November 2015

The Future Digital Identity Landscape in Europe

Table des matières

Executive Summary

This document presents Eurosmart 2020's vision about Digital Identity in Europe: the definition, main trends, future requirements, evolutions and associated standards, as well as the workings of the European smart security industry regarding future challenges that should be addressed when implementing the eIDAS Regulation (910/2014) and preparing a bridge with other regions in the world, such as the U.S. (NSTIC project) and/or the Mediterranean region.

According to Eurosmart, Digital Identity is "the sum of electronic identification plus electronic authentication."

Electronic Identification is defined as "who I am" and electronic authentication as "this is the proof I am the person I claim to be".

Introduction

Digital Identity covers several aspects, such as economic growth, competitiveness and also cyber security, as Digital Identity is key to any IT information system.

These horizontal aspects have an impact on all the actors of the State-Nation architecture, from citizens to central administrations, local authorities, the private sector and consumers.

This topic of strategic importance has been embraced by several leading countries in Europe since the beginning of the 2000s.

Already in 2015, Digital Identity has been massively implemented by governments across Europe: **21 European Member States** are now issuing national eID documents. 20 of them are proposing secure electronic identification, authentication and digital signatures to hundreds of thousands of online services using the Internet, tablets and mobile devices.

More than **150 million** eID documents are in circulation today, capturing more than **30% of the total European population**.

Market penetration rate is close to 100% in some countries, such as Belgium, and reaching half of the population in large countries such as Germany.

This Digital Identity deployment trend is now progressing more quickly, helped by several initiatives from both the public and private sectors.

First, the regulation on electronic identification and trust services for electronic transactions in the internal market entered into force on 17 September 2014 (eIDAS Regulation), providing 500 million European citizens with a clear, legal and stable framework for electronic identification, electronic authentication and the associated trusted services. Furthermore, it establishes the mutual recognition and acceptance of electronic identification and authentication across borders, laying down the grounds of European interoperability.

Second, some major private sector initiatives were launched by mobile telecom operators such as the Mobile Connect solution, providing a worldwide interoperability of electronic identification and

authentication, and by web giants such as the Fast Identification On-line (FIDO) specifications released in December 2014.

Finally, handset manufacturers have embraced the Near Field Communication (NFC) contactless technology for mobile payment, as well as for Digital Identity Management.

These macro market trends demonstrate that Digital Identity is at the heart of the digital economy, but also at the heart of societal concerns such as data protection, data ownership, behaviour prediction and, in the end, who owns of the Digital Identity of 500 Million European Citizens sharing the same values of freedom and protection of private property (material or immaterial).

What will be the future evolution of electronic identification, authentication and signatures?
What will be the driving force or forces for Digital Identity? This document will provide answers to these questions.

Future trends in Digital Identity

The **Digital Agenda** addresses all relevant aspects of a European citizen's daily life: Shopping 24/7, car share booking via smartphone, online activity on social media platforms, online banking at home, government web services, telemedicine over long distances and many other services demonstrate this trend today and in the near future.

On the other hand, we see an increasing discussion in the public domain about **Big Data** (previously named Data Mining) and on **citizen profiling** on the Internet, tablets and mobile devices, and, very soon, in smart objects and connected cars. These devices and their related networks create a new territory: cyberspace.

Big Data means more and more data about citizens is publicly available – and much of this data is identity-related.

Cyberspace plays a major role for citizens, and also for developing new business models or increasing the existing ones in both the public sector and other sectors such as energy, the automotive industry, production plants and healthcare.

Securing transactions in cyberspace is critical to the economic prosperity of Europe, but also to protecting and promoting European values.

A secure and trusted Digital Identity is a key element in the digital world, as cyberspace plays an increasingly significant role when moving from the real world to the digital world. **Electronic Identification** and **Authentication** of the user forms the basis of trust in the cybersecurity of all IT systems. In the past, citizens were physically in front of a service provider (e.g., at a shop), but today – and especially in the future – this physical process will not always exist.

