About Gemalto

Gemalto is the world leader in digital security, with 2014 revenues of 2.5 billion euros. To date, Gemalto is contributing to over 40 electronic identity document initiatives and 30 electronic travel document programs. Gemalto relies in particular on the offer of its MOBILE entity, the leading supplier of solutions for user authentication and mobile digital signature, with more than 20 ongoing projects.

To promote the emergence of a freer and more sustainable society by making it more secure, Gemalto has built a structured approach and mode of contribution to government programs, sharing international experience, industrial know-how and its position as partner to public authorities in numerous countries.

Its approach addresses three main areas:
- Securing the identity of citizens
- Protecting their privacy, personal data and digital rights
- Promoting an optimal framework of trust for digital exchanges in order to create the conditions for a reliable deployment of online services.

In the same spirit, Gemalto collaborates with its customers to analyze and promote best practices in these areas across the planet. This is what this white paper is about.

For further information, visit www.gemalto.com
I – Challenges

The digital revolution is impacting all sectors of society. The most visible change is the growing multi-channel access to online services, whether via the internet or mobile applications. As our lives shift towards the digital space, most countries are finding it important to maintain continuity in the way society is organized, improve economic circuits and mechanisms and develop services to citizens.

For all citizens, managing health, organizing children’s education, taking out a loan (or investing savings), signing a rental contract or exercising civil rights are significant acts of responsibility that can be managed in the digital space, as long as this can be done with confidence and peace of mind with regard to their validity.

For companies, whether large or small, their role as economic stakeholders, together with their corresponding legal liability for the scope of their business, means they need to make sure their new digitally-acquired agility remains securely rooted, so they can improve customer service while safeguarding contractual commitments.

For public administrations, the challenge of greater flexibility in public services thanks to the “all-digital” transition and the need to better understand user needs are combined together. Here too, the task is on government services to be reliable, all the more so as governments must act as guarantors in their sovereign task of preserving public interests and the safety of people and property.

This view, shared for some years now by an increasing number of countries¹, has the advantage of promoting the conditions for digital development centered on people and their changing usage habits, based on two pillars: trust services and, above all, digital identity.

Improving the deployment of trust services

To enable public administrations, companies and citizens to freely interact while retaining their formal relationships of liability, there needs to be a progressive development in the use of “digital trust” services. Such services make it possible both to link decisions and acts of management to those enacting them, thereby granting them certain legal validity, and to conserve the elements exchanged by the parties securely.

To this end, regulatory authorities are making great efforts to harmonize such services and promote their legal value. One example is that of the European Union, which recently introduced a regulation on electronic identification and trust services².

In practical terms for citizens, this might mean, for example, having access to the confidential health data shared with a doctor before a medical operation, or being able to transfer money to a third party while complying with declaration obligations. For companies, especially very small, small and medium enterprises, it represents an opportunity for improved management of social and fiscal obligations, as well as sensitive processes such as supplier purchases and financial transactions.

For trust to be established, both parties must be linked via a secure, unbroken chain. The capacity to demonstrate that you are who you say you are (authentication) is a strategic imperative. An additional step is identity. Identity is in essence the link that connects an individual and the community. Protecting identities against fraud or theft is key to maintaining confidence. The greatest challenge is ensuring that a digital identity matches a real identity, i.e. ensuring that it is authentic and unique. Establishing a digital identity and providing secure access to services can be carried out using a twofold authentication and identification process (verification of a person’s identity).

² Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market
Governments worldwide are seeking to boost efficiency and transparency in numerous essential functions, with the ultimate aim of better serving their citizens in a reliable, secure and transparent way.

They deploy national identity trust systems not only to rationalize services and processes in areas such as social services, taxes, local voting and administration, but also to promote private services by stimulating the digital economy, all while reducing costs.

National public services that are secure, efficient, accessible and reliable can also facilitate citizens’ contributions to public decision-making, and enable them to participate more directly in society, notably at local and regional level.

