RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

conseil national
du numérique

PRESS KIT
June 2020

Digital Identities
Keystone of digital citizenship

PRESS KIT

DIGITAL IDENTITIES

Keystones of digital citizenship

Report by the French Digital Council

June 2020

Table of Contents

Editorial

Since the creation of the civil registry (*état civil*) in 1792, identity management has been a prerogative of the French State. The economic, social and political changes that the digital revolution has brought to every stage of our lives mean that we need to overhaul the forms that our citizenship takes, as well as our competitiveness, our way of life, and how we live together, while maintaining our values and a social model of which we can be proud.

Every day, the digital world is taking shape in front of us, entering and transforming our daily lives – sometimes in insidious ways. New digital uses and unprecedented concerns are upending and redefining bonds and values.

As a result, the connection between legal identity, which is guaranteed by the State, and digital identity, which hitherto has been associated with private service providers, must be re-established and strongly asserted.

The current situation – which we will address later – means that we need to profoundly redefine the ties that bind us as individuals to the State, but also to others, in what constitutes our model of society and our shared values. Today, there are far too many sites asking people to prove their identity online. By harmonising how a person's actual identity is ensured online, a digital identity will provide citizens with greater security guarantees for many public and private uses.

We also cannot ignore the impact of a number of recent stories (Cambridge Analytica, massive data leaks, etc.) which have affected the trust citizens have in private identity providers. In the same way, misuse, identity theft and other online frauds have created an increased need for protection by public authorities. In an era where digital technology is intruding into our daily lives, often in a way that is difficult to understand, the issues of widespread surveillance and data protection are being brought to the fore, and in order to boost citizens' confidence in digital technology, we believe that taking this into account is an essential prerequisite.

Today, given that 92.4% of French people use the Internet and 59% use social media, and that government administration will be fully digital by 2022, we need to examine how to construct a controlled, secure digital identity. These figures do not factor in citizens who don't like or are not comfortable with digital tools, whom should be supported in acquiring digital literacy to enable them to be autonomous in their online activities. Given this, new uses could be designed and developed with a base of users capable of implementing and developing them more fully. Digital identity is the cornerstone of this new reality. It is the pivotal element that will determine how each of us will be able to access the wide range of uses that make up our daily lives, while respecting our freedom, integrity and individuality.

A sovereign digital identity must simplify people's lives, facilitate their administrative procedures and protect their privacy. We are convinced that only joint efforts between the voice of civil society and those active in the digital identity community can take us in the right direction.

To this end, at the French Digital Council, we argue that a sovereign digital identity should be seen and designed as a public service in its own right, with a fundamental commitment to the values of user protection, restricting data to the essential, trust and equality of all citizens in their access to rights and public authority.

An unprecedented context that forcefully raises the issue of the digital identity of tomorrow

Since a digital identity is strongly linked to civic life and to the strength of the bonds of mutual trust between citizens and the State, we at the Council have chosen to take into account the unprecedented context of the COVID-19 pandemic in late 2019. This report is not intended to draw hasty conclusions, but rather to illustrate that a relationship of trust must precede any emergency action, since it guarantees the support and full participation of citizens.

Furthermore, by making citizens one of the linchpins to resolving crises (such as the one we are experiencing), a relationship of trust reinforces their ability to take part in collectively resolving issues encountered during crises, if only through their delegation of trust to the State and their support for solutions put in place.

The pandemic's drastic circumstances (strict confinement, control of the movement of citizens, a health system under pressure, etc.) and the increasing digitisation that comes with them (widespread teleworking, rapid expansion of the digital economy, implementation of new processes for taking sick leave) have accelerated access to new public and private uses. This tension also reveals the government's prominent role in managing this crisis and the desperate need for a trusted digital environment to ensure that life can continue despite the strictest conditions ever imposed in postwar France. This unprecedented situation allows us to spotlight the reciprocal ties that connect citizens and their government.