For this reason, a secure electronic identification and authentication framework, such as an **electronic ID-Document,** could capture all relevant needs for **privacy protection**, **convenience**, **efficiency**, **ease of use**, **security**, **confidence** and many other requirements in the digital world. In order to provide an appropriate level of security, the digital identity shall be either issued or trusted by a government.

Other initiatives than eIDAS legislation may have an impact on the "marketplace" in Europe in both the public and private domain, in particular:

- **NSTIC** in the U.S.
- **FIDO** and **Apple Pay** (from the private sector)
- **GSMA Mobile Connect.**

Private initiatives are mainly focused on business cases. Public initiatives may address both public and private sectors and enable private players to benefit from the know-how and trust of governments in terms of the security and protection of citizen.

National ID documents are amongst those with the earliest introduction in the area of governmental documents. Their initial purpose was to reliably verify the identity of a physical person, typically in front of a government official or in the case of a transaction requiring a trusted proof of identity, e.g., when opening a bank account. The main purpose of ID documents more than 200 years ago was for travelling [2]. The main purpose of eID documents in the future will be for online services, i.e., within cyberspace. Embedding a secure element into such an ID document, thus making it an eID card, was a logical step to increase protection against forging, counterfeiting and falsification, and so improve the reliability of authentication based on the eID document.

Electronic ID documents are based on four pillars:

- A secure element
- Secure card body
- Biometrics data
- Cryptography mechanisms.

Beyond the first generation of eID documents, today's second generation needs to extend its reach: with today's widespread online services and the ubiquitous presence of networked devices like computers, tablets and smartphones, the need for reliable and trusted authentication in the virtual world has become even more important than in the physical world.

Since online authentication is based on digital protocols and cryptographic algorithms, the secure element in an eID card becomes more than just an additional security feature; the secure element is now itself enabling the online identification. In order to prevent identity theft, it will have to be common practice to base online authentication on two factors: the eID card as a physical token ("to have") and a PIN or password as the secret knowledge ("to know"), or a biometric sample ("to be") used as the commonly known 2-Factor-Authentication (2FA). The 2FA-technology, completed with proven tamper-resistant device (like a certified secure element), addresses the highest security assurance level.

Based on the fact that around 17 million citizens in 2014 live permanently outside their home country, and given that this number will continue to increase by 2020, online services for cross-border purposes hold an important place in the future.

Given the landscape changes, acquisitions and bankruptcies in the area of commercial enterprises, people are looking for stability, trust and consistency when it comes to the source of their online identity.

Already entitled to hold all citizen identities from birth onward, national governments are seen as an independent and unbiased source of identity, also avoiding conflicts with commercial interests from private identity providers. Hence, national eID cards will be perfectly fitted to provide virtual online identity for the ever-broadening set of online services, both private and governmental.

However, secure national eID documents in smartcard form will not be enough in the future

With the increasing penetration of mobile networked devices like tablets, smartphones and wearable technology, people will expect more flexible and more convenient ways to securely identify themselves. By carrying a smartphone around the clock, which is nothing less than a full-fledged networked computer, people will also expect to use these devices as carriers of identity. With embedded security containers, based on the same secure element technology as in the eID card, and protected ways to enter a PIN or password, the smartphone itself will become the carrier of the holder's identity.

In order to ensure this convenience, governments have already been investigating whether a temporary ID can be derived from the original eID card directly into a smartphone just by tapping the card on the smartphone's reader. This derived identity might be valid for a few weeks only, and may be restricted to base authentication scenarios such as online shopping from the smartphone. The same, of course, is true for wearables – why not prove your age just by holding your smart watch or fitness tracker up to a vending machine?

A core demand for online authentication will be to respect privacy. With various personal data stored on an eID card or in a smartphone as part of a derived identity, the citizen as holder of the card wants to be sure that only the data necessary for a certain authentication will be disclosed to third parties – e.g., age verification needs to answer "yes" or "no" to a request about whether a person is of a certain age, but does not need to reveal the exact birth date. A postal address is necessary to receive a shipment of goods ordered online, but the person's marital status is of no concern to the vendor. The citizen expects to be empowered to decide by himself which data to disclose and which not to. The eID carrier will need to offer respective configuration options under full control of the holder.

