

Proof of identification on line: A sovereign solution for trust-building

Valérie Péneau,
interministerial program France Identité Numérique

Abstract:

The growing need to be able to prove one's identity online, in a simple, convenient, and secure way, justifies the provision of a trusted public electronic identification tool to citizens, in addition to possible solutions offered by private actors. In accordance with the European eIDAS Regulation, which defines the different levels of security and establishes the principle of interoperability of these tools in the European digital area, the French government has initiated a program for designing and deploying national electronic identification, which will be in line with the future national electronic identity card to be issued starting in August 2021.

In an environment with increasingly dematerialized procedures, guaranteeing the identification of contacts on the Internet (whether with natural or legal persons) is the keystone of trust. As a consequence, proving one's identity on line in a simple but secure manner has become an issue for service-providers as well as the victims of the growing number of scams and all users who want to control their personal data and guard against identity theft.¹

Since 2014, the EU's so-called "eIDAS regulation" has defined "*identity assurance levels*" (low, substantial, high) and, thereby, levels of trust, related to electronic methods of identification as a function of the technical, procedural or organizational security measures that have been taken.² In addition, it has established a principle of interoperability and opposability Europe-wide for the "*electronic identification schemes*" notified by member states to the European Commission. Till now, seventeen member states have filed a scheme of high-level identity assurance (with information on the technical methods used and directions for users).

To make up for this lag and help make secure France's ever growing digital ecosystem,³ where with massive quantities of data being exchanged, the ministers of the Interior, of Justice and the state secretary in charge of the Digital Transition set up, in January 2018, a program with the objective of designing and deploying a method of official electronic identification (*identité numérique régalienn*e) for attaining the highest level of security guaranteed. Starting in the summer of 2021, a new national identity card with a chip could serve as the grounds for this future means of electronic identification. This card's widespread distribution will be a major step forward in this program.

¹This article, including any quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in June 2021.

²eIDAS Regulation: EU Regulation No. 910/2014 of 23 July 2014 on "electronic identification and trust services for electronic transactions in the internal market" available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

³Especially in the public domain, as part of the Public Action 2022 Program.

What is an “electronic identity”?

The report in June 2020 by the Conseil National du Numérique (henceforth CNNum) used the plural: electronic identities. In fact, any single user might go under several identities on the Internet.

- In the broadest sense, electronic identification can be likened to “digital fingerprints”, encompassing all the tracks left on the Web (geolocations, browsing history, services consulted, etc.).
- Cybernauts freely choose a “declarative electronic identity” for interactions on the social media (e.g., the choice of a pseudonym on Twitter).
- The so-called “civil”, “legal”, “official” or “pivotal” electronic identity corresponds to the data from the person’s official vital records — the data that serves as the grounds for the rights and duties of citizenship. With regard to the terminology in eIDAS, this identity is the name (current or usual), the first name, the date and place of birth, and the sex.

From this point forwards, this article adopts this last definition, a “transposition” of the physical person’s identity into the digital realm.

The many issues involved

As CNNum (2020, p.5) has recalled, an *“electronic identity is the pivotal element that will determine how each of us can access the many uses that occupy our everyday lives, while respecting the person’s freedom, integrity and individuality”*.

Besides the question of trustworthiness that, as mentioned in the introduction, obviously conditions the continued development of the digital ecosystem, building a secure electronic identity revolves around several issues:

- SOVEREIGNTY. Since 1792, the management of vital records is an official duty of the French state. This involves reproducing certificates of a person’s civil status. If the state cannot, within a reasonable period, offer an equivalent service to its citizens in the digital realm, it will be forced, *de facto* (given the mounting need of identification) to adopt a solution that (interoperable in compliance with eIDAS) has been proposed by a foreign public entity or been delegated to a private party. In effect, big tech firms are making massive investments in electronic identification. The government would thus lose control over the access to its own dematerialized services, including the most sensitive ones. According to CNNum (2020, p. 5), the effects of the digitization of transactions and social exchanges on our society and its values, *“require restoring and forcefully asserting the relation between identity, as guaranteed by the state, and the electronic identity, which has, till now, been associated with private service-providers”*.
- THE FIGHT AGAINST ONLINE FRAUD AND IDENTITY THEFT. These risks weigh ever heavier on everyday life, as people worry about the protection of their personal data. According to an IPSOS poll on electronic identification in October 2019, one out of five people in France said that they had already fallen victim to identity theft on line. This is an immense issue for the providers of dematerialized services. For instance, the fifth EU directive (2018/843) on the fight against money laundering and terrorism requires that banks strengthen their procedures for online authentication. Its transposition into French law (through the decrees and executive order of 12 February 2020) requires that the security of electronic identification qualify as “substantial” under eIDAS.

- “INCLUSION”. Once an electronic identity is a *de facto* condition for access to the Internet and for the exercise of the rights and duties of digital citizenship, the proposed methods of electronic identification must be both easily accessible and trustworthy. A safe and secure official electronic identity can be a bridge for spanning the “digital divide”. Not only does it spare citizens legwork or the complicated task of scanning the proof of their identity, but it also offers a simple, for-free solution for security that, till now, has too often been reserved for the chosen few who are fully informed about online security.
- ECONOMIC GROWTH AND THE DIGITAL TRANSITION. Secure electronic identification will make possible an end-to-end dematerialization of uses that, till now, have been deemed too sensitive to be made paperless or that require satisfying several conditions in order to vouchsafe the beneficiary’s identity. Likewise, it will make it possible to open and/or simplify new private online services. The lockdown during the pandemic has proven the usefulness of such services. Electronic identification — a market estimated to amount to more than a billion euros within the coming decade (EY-PARTHÉNON 2019) — is an incredible vector for innovation and growth that figures as such in the stimulus program. French industry is recognized on this fast-growing international market.