We believe that digital identity is the primary tool that will enable us to examine our relationship with the State and with new emerging stakeholders. Digital identity will enable us to chart a correct, useful and viable path towards a trusted, inclusive and accessible paperless administration at the service of the user. Furthermore, the COVID-19 crisis has highlighted the power of solutions developed by foreign private stakeholders and the urgent need for France to develop sovereign responses that are faithful to our values.

Given the current situation, a well thought-out digital identity could also, in the future, facilitate, at least partially, certain challenges posed by crisis contexts such as the one we are currently experiencing. It could also, as called for by the community which we have consulted, generate very strong positive externalities that would be beneficial to all: innovation, jobs, investment appeal, etc. We are confident in the ability of the public authorities to make the informed choices that will support the implementation of a digital identity that is civic-minded, trustworthy, inclusive, forward-looking and conducive to the development of innovations: a French-style digital identity.

Mohammed Boumediane and Karine Dognin-Sauze,

Heads of the working group,

Gilles Babinet, Olivier Clatz, Gaël Duval, Jean-Michel Mis,

Members of the group.

Setting and working methodology

In January 2019, the *Conseil National du Numérique* (French National Digital Council) began to examine the issue of digital identity. It was not its first acquaintance with the matter as the Council worked on the Secure Electronic Documents file in 2016[1] and on digital citizenship in 2013.[2]

In July 2019,[3] the Minister of State with responsibility for Digital Affairs tasked the Council with:

- "*Exploring and developing the concept of digital citizenship, at both national and European levels, implicit in the notion of digital identity*
- *Based on the needs thus identified, proposing communication and educational materials to accompany implementation of the digital identity with an eye to improving understanding and promoting its inclusivity*
- *Ensuring, on the basis of tests carried out by the [interministerial][4] program, the ergonomics, ease of use and quality of the user support associated with the chosen solution, to guarantee take-up by the greatest number of users, in an inclusive approach*."

To address these concerns, the Council drew on scientific literature as well as the various reports published in recent years. In January 2019, it organised a one-day conference on the theme of digital identity, during which 24 experts discussed on three main topics: the market and usage, data protection and cybersecurity, and citizenship.

The members of the working group as well as the rapporteurs undertook a study trip to Estonia where they met with the staffs[5] of the e-Governance Academy, the Information System Authority (RIA), the Police and Border Guard Board, the e-Estonia Briefing Centre, the State Electoral Office, and the Foresight Centre dedicated to future e-government scenarios. The group also carried out an international comparative study of the various solutions chosen by Member States and visited Brussels.

In addition, seven consultations in French cities (Paris, Lyon, Montpellier and Douai) were held. They were structured as follows:

- Public consultations (open to all with no prerequisite, and widely publicised on social media and via the Council's mailing list)
- Consultations of experts (by invitation)

1 Opinion of the French Digital Council on the Secure Electronic Documents file (TES), December 2016.

2 Report by the French Digital Council, Jules Ferry 3.0., October 2014.

3 Letter of referral.

4 As specified in the letter of referral, the interministerial programme was officially introduced in January 2019.

5 The Council is particularly grateful to the French Ambassador to Estonia, Mr. Éric Lamouroux, and the teams that helped organise these meetings.

As part of this, over 150 people gave their thoughts on the subject. Lastly, the Council spoke with 58 individuals from government, the private sector and the academic world.

Report summary

This report was commissioned by the Minister of State with responsibility for Digital Affairs in a July 2019 letter of referral. It begins with an introductory statement that qualifies and defines the connection between citizenship and digital identities (1). Having established these definitions, the report focuses on the European perspective and the Commission's various actions (2). This enabled us to shed light on the national history of the various digital identity projects and the associated legal framework (3). Lastly, we examine the drivers that have enabled digital identities to emerge abroad as a support for a form of citizenship (4).

Although this report establishes from the outset that a public digital identity is a public service that must be universal, the first chapter focuses on actions to be implemented to ensure equality for all prior to this service, as well as continuity and adaptability. Bearing in mind that all citizens are not equally digitally literate, an updated mapping of mediation centres and the type of training available at each one should be given to users (Recommendations 1 & 2). Digital support providers play a key role in the connection between citizens and the administration and in the transmission of trust. They must be trained in best practices and protected via a legal framework and a specific toolset. (Recommendation 3).

