, the proposal requires the identity card and the chip to comply with ICAO specification (Doc 9303). It is key to ensure interoperability of identity card throughout Europe but above all to ensure effective controls.

The EC proposal brings travel document and national ID document on the same security level and same basic data set, included biometric data.

Eurosmart calls for not regulating e-Government application

Eurosmart stresses that there is no need for this text to regulate in any manner the e-Government application as the interoperability and interconnection issue has already been solved, and calls for not regulating them. In contrary, any attempt to regulate e-Government application would deter Member State to support this text as it would result in major impact on their national digital identity and trust services ecosystem.

Eurosmart proposal on Emergency Passports

Many EU member states distribute two types of travel document, the regularly passport, typical valid for 10 years and the so called emergency passport, which have a validity of only 6 to 12 month. The regularly passport fall under the EU regulation EC/2252/2004 must have electronic security and must store electronic biometric data, since 2006. The emergency passport goes as blank document to the embassies round the globe and has no electronic security. Eurosmart see this as a weak point in the travel document policy of the EU Commission.

The European initiative to strengthen the security of national identity documents

The European Commission has unveiled on April 17th 2018 a proposal of regulation "*on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement*".

This proposal aims at enabling citizens of each Member States to fully exercise their right to free movement within the European Union as per the directive 2004/38/EC. This right implies that each European citizen shall be able to (1) cross the borders of any Member State and also (2) reside in any Member State using only their national identity document, i.e. national identity card or residence document (for foreigners) delivered by their home country, and not a passport.

The European Commission – through this proposal of regulation - acknowledges that citizens of Member States can't fully exercise this right as the risk of counterfeiting and falsification of national identity cards creates difficulties (1) when crossing borders and (2) when residing in another country to benefit from the same rights as nationals (access to public and private services).

Therefore, this text proposes a harmonisation of the format, security and content of national identity documents to lift these obstacles. Key factors for

Content of the proposal

This text proposes to regulate the format of the following national identity documents: (1) national identity cards, (2) residence cards for family members who are not nationals of a Member State, and (3) residence documents for union citizens. However this text does not deal at all with the conditions upon which these documents are delivered, which fully remains on the Member States' hands. It doesn't either require Member States to issue these documents : they remain free to issue or not any of these documents. In particular, it does not require Member State to issue national identity cards.

"*Residence documents for union citizens*" are documents containing identification data of the holder issued by the resident State. For this category of identity documents, the text only proposes to harmonize the identification data they contain.

"*Residence cards for family members who are not nationals of a Member State*" are specific resident permits, not covered by regulation on European resident permits (*Schengen Acquis*), and so far are only regulated by national laws. The text proposes to align the characteristics of this type of residence permit with the European resident permit. In particular it means that it shall (1) have the same format, (2) have the same security features, (3) contain the same holder's identification data, and (4) contain an ICAO compliant chip storing the portrait and two fingerprints of the holder.

Most dispositions of the proposal relate to the "National identity cards". The text proposes to (1) harmonize the format, (2) harmonize the holder's identification data, (3) add an ICAO compliant chip storing the portrait and two fingerprints of the holder, and (4) limit the validity period to 10 years. In particular the text proposes that national identity cards be in ID1 format (credit card format), and that the layout complies with ICAO requirements including a MRZ. On the other hand, the text still leaves the freedom to Member States to add an e-Government application in the chip of the national identity card.

Last but not least, for each of these documents, the text also proposes phasing out dispositions to ensure that in the mid-term (5 years), all identity documents that are non-compliant are replaced.

Main purpose : fight fraud on national identity cards

Amongst the three types of identity documents covered by this proposal of regulation, the national identity cards are the most critical because of the overwhelming volume currently in circulation (tens of millions), and their strengths.

The varying degrees of (1) security levels for national identity cards and (2) quality of identification data they contain throughout Europe constitute a major loophole. This said loophole is generating growing concern within the European Commission (EC) and Member States as it may be, and is, exploited by terrorists and organised crime (human trafficking, migrants,..) to cross internal borders but also external borders (to enter/exit Schengen area), taking advantage of the freedom of movement granted by national identity card. Official figures show the extent of fraud on national identity cards.

*"**According to FRONTEX while at the external borders passports are slightly on the lead, on the intra-EU/Schengen movements the ID cards are by far the most fraudulently document used.**"* (Source : Impact assessment accompanying the proposal of regulation)

"***At least three quarters of fraudulent documents detected at the external borders, but also in the area without controls at internal borders, purport to have been issued by EU Member States and the Schengen associated countries. In the second quarter of 2016, 74.33 % of false ID cards, 60.46 % of false residence permits and 17.11 % of false passports were EU documents (European Border and Coast Guard's quarterly risk analysis report).***" (Source : "Action plan to strengthen the European response to travel document fraud" - communication from the EC - 2016)

This loophole is also a great concern for any Member State as it can be exploited for more "regular" frauds they face. "Weak" identity cards are forged to create false identities in order to obtain other documents (passport...), Access and exercise undue rights (social benefits, employment, bank account...) And also to prepare crimes leading to money laundering and other such consequences. "Weak" identity cards also raise the question of how trustworthy Member States issuing such identity cards really are.