In addition to privacy concerns about an individual service, privacy concerns across different services are also an important element. Even if data obtained from different service providers – e.g., from a data breach or as part of a merger – the individual IDs must not be matchable by unique ID numbers or a similar criterion. This requirement can be implemented through so-called "pseudo-IDs", changing personal identifiers for each individual service used by a single user and from a single eID card. Respecting all these privacy demands will require inclusion in the eID itself as a mandatory part, impossible to circumvent or disable from the outside, thus "privacy by design".

Many governments today have already been investigating or planning such future eID schemes. A core requirement for citizens to build trust in, and for industry players to develop and offer, these solutions is to create the necessary underlying legislation. Only by adopting respective regulations for such trusted, secure and convenient future eID schemes can a framework be laid down. Here, of course, lies the main challenge for governments today.

New online services are emerging every day, yet the outdated and insecure username-password identification scheme still prevails.

The speed with which the private sector is acting is tremendous, while governmental legislative processes typically progress at a far slower pace. Governments will be urged to act more decisively and be more focused in order to provide their citizens with eID schemes as trust anchors for the emerging

online world. A lot of work still remains to be done here; yet promising initiatives like the European Union eIDAS regulation and the U.S. American NSTIC [5] initiative have already emerged as good examples for such future legislation desperately needed in the public domain.

Activities in the private field can impact the public sector. Two examples in the past:

SuisseID, Switzerland
Since 2010, this eID document has been issued to citizens from four authorized private trust centers in Switzerland and supported by the government, e.g., the Federal Police [3]. The SuisseID can be used as a 2FA-token for online services as electronic identification, authentication and signature in the public sector as well as in the private domain. The SuisseID document is voluntary for citizens in Switzerland and is a companion to the national eID-Card.

BankID, Norway
The BankID is used by the Norwegian Banks' Payment and Clearing Center (Nets). The BankID Digital Identity solution runs on a secure SIM-Card in mobile phones and can be also used for payment of any services in the public domain [4].

Both examples show a collaboration between the public and private domains. Private companies are responsible for the selected security level for services and business cases. Government officials also accept this approach for services in the public domain. It is a very interesting case where secure elements are used in the mobile ecosystem.

The future will involve creating several Digital Identity companion concepts with different form factors and device supports, but the "Root of the Digital Identity" will remain the official electronic document issued by European Member states, as it is today with the Know Your Customer (KYC) regulation.

Future requirements of Digital Identity

Requirement number one: Freedom to travel.

Freedom to travel across the European Union is of major importance. Travelling across Europe requires a cross-border interoperability. This interoperability has been created thanks to a common standard for identification at border checks. This standard is known as eMRTD (electronic Machine Readable Travel Document Standards).

The European Member States have established Automatic Border Control Systems (ABC-Systems) at airports, railway stations and harbours to cope with the ever-increasing number of travellers.

Future eID documents need to be compatible with electronic Machine Readable Travel Document standards (eMRTDs) to allow integration into these systems. With the increasing capabilities of document forgers, cryptographic security and the possibility to verify it everywhere will become more and more important. The necessary information for verification, such as CSCA certificates, must be made available by the issuing countries.

Requirement number two: Interoperable Digital Identity Standard.

Citizens require reliable and privacy-by-design identification not only in the physical infrastructure, but also in the cyberspace world.

Companies are failing to protect the data of their customers or using it in inappropriate ways. As in the physical world, governments have an obligation to protect their citizens from identity theft, abuse and fraud. Governments would like to offer their services over the Internet – and for that, a method of identification is required that offers interoperability and security and follows the principle of privacy by design, keeping the citizen in control of his or her data as much as possible.

A common standard of identification is necessary to enable cross-border use of eGovernment services. The eIDAS Regulation 910/2014 and the eIDAS Token standard, aligned with European Standards (CEN TS 15480, EN 419 212), offer a unique opportunity to establish such an identification scheme in Europe.

Requirement number three: Limit the footprint of the user on the Internet.