The digital divide must be taken into account when putting administrative procedures online. The same is true for regional gaps in terms of digital coverage and access. This practice must be included starting from the design of digital identity technologies and the dematerialisation of procedures and paths, by testing whether designs are both accessible and inclusive (Recommendation 4). This feedback is critical, since the most accessible technological pathways and building blocks should be used to create benchmarks for future technological developments (Recommendation 5).

The rest of this chapter establishes that the initial interaction between an individual and his or her digital identity – the enrolment – is a crucial stage in the process. It must be inclusive, empowering (i.e. give people the ability to make free and informed use of it) and anchored in places of trust in order to uphold the relationship between identity and citizenship. To do so, we need to rely on town halls: long-standing centres for national identity card enrolment. Moreover, if the government chooses to delegate enrolment to an external stakeholder, it seems important to define this procedure via specifications that protect both citizens and staff (Recommendation 6). At the end of the first chapter, communication and training are identified as the two drivers that can bolster the government's role with respect to digital identities .

Firstly, the various government projects require greater clarity and transparency. Whether it is Alicem, the CNIe or France Connect, the lack of communication easily assimilated by the majority all too often hinders the overall project (Recommendations 7 and 10). More generally, media coverage of the how digital public services work would be beneficial

(Recommendation 8), and could address citizens' fears about how their personal data is managed and their control over it (Recommendation 9).

Secondly, and in conjunction with the deployment of digital identities, to develop real digital citizenship, citizens must be trained and widely acclimatised to digital technology. This training will have an impact if it is addressed to all age groups (Recommendations 12 and 13). Also, as representatives of an authority that affects their fellow citizens, elected representatives must be digitally trained (Recommendation 11).

To advance the goal of proposing a trusted digital identity, the report's second chapter expands on the concepts of transparency and governance, as well as security and sovereignty. From an organisational perspective, transparency through shared governance can foster the emergence of auditable and accountable trust tools (Recommendation 15).

This is the purpose of the first part of this chapter, which seeks, through governance, to place the citizen at the centre of the digital identity project. Although the government must, for obvious reasons, maintain a holistic vision of the digital identity projects that have been launched, it cannot act alone and without the support of a structured economic sector and local authorities with sufficient human, financial and logistical resources (Recommendation 16).

Furthermore, the widespread use of digital identities to prove one's citizenship is a challenge with sufficient impact to call for the introduction of new mechanisms of societal governance, including functions for monitoring and consulting civil society (Recommendations 17 and 18). A watchdog body would make it possible to support recognised players, while curbing abuses. Lastly, to increase transparency, the system would benefit from making publicly available the metadata resulting from the connections of individuals (Recommendation n°20).

Since possible digital identity abuses were frequently highlighted during the consultations. They must be defined by legislative texts. First, through improved supervision of private identity providers connected to the France Connect platform. Such providers have a partial public service remit, particularly when users are registered. As part of this, they will need to comply with strict criteria as regards staff training, clarity of services provided, data transmission and storage, and monitoring (Recommendation 19). Secondly, a digital identity reform act subject to democratic debate would help reassure citizens that the tool has been designed for and with them (Recommendation 21). Lastly, the capacity for misuse of the system by authorised personnel is a great source of mistrust. While offering a system of permissions, for better traceability, misuse and misappropriation of the system must be strongly penalised (Recommendation 22).

In a service-oriented approach and in line with the "Tell Us Once" Decree, mechanisms should be put in place to ensure transparency, access traceability and respect for consent (Recommendation 23).

Of course, architecture and security must be taken into account to achieve a system that respects citizens' freedom, technological sovereignty also affects system security. This is

discussed in the second part of the second chapter. In the reflections on digital identity and identification schemes, norms and standards are defined by international bodies, in which a strong French presence must be maintained (Recommendation 24). To ensure sustainable deployment of the digital identity scheme, European standards and certifications are to be preferred (Recommendation 25).