The approval of this regulation

This proposal of regulation allows Member States to also include a national e-Government application in the chip of the national identity card that may provide for instance digital identity and/or digital signature to citizen for national purposes.

The current state of play of national identity cards within Europe shows a general trend for adding an e-Government application as soon as the identity card is equipped with a chip. However, the landscape of national e-Government application is very heterogeneous. Nearly each State has its own e-Government application (ITA, BEL, EST and DEU are all different) on which a complete national ecosystem has been built.

This situation is not expected to change as the issue of interconnection and interoperability of national e-Government application throughout Europe has now been solved. eIDAS regulation has acknowledged the principle that digital identity shall be interoperable at the back-end system level (through eIDAS nodes), and not at the identity card level. Furthermore, from September 2018, notified digital identities (under eIDAS regulation) shall be recognized by all the Member States. As a matter of fact there is no need for this proposal to regulate in any manner the national e-Government application as the interoperability and interconnection issue now is solved.

Changing a national e-Government application would imply numerous consequences on the national ecosystem, spanning from the middleware, the identity provider infrastructure, the identity validation platform, the identity acceptor infrastructure, the trust services providers,…. impacting both (1) the State issuing the national identity cards, and (2) the private sector (using the digital identities and trust services). It means a new IT organization, millions of euros of investment both for the State and the private sector, and above all, succeeding in embarking again the private sector which is an essential stakeholder.

Therefore, the national e-Government application shall not be governed by this regulation to come, but on the contrary shall remain under the sole control of each Member State. Any attempt to regulate the national e-Government application would deter Member States to support this proposal as it would result in major impacts on their national digital identities and trust services ecosystem.

Opportunities for Member States

This proposal for a regulation is a key opportunity for Member States to enhance their national identity cards, in particular to (1) ease mobility of citizen within the union and (2) give them access to new and better digital services.

Easing the mobility of citizens within the union relies on strengthening the trust put in the identity card itself. In particular, it implies ensuring the identity card (1) can be easily and swiftly controlled with a high level of confidence, and (2) is secure, meaning is hard to counterfeit (creation of a copy of a genuine document) and falsify (tamper with a genuine document), and.

Ensure effective control of national identity card within the European Union

Authorities across the European Union (EU) suffer from an excessively wide variety of national identity cards (more than 60 models) making it increasingly difficult for them to differentiate between a genuine, a counterfeited, or falsified document. There is a growing need for authorities and organisations within the EU to be able to swiftly and effectively control national identity cards issued by Member States with a high level of confidence, thereby facilitating control procedures and strengthening security throughout the European Union. In the current climate, the necessity for an accurate, swift and cost effective, control method is stronger than ever. It is worth considering what has been achieved in terms of harmonisation of the European Resident Permit (ERP) that can, by some measure, be considered as a form of identity card for Third Country Nationals (TCN). Appearance, security and content of the ERP have been defined and ruled by the European Commission (EC) and the document has a unified format, layout and security features thereby enabling Member States to easily check its authenticity. Today, the ERP acts as the identity card for Third Country Nationals as ruled by the EC and, unlike identity cards, the ERP can and is easily controlled by any Member State within the EU.

Strengthen the security of identity cards

The security of a document is not everlasting. It is only valid for a given lifetime which is the time required by fraudsters to get access to the required technology and to learn how to use it.

An example is the case of regular hologram. At the beginning of their introduction the technology required to produce them as well as the expertise was only available to very few and trustable industrials. Therefore the security brought by this technology was strong at that time. Today, this technology is widely diffused and available to nearly anyone. It became very easy to counterfeit or even falsify genuine hologram and use them to produce false documents. It is exactly the same for any security features used in identity documents.

Therefore, it is key to regularly review the security of identity cards to (1) assess the strength of security features against falsification and counterfeiting, and (2) upgrade them if necessary. In particular, it means that new security features shall regularly be introduced to always stay ahead of fraudsters in term of technologies and expertise. This is the price to pay to ensure identity cards remain secure.