The French approach to electronic identification

Day in, day out, we authenticate our online identities with a login and password in order to access the many accounts we have opened. As passwords grow in number and complexity, managing them is becoming a factor that hampers using the Internet. Opening an online account is the first source of dissatisfaction among cybernauts (ONFIDO 2019). This method, which is increasingly unreliable, ranks as a “low” identity assurance level under eIDAS. This forces the providers of sensitive online services to add more, sometimes complicated, arrangements for building trust.

For the public administration, a first step toward simplification and security for online identification and authentication was made by setting up the official platform FranceConnect in 2016. It provides access to more than 600 different public services from a single portal via an electronic identification: the person’s fiscal number for taxes (impots.gouv.fr) or social security number (ameli.fr). It verifies whether the identification data correspond to what is stored in the National Repertory of Identification of Physical Persons (managed by INSEE) before transmitting them to the services requesting them. The identity assurance level is still low however.

As a consequence, the objective is to soon make available to users electronic identification with a substantial or high level of security under eIDAS. This implies combining at least two of three types of factors: what I have (a telephone, e-mail, card, etc.); what I know (a code, pass word, etc.); and what I am (biometric data). The person’s identity will be verified; and the data related to identification, encrypted. In practice, electronic identification will take the form of a mobile or Web application in interaction with a certificate of electronic identification.

Many European countries do not have national identity numbers for all citizens or a single population registry. In France, only the identity certificates guaranteed by the state carry authority for proving and verifying the identity of physical persons. Equipped with chips for protecting the data used for identification, passports, residence permits and, soon, national identity cards will be (if users choose) a source of online electronic identification without any need for a central registry and under the user’s full control.

A limited, optional use of facial recognition technology (always under human control)

To reach a substantial or high identity assurance level, an electronic identification must be created for the benefit of the legitimate holder of that identification; and special attention, paid to verifying the holder's identity. Under eIDAS, this verification may be made face-to-face (by a sworn clerk) or via an equivalent arrangement from a distance. As experiences elsewhere have shown, both methods of registration are necessary for adopting and rolling out electronic identification. The first requires legwork but is more inclusive, whereas the second allows users to create an electronic identity when and where they want.

Given the recommendations of CNNum and of a parliamentary committee, plans are being made to satisfy the requirement of face-to-face contact (prior to electronic identification) at the time of delivery of a new national identity card. This card will be delivered in person by public servants at city hall, an emblem of confidence. A fully electronic registration could then be offered to whoever requests it. In this case, identification would be verified in two phases: through an algorithm that will compare the user's face (from a selfie or video) and the photograph on his/her national identity card; and the result of this verification would be confirmed or refused by a specially trained agent who abides by the conditions set by the National Cybersecurity Agency of France (ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information). Facial recognition technology would thus be used for authentication only at the time of creation of an electronic identity, only if the user prefers this and always under human control (CNIL 2019).

The promise of a new, trusted public service

Online identification holds the promise of a new way, both sure and simple, to identify oneself and authenticate one's identity on line when need be (for access to secure websites, for filing a proxy, etc.). The future "official electronic identity", based on France's national identity card, will not, however, be intended for use in all interactions, in particular in the many everyday situations where a lower level of security is satisfactory.

After all, electronic identification in France has a history. For twenty years now, several plans more or less directly related to this question have failed for various reasons. But all of them aroused strong resistance. This lesson from the past should not be forgotten even though the national and European legal frameworks have undergone major changes and security issues are now better understood.

What is at stake is to build confidence and rally support. It is complicated to do this. The success of current plans depends not only on the quality of the technical solution and the relevance of the uses associated with it but also on the confidence that users will place in it. The proportionality and untraceability of uses, the protection and "frugality" of the data collected, the reversibility and transparency of application, all these are indispensable; but they must be accompanied with hard-hitting information campaigns in association with all stakeholders. The shared objective is to be, in the words of CNNum, the "*establishment of an electronic identity that is for citizens, builds confidence, is inclusive, dynamic and favorable to the development of innovations: in other words, a French-style electronic identification*".

References

CNIL [Commission Nationale de l'Informatique et des Libertés] (2019) "Reconnaissance faciale. Pour un débat à la hauteur des enjeux", 25 November, 11p., available at https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf.

CNNUM [CONSEIL NATIONAL DU NUMÉRIQUE] (2020) *Identités numériques: clefs de voûte de la citoyenneté numérique*, a report requested by the state secretary in charge of the Digital Translation in July 2016 and made in June 2020, 122p., available via https://cnnumerique.fr/files/uploads/2020/2020.06_rapport_cnum_idnum_web2.pdf

EY-PARTHÉNON (2019) *Modèle économique de l'identité numérique des particuliers et des entreprises*, 27 September, 250p., available via <https://www.acteurspublics.fr/upload/media/default/0001/33/de3ca498b989941637f253392c3f4c3f15941f40.pdf>.

ONFIDO (2019) "Customer attitudes to digital identity: Meet the expectation of tomorrow", 43p., available via https://schwartzpr.de/website/uploads/Onfido_customer-attitudes-to-digital-identity.pdf.
<https://onfido.com/landing/customer-attitudes-research/>