Furthermore, Europe, via the elDAS Regulation, has already taken a strong position on the subject. The upcoming amendment of the regulation could provide an opportunity to introduce improvements to ensure the review and notification system, and thus the security of citizens who will soon be confronted with extra-national digital identities (Recommendations 26 and 27). Moreover, the forthcoming opening of an interoperability point raises questions and calls for improved documentation on current developments and future uses (Recommendation 28). While the Regulation proposes three levels of security, everyone seeks to propose the most secure system possible in order to match uses and services to the appropriate levels of guarantee. In fact, it seems essential to encourage the development of a substantial level of state identity (Recommendations 29 and 30).

Although the control of technological sovereignty is important in international and European bodies, it is also essential on the ground and within the government itself. Subcontracting in certain areas may entail a large number of risks if the administration does not make the effort to use substantial career paths to recruit competent technical staff to ensure that it retains control over know-how (Recommendations 31 and 33). More generally, the scientific community must also be involved in examining the government's choices in terms of security (Recommendation 32) and in certifying technological building blocks and digital identity technologies.

Given that scientific choices are also political ones, some technological trade-offs are highlighted at the end of the second chapter to reduce the risks to individual freedom:

- First of all, a decentralised information storage architecture should be used and data should be encrypted
- Audits, in particular of the Secure Electronic Documents file that stores the biometric data of the National Digital Identity Card (CNIe), should be carried out more frequently (Recommendation 34). In addition, to respond in part to this first proposal, the French Data Protection Authority (CNIL)'s resources and remits need to be expanded, since they could be increasingly sought out
- Next, the CNIe system should provide the means to check information without disseminating citizens' identity data based on the theory of zero knowledge proof (ZKP)
- Finally, for the CNIe to serve as a vector of digital citizenship and the principle of "tell us once for multi-channel users" (Recommendation 35)

This report concludes that in order for a French-style digital identity to emerge, care must be taken to ensure that it is designed as the primary driver of digital citizenship. This citizenship

is likely to be reexamined and redefined in the coming years through new uses accompanied by new technical solutions. The government's arbitrations and positions, as well as the amendment of the eIDAS Regulation in the coming months, will probably affect this report somewhat, making some of its parts obsolete. Nevertheless, to date, the positions expressed by the National Digital Council reflect digital ideals that have been promoted for many years by civil society and the communities with which it is closely linked.

35 recommendations for the Government and its administration

The French Digital Council is proposing 35 recommendations to the government based on four main lines of action:

1. Promote an inclusive, cost-effective solution that serves users
2. Take an educational approach and introduce all citizens to digital technology
3. Adopt a shared and user-centric governance
4. Ensure security for all

Line of action 1 - Promote an inclusive, cost-effective solution that serves users

N°	Theme	Recommendation
1	**Mediation and mapping**	**Identify the digital mediation points on a map that is accessible throughout the user's route through administrative procedures so that users can refer to those if they experience difficulties while online.** This cartography, which could be modelled on that of SIILAB,6 should show the different points of mediation on a map, based on user needs (digital public letter-writer, social worker, Maison France Service, etc.).
2		Arrange trainings for those least familiar with digital technology in dedicated locations with substantial resources: – Secure enrolment and training in basic functions – Training for staff – Availability of walk-up equipment – Harmonised training offers for citizens based on regional needs – Recognition of varying levels of literacy
3	Support providers	Implement a basic set of rights and guarantees to protect the implementation of support providers: – Protecting users against the risks of identity theft and misuse – Protecting support providers' liability when they have to accomplish formalities for users
4	Design and user testing	Include accessibility and inclusion criteria in the design of digital identity-based services, and test them on a regular basis.

