When your identity becomes electronic

Joël Vanoverschelde
Partner
Technology & Enterprise
Application
Deloitte

Damien Ghielmini
Director
Technology & Enterprise
Application
Deloitte

Loic Saint Ghislain
Senior Manager
Technology & Enterprise
Application
Deloitte

Ismael Cisse
Manager
Governance, Risk
& Compliance
Deloitte

The emergence and irrepressible rise of electronic identity cards (eID) comes as no surprise. Advances in digital technology, mobility, and multimedia access to private services establish conditions in which clients and citizens naturally expect the same from public services. Deloitte openly discussed this development in its study on the future of public services and the switch to digital on a 2020 horizon. Conducted over more than a year by collating the views of all stakeholders in the government and quasi government realm, this study will be updated regularly and is available free of charge on the Internet. For example, the development mentioned can be found at http://government-2020.dupress.com.

The greater the number of remote procedures and related issues there are, and the bigger they are —all constantly accessible and requiring strong authentication—the more obvious the attraction to criminals will be

An ever greater need to identify a person…

The need to identify an individual beyond doubt, whether this be a citizen—as is usually the case—or a category of person in general (resident, etc.), inevitably grows as the number of procedures that can be carried out online, without direct contact, increases.
When the individual is considered to belong to an organization (typical example: an employee authorized to represent a company with a certain degree of authority), the issue is even more sensitive. Complicating factors naturally appear in such a situation: greater time aspect, increased need to monitor and track procedures and implement security measures if the representational link is broken so that, ultimately, only one identity is managed.

…and a threat that is growing as a result

Alongside the spread and diversity of these types of situation, the threat to our modern society is growing exponentially as it feeds on the surge in contactless transactions, whether or not there is a financial impact. The greater the number of remote procedures and related issues there are, and the bigger they are—all constantly accessible and requiring strong authentication—the more obvious the attraction to criminals will be. Then there is the fact that gains are often easy and lower risk (legislation is struggling to keep up and investigations are incredibly slow), and victims are in a position of weakness. Identity theft, which can affect all of us in every guise (citizen, subject, employee, parent, social network user) is a blight on our modern society yet paradoxically we have never had so many ways of recording and exchanging data between us.

Unrelenting growth…

If we go back to the basic service in which an identity document allows a citizen to initiate an administrative procedure or at least prove who he or she is, we see that, historically, the need to access eGovernment services did not necessarily require security ID or even, more prosaically, proof of identity. The first services were often relatively basic in form, level of supervision, efficiency and importance. Typical example: accessing a form—often downloaded, sometimes interactive—and sending a request, often by email. Not so long ago, entering an ID (e.g. national number) was often enough, and the risk was limited ipso facto by the possibility of checking and processing this later.

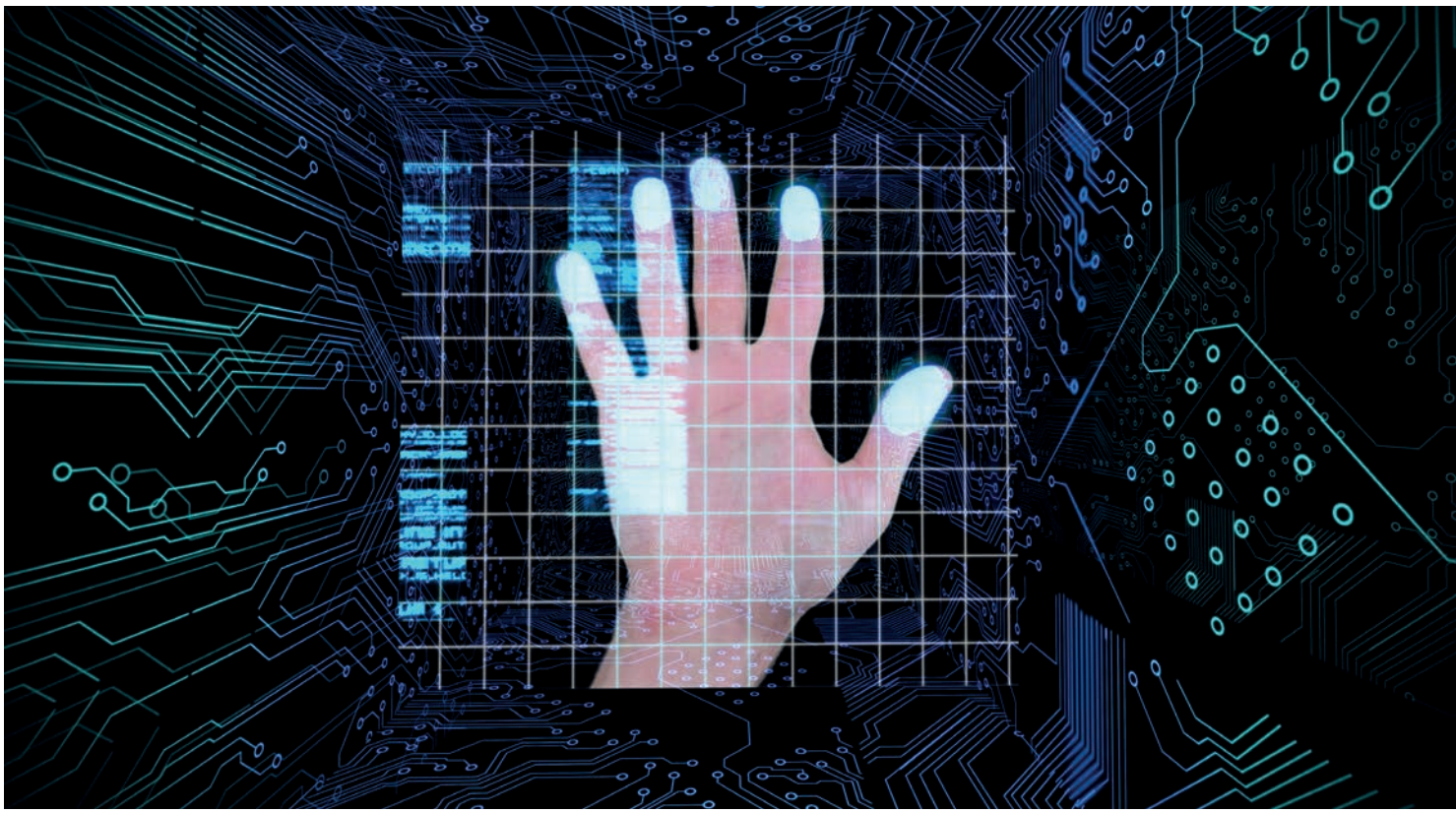
Since the turn of the century in particular, governments—under the impetus of the European Commission—have rushed to offer more and more digital services. This could once be justified by internal brand image reasons and/or the wish to make people's lives easier with wider access: who hasn't complained about bank counters being closed when our free time is constantly shrinking yet the need for administrative documents remains unchanged?