Big Data

Three stakeholders have different points of view and different interests regarding Big Data:

- Citizen: privacy, data protection and the right to be "forgotten" on the web
- Industry: direct marketing, individual offerings, increasing customer lists, etc.
- Government: search and detection of criminal activities.

Profiling of citizens

Each activity in cyberspace creates a "footprint" of a citizen. Two examples illustrate this in a simple way:

- **Newspaper, user profile**

  If a citizen buys a newspaper at a kiosk on the street, everyone assumes the reader's behaviour is anonymous, i.e., nobody counts the time spent on a page or which page the user is reading. However, if the citizen orders an online newspaper, the issuer can collect a profile of the user, including an overview of the current areas of interest, e.g., politics, sports, culture, etc. The simple way to do this is to set up a monitoring process to review how long the user has opened which pages.

- **Payment, user profile**

  If a citizen gets money from an ATM, nobody would know where or how this citizen uses the money, i.e., the type of banknotes used at which place and for what purpose. In the case of an online payment, every transaction can be monitored with a computer. When a payment that is outside of the "normal profile" of a given citizen is started, a computer can send an alert to the bank or to the credit institute in real time. The user can be contacted to check if the bank or credit card was stolen or lost.

Both examples show one important aspect: Every activity of the citizen which moves into the web service area can create a "digital footprint" of the user. This means that services that guarantee anonymity as part of the privacy of the citizen are required. International standards on this are available (see also chapter 5) and many references are related to the issuing processes.

The following tables aim to synthesize the eID requirements of all stakeholders.

Individuals	Citizens	Consumers	Internet users
Requirements	▪ Freedom to travel across the EU. ▪ Protection against identity theft. ▪ Ease of use. ▪ Convenience. ▪ Interoperability of eAdministration services.	▪ Trust in electronic transactions. ▪ Personal data protection. ▪ Privacy protection (no tracking). ▪ Fraud protection. ▪ Convenience. ▪ Clear user consent.	▪ Freedom to browse on the web. ▪ Child protection (safe chat). ▪ Personal data protection. ▪ Privacy protection (no tracking). ▪ Protection of eReputation. ▪ Protection against digital harassment.

Service providers	Public SP	Private SP
Requirements	▪ Possibility to use cloud computing in security. ▪ Assurance level of authentication compliant to the needs. ▪ Savings, thanks to more dematerialization.	▪ Trust in electronic transactions. ▪ Interoperability, whatever the identification and authentication means are. ▪ Clear definition of rights and liabilities. ▪ Savings through fluidity. ▪ Provision of new services with higher value.

eID providers	Public eID providers	Private eID providers
Requirements	▪ Ease of notification to the EC in the context of the eIDAS. ▪ Trust in electronic identification means notified by other Member States.	▪ Reliable business model. ▪ Clear definition of rights and liabilities.

Future Digital Identity Standards and related applications

Facing global deployment, mobility and connectivity, there is an obvious need for standardization of the Digital Identity.

Existing standards such as the ICAO 9303 eMRTD, defining a global, standardized and interoperable eTravel documents ecosystem – or like GSM in telecoms or EMV in banking – demonstrate that massive deployment of interoperable identities can be done successfully.

These standards are all based on the Secure Element, as the data stored needs to keep its integrity as well as be protected from potential attacks in a "hostile environment", and the loss of this data will create important financial or security dangers.

International standards can be classified in three groups:

- Technical (or technological) standards, like ISO/IEC 7816 or ISO/IEC 14443. These standards define a global and general scheme for any type of application.
- "Application" standards, like ICAO 9303 (ISO/IEC 7501 (for travel document)) or ISO/IEC 18013 (Driving License). These standards rely on the technical standards, but define a comprehensive and exact field of application within an interoperability framework.
- Industry standards such as Global Platform (Secure Element and Secure Trusted Executed Environment), W3C (for the Internet), G3PP (for 3G/4G mobile communication).