Based on the circumstance, that today EU citizens can travel outside and inside of the Schengen area without biometric passports, it is important to start this migration from visible ID document to electronic ID document as soon as possible. Some examples for travel into Schengen w/ ID-cards are

- French citizen from Morocco to France
- German citizen from Turkey to Germany
- Polish citizen from Ukraine to Poland
- Greek citizen from a Greek island to mainland

Give citizens access to the digital world

Adding an e-Government application in the chip of the document enables bridging national identity cards and digital services. The e-Government application allows giving citizens an easier and dematerialised access to the online world thereby allowing them to prove with a high level of trust their identity online (digital identity) and to enter legally binding agreements (digital signature) while protecting their identity and personal data.

This approach has two major benefits. First, citizens are already used to obtain and use national identity cards - as it is a part of their everyday life – which increases the acceptance of digital services across the population. Secondly, national identity cards usually have a very high penetration rate amongst the population allowing digital services to reach a larger part of the population.

Despite digital identity and digital signature may be seen completely disconnected from a national identity card's primary usage, many Member States have opted for these additional functionalities because of the largely beneficial impact they represent in the eyes of their citizens.

Today's State duty is not only to protect their citizen and secure their transactions in the real world by delivering them a sovereign identity, but goes now beyond. With the advent of the digital world, each citizen shall also have the right and the means to securely access the online world with a high level of trust and privacy protection. It implies providing to citizen a secure digital identity, and a way to securely enter legally binding agreements while protecting their identity and personal data.

Move from e-Government to m-Government

Most countries offering digital services on their national identity cards do so through a contact interface that entails having a small contact plate on the card, just like the one on a bank card. It represents a major hurdle as it requires the user to possess the relevant software and card reader - which implies to only use the national identity card with a computer (laptop or desktop), making it a very 'heavy' and non-user-friendly feature from a citizen's perspective. It hampers the widespread development of digital functionalities through identity cards.

Today, the current generation of smartphone can solve the convenience issue but also reshape the user experience. Near field communication (or NFC) technology allowing contactless communication with mobile devices (e.g. smartphones) overcomes

the hurdle of the contact interface. It has two major consequences that have the potential to revolutionize the identity card usage when providing digital services.

First, using one's identity card with one's smartphone through contactless is possible without any particular device (reader) or software configuration issues thanks to NFC. It becomes seamless and easy to access digital services.

It also allows shifting usage from a computer to a mobile phone. This shift is key from a user friendliness prospective. A smartphone is an extraordinary tool enabling easier access to digital services for everyone. The very nature of smartphone offers a much better digital inclusion: (1) people always have their mobile with them, (2) they know how to use it unlike a computer or at least find it much more handy to use, (3) the mobile network coverage allows reaching much more person than with a fixed network accessible through computer, and (4) penetration rate of mobile phone is higher than computer's. As a matter of fact smartphones are instrumental to foster the development and usage of digital services by enabling most citizens to access them, and also making them easier and seamless to use. Ultimately, it allows offering value added services for the citizen, as well as promoting citizen inclusion. This new paradigm has a name: m-government – relying on mobile - unlike e-government relying on computer. Undoubtedly the combination of NFC technologies and smartphone will revolutionise the development of digital services to citizen, available and secured through identity cards functionalities.

The market of smartphone is very quickly evolving due to two major trends: (1) extinction of "regular" phone replaced by smartphone, and (2) the advent of NFC enabled smartphone able to communicate through contactless with other devices. According to a survey from IHS technology, NFC will be included in 64% of the mobile phones shipped in 2018, up from 18.2% in 2013. Furthermore Apple has announced in May 2018 that it would open the access to the NFC API of iPhone to application developers. Combined to the life time of smartphone, it means that within the next 4-5 years, the overwhelming majority of smartphone in the field will be NFC enabled.

Thus in order to access the m-government world, national identity card should offer digital services through a national e-Government application usable in contactless.

Ease the usage of the chip using a smartphone

The access to the content of the chip of the identity card requires unlocking the chip, either by using (1) a PIN only known by the holder - when using the e-Government application, or (2) an information printed on the document - for ICAO or e-Government application - usually the Machine Readable Zone (MRZ). However, capturing the MRZ using a camera of a smartphone may be challenging for both the user and the smartphone application. Many factors may impede a swift, easy and user friendly capture of the MRZ by a user with a smartphone : the lighting conditions, the light reflection on the document, the distance, the positioning of the camera,….An alternative method shall be designed, able to eradicate these issues, and being easy, swift and user friendly.

2D barcodes have proven to achieve this goal. They are today used across a wide range of use cases in which they are captured and processed by smartphone and for which users learnt how to handle them.

Therefore adding a 2D bar code on identity card could be a strong factor to increase user acceptance and user friendliness. It only requires defining a format and a location through a standard. However, it shall be kept in mind that adding such barcode on identity card should not lead to the removal of the MRZ which shall be kept both for ICAO compliancy and backward compatibility.

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 manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART

The Voice of the Digital Security Industry

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | www.eurosmart.com