In an era that can be described as transitional in terms of trying to optimize (human) resources, the speed with which appropriate responses are provided and the search for operational efficiency have come to the forefront and become a lasting concern for governments and administrations.

…and naturally the emergence of new equilibria

Now there is room for competition between countries (improvement in the country's brand image, generation of income from intellectual property, attraction of talent from the younger generation around the globe—full of life and brought up in a world in which Facebook and Wikipedia have replaced the print encyclopedias of yesteryear). We see increasingly modern products, complicated screen sequences and decision-making processes, and a level of complexity that has largely caught up with the private sector. The sophistication of administrative and government services in particular is quite natural. It stems from the proliferation of regulations—for which our particularly wary generations are enthusiastic (transfer of services to the private sector, outsourcing, international cooperation, etc.)—and major tectonic shifts affecting governments. It also meets a need to consider a higher expectancy from consumers who increasingly want to understand every part of the decision-making process (legislation, case law, options).

If we look at the trends revealed in Deloitte's GOV2020 study on the future of government services, the transfer of certain operations to the private sector, traditionally seen through PPP (Public Private Partnerships), and which involve complex, lengthy processes, will be extended to more cases where governments call on franchises to carry out certain basic procedures. This type of situation already exists for remote operations such as handling visa applications in countries around the world. However, this ubiquitous public presence also increases applicants' and professionals' level of expectation for consistent identification and tracking. As such, strong authentication of the person logging in is increasingly required as highly complex procedures adding real value can only be considered with this level of guarantee. This structural trend coincides with a need for simplicity in this form of strong authentication. Part of the challenge lies in the combination of these factors: infallibility, frequency, and simplicity.



The eID card today…

Having so many small, cheap, practical but relatively specific tokens remains laborious. Some major players such as LuxTrust in Luxembourg may be emerging to give access to several leading banking systems, but barriers remain, often requiring people to hold more than one token. Meanwhile, relative slowness in introducing eID chipcards with a certificate, whether contactless or not, and perhaps the need to find an accessible and portable personal storage system (personal safe), have lent credibility to the idea of a government-issued "universal key" for different public and private usages. This key may also be viewed as a first step towards there being a "key of keys", bearing in mind that each individual now has to hold and (try to) memorize a huge number of passwords for professional or private purposes, and has to change them regularly.

Since the turn of the century in particular, governments—under the impetus of the European Commission—have rushed to offer more and more digital services

From here, it is very easy to imagine a reference key, access to which could be more sophisticated and offer the highest degree of protection, potentially including biometric data. This key would open a box of other keys. Private stakeholders are trying or have already tried to do this but we think a national or even supranational guarantee is required for it to take off. If we return to the study on government services in 2020 (http://government-2020.dupress.com), we cannot rule out facial recognition to access a card that would ultimately contain all the data that an individual could need, either directly at a card level (i.e. in the chip), or in super-secure places that can only be accessed with a combination of keys. Where such an approach reaches its limits is at data protection agencies—such as CNPD in Luxembourg—, which will quite naturally demand indisputable proof, and no doubt observation periods too, before allowing such developments.