Standard in 2015

At the end of 2015, many important international standards were created, made publicly available and put in use. Some examples of key standards on electronic ID documents:

ICAO 9303 (ISO/IEC 7501) for travel documents (worldwide)
More than 110 States worldwide issue electronic passports with biometric data compliant to ICAO. In Europe (since 2006), all 28 Member States issue travel documents according to EU Regulation 2252/2004 and the ICAO standard. This standard is also in use for other types of documents like National eID cards (Albania, Sweden, Monaco, Lithuania, Germany, Turkey, etc.), and Electronic Residence Permits (28 EU Member States as required by Regulation 380/2008 as well as 40 other States worldwide).

European Citizen Card (Europe)
The CEN TS 15480 (European Citizen Card) framework and its eIDAS token implementations constitute the reference for electronic identification, authentication and electronic features. This standard is in use by numerous Member states; for example, the eID cards in Germany, Bulgaria, Cyprus, Slovakia, Sweden, Portugal, Belgium, Monaco and Lithuania, as well as the healthcare card in France, Slovenia and Romania.

e-Driving License (Europe)
An ISO/IEC technical specification [9] on an electronic driving license was published in combination with the EC recommendation EC/383/2012. At the end of 2014, four countries issued electronic driving licenses: Ireland, the Netherlands, France and Croatia.

Trusted Identities in Cyberspace (USA) may create a set of industry standards
In April 2011, the White House started an initiative called the National Strategy for Trusted Identities in Cyberspace (NSTIC). Since 2011, a National Program Office (NPO) has been established by the Secretary of Commerce [5]. NSTIC addresses services in cyberspace in both the public and private domain. NPO works with academia, industry, advocates and government agencies like the Department of Homeland Security (DHS) and the White House. The NSTIC program covers the identities of individuals, organizations, networks, services and all devices involved in online transactions. One particular goal of the NSTIC program is to reduce the use of dozens of different usernames and

passwords. From 2012-2014, more than 10 pilot programs were started in the U.S. based on different industry standards or proprietary solutions.

Future of standards – time window 2015-2020

ICAO 9303 for travel documents (worldwide)
Since 2012, ICAO and its related working groups – like the Technical Advisory Group (TAG), New Technical Working Group (NTWG) and especially Task Force 5 (WG3/TF5) – are in standardization phase on the fourth generation eMRTD, named LDS2.0 [6]. The LDS2.0 will provide the opportunity for governments to digitize the content of visa pages with electronic visas, entry/exit stamping for border crossing or additional biometric data.

It is expected that this new standard will be achieved in 2015, as well as a pilot.

eIDAS Token (Europe)
Taking into consideration the eIDAS Regulation, some governments and industry players have developed an ecosystem to answer the challenges of the regulation by publishing an eIDAS Token specification and ecosystem based on the TR 03110 [10] defining protocol and interoperable profile. The ecosystem also encompasses a conformity and interoperability test framework, as well as a protection profile, to assess the high level of assurance. Furthermore, eIDAS Token features are being incorporated to the official European standards by CEN (as EN 419 212).

In addition, the eIDAS Token specification includes the framework to achieve qualified and advanced signatures as defined in the TR Signature [11], as well as biometric authentication defined in TR Physical User Authentication [12].

These standards ensure secure citizen authentication using a secure server signing solution granting mobility for citizen by accessing anywhere anytime the Qualified Trust Services.

e-Driving License
ISO/IEC JTC 1 SC17 WG10 focuses on a mobile driving license, proposing a “tour d’horizon” of the pilots or projects that are using smartphone technology as an alternative to a physical driving license. Pilots exist in the United States, bringing convenience to citizens but raising questions related to legal issues. This approach could allow online verification of a driving license in the street without any printed or tangible documents, like the electronic boarding passes used by some airlines in Europe.

New standards from private initiatives

The private sector, driven by fast-growing digital markets requiring identification and authentication, develops solutions at a faster speed than government legislation. It makes sense to observe and take into account such solutions that can become de facto official standards.