Secure digital identities

In life, any act of involvement or commitment requires a means of identification, whether to establish a right, allocate a service or check that the holder is indeed the person requesting a service: it constitutes an implicit form of authentication. Any agreement between two parties, or authorization by a third party, is conditioned by this means of identification. The same naturally applies to the digital space, where trust services and reciprocal commitments can only operate once credentials are suitably established.

Identification in the physical space is generally provided by a secure identity document (passport, card or driving license), with especially important acts requiring additional confirmation by a trusted third party such as a judicial officer, notary, banker, health professional or mayor. In the digital space, meanwhile, identity for trust services must also be attributed and secure, under the responsibility of the sovereign state.

One “National Identity” issued by States. According to Cornu*, this identity is that which makes a person unique, i.e. itself and not another, and by extension recognizable and distinguishable from others: > confers rights and duties

Multiple “Digital Identities”
• E-mail addresses
• Aliases on internet
• Profiles on social networks
• Traces often left inadvertently when using digital applications
• IP addresses
• SIM cards on mobile phones
• Bank account details
> For communicating, conducting business, etc

(*) CORNU, Gérard, Vocabulaire juridique, 8ème édition, Paris : PUF, 2007
National Identity will contribute to a build secure Digital Identity.

It is clear that writing a name on a piece of paper is an insufficient expression of identity in the physical space, even in “face-to-face” situations and especially when accessing “trust” services. Likewise, providing a disposable email address or password login in the digital space is an inadequate way of establishing identity in the strictest sense of the word. Rather, it must be supported and managed according to the service required, and sufficiently “secure” to enable trust interactions between society and each citizen. Indeed, it must be possible to recognize citizens in an unequivocal manner, and verify their position and credentials, whenever so requested in the digital space, whether citizens are acting as natural persons or on behalf of a legal person.

This need to manage or structure digital identities invokes the sovereign role and responsibilities of states.

The role and responsibilities of governments

The role of governments is fundamental in this area, as states have both a right and a duty to exercise their sovereignty by virtue of and in compliance with international law and their own constitution. It is therefore logical to assume that this sovereignty shall be exercised consistently across the digital sphere and the physical territory of the nation. Identity is one of the basic attributes of this sovereignty, responding to the state’s role in terms of justice and citizens’ rights, the organization of civil life and the social contract, or even defense and security.

As a result, governments today, just as they did in the past when issuing or regulating “sovereign identities”, must provide or approve digital identity solutions in response to the challenges of efficiency and modernization, as well as the longer-term challenges faced by states as part of the digital transformation of civil society.

Short- and medium-term challenges include:

> Providing a high-quality public administration system for citizens and companies: user-friendly public services that are more reliable and more agile thanks to the deployment of identities, making state services more accessible.

> Developing the usage of digital trust services, with more transparent, reliable and structured digital exchanges, and greater technical and legal security for very small, small and medium enterprises, and consumers.

> Enabling greater integration with private sector services.\(^3\)

> Improving data protection and modes of consent in transactions or contracts in the digital space.

The challenges of sovereignty

These digital challenges flow into the core challenges of state sovereignty: the organization of society, economic development and social cohesion.

These long-term challenges can be described briefly as follows, with emphasis on their strategic importance:

> Trusted Digital Identity is at the heart of the digital economy, but also at the heart of societal transformation. Key sectors like healthcare, education, social protection and welfare, as well as simple civil security, can benefit from this.

> Promoting economic development and healthy, sustainable growth. By encouraging high-value usage, digital infrastructure will be used more effectively by the public and private sectors, and the whole economy becomes more productive.

> Upholding values such as the protection of fundamental rights; integration and the social bond; economic, cultural and linguistic influence; and interoperability with other states.

In short, the role of governments with regard to identity is not restricted to that of issuer, regulator or security operator, but is of strategic importance for the development, reach and influence of each nation. It starts with the digital transformation of administration services, continues with the introduction of trust services that benefit the economy and society as a whole, and persists over the longer term with efforts to harmonize sovereignty between the physical and digital spaces.

It is with this in mind that we will examine the introduction of “national identity schemes”, also paying attention to schemes emerging in Europe under the new European regulation.