Citizen's consent—even if given in full knowledge of the facts—will probably be essential but without some new public/private, innovative use that could trigger broad acceptance and exert pressure on agencies, this type of situation will only arise in the long term.

Talking of usage, it is natural to consider the level of use, frequency and variety of eID cards as it is clear that simply checking identity for legal purposes (police, customs, etc.) is only a very basic objective. So having an ID document that uses the most up-to-date technology and security is not necessarily enough. As the world of IT and telecoms shows each day, for a virtuous circle to be established we need a standard and for potential usages based on this standard, or this eco-system ("IN" usage), to be visibly greater than the usages that require an alternative resource ("OUT" usages). Such a movement will only happen if close interconnection is possible between documents in different countries, i.e., if a Luxembourg eID is widely recognized by a series of European government sites, for example.

Fortunately, such interoperability is under way, driven by the European Commission. Its name: eIDAS (regulation (EU) No 910/2014). More than a form of interoperability, eIDAS is an attempt at mutual recognition of electronic identity schemes (for example national electronic identity documents) between Member States. This automatically assumes monitoring systems that allow each country to check the validity of documents from other countries, and therefore standardized exchange protocols and security levels. For citizens of countries that sign up to this open-to-all approach, major simplifications will emerge in the mutual recognition of electronic identity documents and, in particular, access to government and non-government websites and e-signatures will become recognized on a cross-border level. Changes in the intra-European movement of people may appear modest at first glance, with the potential risk of having different groups of countries working at different speeds (Schengen? eIDAS?) but in practice national electronic identity documents are now being used to register with foreign universities and prove identity to stakeholders in other countries. For the countries themselves, no one can say at this stage whether the ones that are ready first, for government sites and especially commerce sites, will attract a

new influx of demand, or more reasonably enjoy a more privileged position. Our analysis suggests that government initiatives and developments, such as in Estonia, will lend credibility to proposals from private entities based in the country with strong national identities. Indirectly, this is a way of diversifying the economy and it is an important issue in Luxembourg.

Between 2014 when this new regulation was introduced, 2015 when recognition of electronic identification schemes between Member States will be on a voluntary basis, and 2018 when mutual recognition of electronic identification schemes notified to the European Commission will be mandatory for access to online public services, public and commercial websites will gradually promote the advantages of mutual recognition of electronic identity documents. At the very least, this will enhance the country's image and even eliminate certain procedures or facilitate access to certain services that currently see little competition. This brings to mind medical services and not just certain types of surgery (e.g., dental) for which certain—largely psychological—barriers may be present, leading to more global competition or at least changing habits and a redistribution of market share. European integration is already well under way with the European standard social security card (chip-free), and the incorporation of eID functions would immediately reduce the weight of purses and wallets (fewer cards), something that is not necessarily as trivial as it may seem.

…great potential if conditions are met

All of these predictions concern a relatively near future and pan-European trend. From there to imagine that electronic ID cards could one day replace passports and other ID and/or travel documents is a step too far for us at present. Closer to home in Luxembourg, and hopefully on a nearer horizon, progress is likely with public services in healthcare, which is a natural outlet but it is not the only one. There could also be developments in the private sector (for example with pharmacies, which are also part of the healthcare industry). For these significant developments to see fertile ground and be practical, we first need to establish conditions under which people are more willing to put their trust in these new systems and the certificate used than they are in current cards, bearing in mind that not all applicants for Luxembourg ID cards take the certificate option. The reasons for this situation clearly lie as much in the confusion over future usages—unknown, poorly understood, or imagined—as in general distrust of such technology.

Cost, which is the same with or without a certificate, is not a decisive factor. As was the case in Belgium, the new system would probably go beyond a purely national Luxembourg ID card to be used by residents or even a wider public. This discrepancy between the initial (national) population and much broader public is a structural characteristic of Luxembourg and could also help facilitate the conditions for tighter cohesion, which would result in identical features being offered to as many people as possible, without discrimination. This would certainly be a step in the right direction.

Conclusion

In concrete terms, at an e-healthcare level, it is worth remembering that the ultimate target is for 300,000 Luxembourg ID cards, including babies and pensioners, yet around 2,000,000 individuals in the wider region are covered by the Grand Duchy's provision of medical services. This clearly shows the gap that may have to be closed, and the differences of scale to switch from a strict electronic ID card used for identification and intra-EU travel purposes, to a card with a combination of uses, and users, on a completely different scale.

Beyond public interoperability, the coordinated extension to private (access to bank websites) or mixed (pharmacists' access to databases) use is the obvious prerequisite to more widespread adoption, bringing major improvements for citizens. Once this target has been met with a "Swiss army knife" eID, the only limit on potential use will be our imagination.