Identity Derivation
Some private actors are looking to issue secure and trusted identities for their own uses and under their own brand name. Deriving a secondary trusted identity from an initial trusted identity (such as an identity card) is currently being tested in some pilot projects. The support can be a dedicated token or a virtualized mobile identity. This is, for instance, the case in Iowa (USA), where having secure driving license information in a mobile phone is being explored. A recent NIST publication (Special Publication (SP) 800-157) addresses the need to derive a PIV credential in a smartphone or a tablet for remote access.

Fast Identity Online (FIDO)
In July 2012, FIDO (industry initiative) published technical specifications for strong authentication as well as for risk-based authentication [7]. It defines an open, scalable and interoperable set of mechanisms with the aim of reducing the use of passwords for the authentication of users. The 1st use case moved into the payment field by means of a smartphone payment made with a fingerprint in the PayPal frame using a shared, unique cryptographic public key stored on a embedded secure element.

Apple Pay
In September 2014, Apple announced a payment system using only a single touch on devices such as the iPhone6, the Apple Watch and the iPad [8] in combination with the use of NFC technology. At this time, such payment services are available only at select locations in the U.S. -- for example, at gas stations, in fast food restaurants and retail stores.

Mobile Connect
Mobile Connect is the online identity solution from Mobile Network Operators and defined by GSMA. The basic principle is to use a SIM card as a secure vault for storing the electronic Identification and Authentication and use the Mobile Operator Network to provide a trusted Digital Identity to e-services from either the public or private sector.

Harmonization, interoperability and synergies

Eurosmart would like to highlight some key points on eID documents issued by governments, but also on Digital Identities whose form and support may vary depending on the policy of the issuer, from either the public or the private sector.

eID documents
A convergence of policies is suitable, for instance in regard to:

- The photo
- The electronic component, with the same contactless interface
- The inclusion of a travel document application
- Document life cycle
- A European harmonized card for EU citizens living abroad.

Digital Identity
We have been in the digital world for some 20 years now. The youngest generation, born during that time, is fully and continuously connected.

Use of online services requests electronic identification and authentication with a level of assurance that depends on what is at stake. Digital Identity use requires convenience and flexibility, in particular for the new and upcoming hyper-connected generations and their massive use of private e-services.

The eIDAS Regulation adopted in 2014 determines the rules for public online services, with the encouragement for use by the private sector.

Clear definition of identification – authentication levels of assurance

According to the eIDAS Regulation, the levels "Substantial" and "High" shall be documented by these specifications:

Organizational factors, which concern the registration phase, are:

- The quality of the identification process
- The quality of the issue of the credential
- The quality of the entity issuing the credential.

Technical factors, which concern the electronic authentication phase, include:

- The type and the robustness of a credential (e.g., an ID token)
- The security features of the authentication mechanism for remote authentication.

Eurosmart's 1ST wish is that the differentiation of levels "Substantial" and "High" shall be clearly made in both technical requirements and liability effects. The level "High" shall not be restricted to very few cases, since it could lead to a lack of economic interest.

Definition of the Interoperability model

Eurosmart 2nd wish: Definition of a full ecosystem.

As it has been made for successful previous models such as GSM, EMV and travel documents:

- Technical specifications and standards, the eIDAS token specification is public and shall be recommended
- Test suites for conformity and interoperability testing.

Definition of the security model

Eurosmart's 3rd wish is that C.E.N. WG17 works on Protection Profile (local or remove) shall be the reference for the security evaluation and certification, at minimum, for the QSCD:

- Local QSCD Protection Profiles : EN 419211 series
- Remote QSCD Protection Profiles : CEN EN 419 241 part 2 & 3
- Cryptography qualification.

Privacy protection

Eurosmart's 4th wish is that Privacy Impact Assessment and privacy by design duties shall be defined by means of:

- Favouring the user's device rather than databases
- Recommendation of a user's device giving full control to the user. The device shall include embedded features allowing for:
    - data minimization
    - pseudonymous authentication and signature

- the same management for personal attributes as for personal data
- Standards
- Evaluation and certification.

Technology flexibility

As determined in the Regulation, technology neutrality is a principle that enables innovation and avoids monopolistic market situations.