---

\(^3\) It should be noted, however, that in certain cases, following a constitutional validation process, certain states may delegate part of their sovereignty. For example, the issue and control of currency, another attribute of state sovereignty, may be considered a delegated sovereign function in Eurozone countries.

\(^4\) One illustration of this is the online system introduced in the United Kingdom in 2015 that allows rental companies to verify driving licenses and driver status (penalty points).
II – National identity schemes

The introduction of national identity schemes represents a response to these various challenges.

What is a "national identity scheme"?

Firstly, the national identity scheme indicates the roles of the sovereign state with regard to digital identity: does it act as a regulator? Does it act as an issuer of sovereign identities or the digital derivatives of these identities? What are its responsibilities within the chosen ecosystem in terms of organization, data and applications, and infrastructure?

Next, the national identity scheme establishes the underlying principles and operating methods of the digital identity ecosystem. It describes the main systems and flows linked to the use of digital identities to access services, authenticate users, and exchange and verify data linked to the service requested. Where necessary, it provides useful details on the approved identity types and trust levels supported by the ecosystem. For example, commercial or transactional uses for identity may have functionalities distinct from those associated with authentication in the public domain.

The identity provider plays a key role:
Furthermore, the national identity scheme is not exclusively limited to national exchange methods for identification and access to services. It can also incorporate interoperability flows with other countries, notably those linked by free movement or integration treaties.

In this, users requesting services have fairly similar needs, although a distinction should be drawn between individuals and professionals on the one hand, and transactional and sovereign usage on the other. They mainly require the capacity to:

- provide authentication according to the level of trust required by the service provider,
- identify themselves easily, with minimal entry of personal data\(^1\),
- perform online verification of certain information to access a service.

Individuals may need to provide verification in a range of areas.
- Does the school want to verify that you have the rights necessary for use of the children’s school canteen?
- Does the local council want to check you are a local resident before it allows access to a service?
- Does a motorcycle rental business want to verify that you permitted to ride an 80 cc vehicle?
- Does your bank want to check that your residence is on the regional land register?

The list goes on.

---

\(^1\) Notably in the case of EU countries in accordance with the eIDAS regulation.

\(^2\) Minimizing the entry of data in this way is important as much for automation and speed of access as for the protection of privacy. The standard process is to indicate the selected public or private identity provider, and take advantage of SSO [Single Sign-On] functionalities.
Types of scheme and some examples

The majority of identity schemes are anchored in cultural habits that vary from state to state. Furthermore, different cases have specific strategic visions of development, corresponding to a particular economic and political vision. However, we can obtain an overview of identity schemes by identifying certain criteria that qualify the various types:

> Sovereign uses and the public sphere

> Transactional and commercial usage / the private sphere

> Homogeneity of digital identities (common root, trust levels)

> Public and/or private origin of identity suppliers

> Degree of integration of the identity market (number of agents, etc.)

> Level of security of the processes and technology

> Regulation and sense of responsibility of the stakeholders

> Centralized or decentralized organization

> Etc.

Certain nations largely delegate the provision of identity solutions to the market, and therefore the private sector: this is the case in the United Kingdom.

[Diagram: Identity ecosystem UK]

Other nations take a more sovereign or citizen-centric view of identity, with the state playing a bigger role in issuing digital identities and integrating them into public administration services. This is the case in Estonia, for example: [http://review.gemalto.com/estonia/?post/special-multimedia-feature-egov-leader-estonia](http://review.gemalto.com/estonia/?post/special-multimedia-feature-egov-leader-estonia) or [http://www.gemalto.com/govt/customer-cases/estonia-eid](http://www.gemalto.com/govt/customer-cases/estonia-eid) and in the United Arab Emirates.

In Germany, the system is both decentralized in terms of information systems, and uniform, with a high-level trust root based on the personal identity document or “Ausweis”:[http://www.gemalto.com/govt/inspired/eid-in-germany](http://www.gemalto.com/govt/inspired/eid-in-germany)
In France, different choices have been made. Information exchange processes under state control have been centralized to a certain degree, although there is a greater disparity of identity solutions and sources between public and private suppliers. The global ecosystem - legal and commercial interactions- between private sector and public one, is currently under construction.