Eurosmart's 5th wish is to be open to the use of future technologies for authentication, amongst them the physical authentication by biometrics, in full respect to privacy and ethics that can be ensured by use of a secure element.

Outlook: Europe in 2020

Data, figures and facts

In 2020, all citizens in the EEA who travel outside Schengen will have e-documents available – around 100 million, or 20% of the total population. It is expected that most of the EU Member States will have e-Gates in use, in order to accommodate EU citizens (e-Pass) and 3rd country nationals (Registered Traveller Program; RTP). Exit and Entry Schengen (EES) should be in operational mode.

It is expected that more than 250 million eID-cards will be held by citizens and around 20 million e-Residence Permits by 3rd country nationals. The eIDAS-token specification will become mainstream in Europe. This approach paves the way for technical interoperability.

It is also expected that more than 10 States will use an e-Driving License, which can be used as a "pseudo-eID" document. In most of those States, an ID card is not mandatory by law.

Digital world: The two speeds

Online services with private Internet providers have now been in use for more than 20 years. In some EU Member States, more than 70% of citizens use the web for hotel bookings. The rate of online flight bookings has climbed to more than 90%. Online services in the public domain follow this model around 10 to 15 years later, regarding multiple applications and regarding the frequency of use.

It is expected that 95% of the e-services in 2020 will be captured in the private domain. The areas of use in the public domain based on two-factor authentication – such as virtual post boxes, eVoting, eTax-payment, eSocial Service, ePension Service and eGovernment Services within a municipality – would be limited.

If service providers deploy their own Digital Identity based on two-factor tokens, such tokens would have much more frequent use than eIDs in the public domain. Why? Industry is purely business-oriented. Service providers need market share. New concepts like FIDO could play a predominant role in 2020, if a big market player promotes this. Such tokens can have a very short lifetime combined with

high exchange frequencies regarding new functionality, features and services as shown today in the smartphone market.

eID-cards in the public domain follow a 10-year policy: there is a 10-year lifespan of documents, and a new generation of document is created every 5 years on average. However, big data, profiling on the web, web-tracking and cloud services generate a demand of privacy that can be provided by "privacy by design" and "privacy by default" features of eID-cards.

Digital Identity: The two worlds

Social media platforms like WhatsApp, Twitter and Facebook need IP-addresses of computers to get access.

In the digital world, the concept of identity has multiple variations: Anonymity, virtual identity (the person I have created for a specific purpose), some of my personal data that may identify me uniquely or only within a profile, my identity based on my "root identity", etc. The service provider may be satisfied with any of these types of identity, although the more he knows about the user, the more benefits he can get by using that user's personal data. The service providers of the private sector have business needs in terms of identity that government cannot satisfy.

Thus, they created their own electronic identity solutions named "soft IDs" (the name was created by JRC), based on declarations made by the user. Reliability, security and privacy are under the sole control of the user and the service provider, who does not always control risks or limits or is able to manage liabilities.

In the physical world, we have police on the streets, border guards at airports, authorities in municipalities, and customs and other government authorities who need access to a citizen's "root identity". Such root identity requires highly secure and long-lasting ID documents, like an electronic passport, electronic residence permit, electronic ID card or electronic driving license (see remarks in 6.1).

In 2020, the concept of assurance level of identities is well introduced. "Soft IDs" have a high frequency of use, but under the impetus of the European Union and the Member States, eIDs with a high level of assurance (with defined liabilities) have been created, protecting both users (in terms of personal data and privacy) and service providers (in terms of security and definition of liabilities). The eIDAS Regulation is the basis for the establishment of a high level of assurance of identity, providing security, personal data and privacy protection.

Cross border e-Services: The two policies

In the private domain, cross-border e-services are mandatory. Service providers, like Facebook for communication and Google for search, are purely business-oriented in the market. Market share is the key success factor for private companies. For private companies, borders as a kind of market barrier do not exist.