In Nordic countries such as Sweden, the banking sector has taken on a key role in both issuing and using digital identities. This ecosystem is evolving. Partnerships, agreements between the government and the private digital Identity providers are under negotiation.

Italy has announced in November 2014, its two major national plans to reach the objectives of the digital agenda: the “ultra-fast broadband” plan and the “digital growth” plan.

With the “ultra-fast broadband” plan the objective is to cover, within 2020, 85% of population with a very high speed connectivity; setting the basis for dematerialization and new e-services.

The “digital growth” plan aims to boost the usage of technology and the intensive and secure use of digital exchanges to stimulate economic growth, and social cohesion.

In particular, the objective of the digital growth plan is to strengthen the framework of trust in digital exchanges which is key.

It is illustrated by 2 projects:

- the “digital security” project aims to increase the security level of information and digital communication. With this initiative, privacy, integrity and continuity of services can be assured using digital and online services;
- the SPID project (sistema pubblico per la gestione dell’identità digitale di cittadini e imprese) aims to create a new public system for digital identity management. It will provide access to offer e-government services to citizens and companies alike. Italy aims to have the system used by ten million users in 2017 (70% of population within 2020). The publication marks a milestone in Italy’s digital agenda.

The Digital Agency for Italy (AgID - Agenzia per l’Italia digitale) is driving the digital transformation of the Italian Government. It involves projects in both infrastructures and platforms, in particular with the objective – and challenge – to boost the usage of the Italian digital Identity Card. Italy’s plans are in line with the eIDAS regulation as interoperability is a key success factor of Italy’s digital transformation.
Identity at the crossover between sovereignty and market challenges: the European example

What can we conclude from this?

It is clear that the deployment of digital identities under different national frameworks represents a dual challenge for nations, which must manage their sovereignty in the digital space while improving services to companies and citizens, in other words the framework for market interactions, and ultimately the healthy operation of the economy.

Yet reconciling market demands and sovereignty is no simple task. It requires constructive negotiation between their respective objectives.

A good example is provided by the European Union. Here, national identity schemes must be viewed in terms of both the actions of individual states, and the implementation of the eIDAS regulation (which may indicate future convergence), as well as the objectives of the European Digital Single Market and European Digital Agenda 2020 strategies.

In the end, these actions surrounding digital identity demonstrate a desire to rekindle economic growth through the more effective use of digital services, and build a single digital space of trust, offering a high level of security, interoperability and data protection.
Appendix

Types of stakeholder:

Users
Users are citizens or small and medium enterprises that wish to access or use a given service.

Service providers
Service providers deliver the service after delegating user identity verification to the identity provider.

Identity providers
Identity providers authenticate users or verify the information requested according to the level of trust required. Identity verification covers several operations performed jointly or separately, such as identity registration, authentication, and the verification of certain data, attributes or documents (credentials). In some cases, these operations may be managed with (or possibly delegated to) providers of data or secure documents.

Attribute providers
Attribute providers may be public or private, and general or specializing in a type of data, for example proof of address or revenue.

Secure document issuers
Secure document issuers generally issue documents in the public sphere. Their role is sometimes combined with that of identity provider.

Registration authority
Registration authorities are involved (in the case of PKI) in distributing databases and providing an unambiguous link between a given public key and the user.

Certificate authority
Certificate authorities (in the case of PKI) control the issue, management [suspension for example] and withdrawal of digital certificates.

Federation services
In this case, federation services refers to several types of interoperability network, infrastructure, perimeters or rules that create conditions conducive to identity management.
About the white paper on national identity schemes

A national identity scheme sets out the roles of the sovereign state with regard to digital identity. It also establishes the underlying principles and workings of the digital identity ecosystem. The aim of this white paper is to give all public stakeholders and partners the understanding, insight and tools that will enable them to contribute to greater success in the modernization of public services and, more broadly, of society, by including digital identity as a defining feature in a digital space of trust, with good levels of security, interoperability and data protection.