In the public domain, an e-service based on two-factor authentication was deployed for the citizen in the "home" land. The 1st program in Europe was started in 1999 in Finland, called FIN-ID. These e-services stop at the border of Finland, because the federal government – such as Ministry of Interior – is only responsible for the citizens in its own country. In mid-2014, in 21 States in Europe, eID-

documents were being used. Most of them have different data sets, capture different services and use different security architecture.

In 2010, the European Commission began preliminary work and launched an initiative along the eIDAS Regulation that EU Member States should accept eID tokens from other States. With large-scale pilot programs such as STORK and PEPPOL, the feasibility of interoperability for cross-border services were explored.

The eIDAS regulation adopted in 2014 defined the interoperability model for the cross-border recognition of electronic identities for the public sector, with encouragement for use by the private sector. It is a huge step in the creation of a trusted, single digital market in the EU.

Citizens: The two generations

The generation born between the early 1980s and the early 2000s is named "Generation Y" or "Internet natives". People born in this generation have been surrounded by computers, tablets and mobile devices from the time of birth, use the computer every day more than the TV, and exchange information, data and photos with others in a high-frequency mode.

At the same time, five or more social media platforms are used by this group. "Generation Y" members are technology savvy, buy new apps on a weekly basis, and navigate in the digital world better, faster and for a longer time than in the real world.

"Generation Y" and the successive generation will be the main market for service providers in 2020. Although older generations do not compulsively use the Internet, they are more and more a part of the connected world. Keeping older citizens abreast of changes is an economic and social priority. These people, who can be more vulnerable, need secure services and more guarantees about the use of their identity and personal data.

Conclusion

Digital Identity is made up of several aspects, including different actors, different values and different timing.

The "Root of Digital Identity" is and will be provided by Member States and the eIDAS, and "Know Your Customer" Regulations are confirming this strategic aspect.

The Root of Digital Identity may be coming from several eID documents: National eID, eDriving License or ePassport, depending on the Member States' business processes.

Europe has a strong Digital Identity strategy as per the Digital Single Market Strategy, and has to promote European values for the wealth of European citizens, Member States and the economy.

The smart security industry is supporting this strategy by promoting the European Values in more than 120 countries.

Sources

[1] http://www.eurosmart.com/images/doc/WorkingGroups/e-ID/Papers/eurosmart%20eid%20landscape%20white%20paper.pdf
[2] Der Passexpedient; History of travel documents, Andreas Reisen, Ministry of Interior, Germany, Published May 2012
[3] http://www.suisseid.ch/
[4] https://www.bankid.no/Dette-er-BankID/BankID-in-English/This-is-how-BankID-works/
[5] http://www.nist.gov/nstic/
[6] http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-22/TAG-MRTD_22_Report.pdf
[7] https://fidoalliance.org/
[8] http://www.apple.com/apple-pay/
[9] ISO/IEC DTR 19446 -ISO-Compliant Driving Licence - European driving licence - Application profile
[10] eIDAS Token Specification TR-03110 : www.bsi.bund.de/eIDAS
[11] TR Signature http://www.ssi.gouv.fr/agence/publication/publication-des-specifications-techniques-en-matiere-didentification-electronique-eidas/
[12] TR Physical User Authentication: http://www.ssi.gouv.fr/agence/publication/publication-des-specifications-techniques-en-matiere-didentification-electronique-eidas/

Contributors

Name	Partner
Carsten Traupe	NXP
Detlef Houdeau	IFX
Didier Chaudun	Morpho
Frank Schmalz	G&D
Jerome Boudineau	Morpho
Stefane Mouille	Gemalto
Wim Hens	STM

About Eurosmart

Eurosmart gathers global technology providers with a strong expertise in the management of digital security within hostile environments. All its members have common European roots and take pride in their support to the achievement of the European Union's Digital Single Market. They joined the association to help carrying the voice of the digital security industry, and are committed to ensuring that Europe builds on their worldwide leadership and expertise. Eurosmart is based in Brussels where it has a permanent office for over twenty years.

Eurosmart aims to enhance the usability of services in the connected world, by promoting security technologies designed to combat fraud and safely manage digital identities while protecting consumers and citizens' right for privacy.

For more information, please visit www.eurosmart.com