6 Mapping of SIILAB mediation sites in the Hauts-de-France region

5	**Design, security and ease of use**	**Draft specifications for identity providers that include requirements in terms of security and ease of use, while guaranteeing the benefits of uses already acquired**, for the reuse of existing authentication building blocks in mobile devices. These specifications could be used to design of high-value services, private services derived from digital identity, as well as for regional user pathways.
6	**Inclusion - Place of enrolment**	**Make town halls (and local authorities) the primary sites for digital identity enrolment to encourage trust in the government.** Precise specifications should bind those (public or private actors) responsible for enrolment: – Obligation to swear an oath and to train enrolment staff – A specific legal framework to protect citizens – Possibility for citizens to verify and amend data collected during the enrolment process – Possibility of tracking the enrolment process (particularly to prevent identity theft) – Private identity providers attached to France Connect must be able to guarantee the same level of security as public identity providers.

Line of action 2 - Take an educational approach and introduce all citizens to digital technology

7	**Communication**	**Introduce genuine communication around France Connect and the creation of the National Digital Identity Card (CNIe), including:** – Simplified, non-technical information on the security of the public infrastructures that store personal data and on the mechanisms used to guarantee confidentiality – Computer graphics, videos, educational texts, etc. on ease of use and the benefits that citizens can derive from France Connect, drawing on efforts by certain private identity providers, if necessary – A reminder that the digital identity project is at the service of broad inclusion of citizens with little involvement in the digital world – Explanations on the role of civil society and the rights of citizens to control and trace the use that is made of their data
8	Communication - Public service and management of digital information	Conduct a large-scale communication campaign on how public services function and the management of digital information, in a bid to respond to users' fears regarding potential abuses and the lack of transparency of public authorities – Legal obligations governing technical solutions deployed for the storage of information, particularly personal data – Legal obligations defining the user information that can be transmitted between central and local administrations. Restricting transmitted data to the absolute minimum to guarantee confidentiality – Supervisory bodies to ensure compliance with legal obligations
9	Communication - Personal Data - CNI	Inform citizens about their rights with regard to their personal data. In addition to long-term learning initiatives for primary and secondary school students, the Council recommends that the French Data Protection Authority (CNIL) be allocated a budget to conduct information campaigns about personal data in major media outlets and at peak listening times.
10	**Communication - France Connect**	**Engage France Connect in discussions of how it explains:** – **Its architecture** – **The relationships between the various identity and service providers** – **The different levels of eIDAS security** – **The European interoperability hub.** In particular, these discussions could be a chance to spotlight some key concepts, including: – The fact that identity providers do not know which service provider is contacting them (and vice versa) – The fact that only civil status data (to avoid duplication) and an e-mail address are communicated between identity and service providers

11	Training for elected officials	Train all elected officials and local authority staff in digital technology, based on mandatory training courses listed in a regularly-updated national training directory.
12	**Training for adults**	**In the first five years of the system's deployment, the Council recommends that the government offer free training courses outside working hours for adults on the following topics:** – Digital health and safety – How public services operate and manage digital information – Proliferation of digital identities – Consent and clarity of the TOS
13	**Continuing education**	**Create a digital citizenship training programme for primary and secondary school pupils** up to the age of 15 (the digital age of majority under the law), so that they are equipped for their first independent uses (enrolment in Parcours Sup, Le Crous, etc.) by taking up the proposals formulated in Recommendation 12.
14		Implement: – A platform bringing together all adult training courses, as well as the related legislation – An annual communication campaign be organized in high-profile media. The first cycle should deal with digital identity in connection with the government's decisions concerning digital public services.

Line of action 3 - Adopt a shared and user-centric governance

15	Transparency	Implement transparency and democratic monitoring tools already used in other contexts. These could include: – Publication of annual reports by digital identity operators: costs and investments in digital identity, reasons for technological choices, public calls for tender, training of administrative and external staff, etc. – Annual independent audit of the most critical systems by the National Cybersecurity Agency of France (ANSSI) and the French Data Protection Authority (CNIL), in addition to audits of system usability (see Recommendation 1)
16	Shared governance	Draw up a roadmap, complete with its own budget, for town halls' deployment of digital identity. This should be a joint effort with the regions for the deployment of digital identity under the leadership of the interministerial mission, in close cooperation with the Ministry of the Interior and the Minister for Regional Cohesion and Relations with Local Authorities.
17	**Societal governance**	**Create an independent, multi-stakeholder (academic, associative, administrative, etc.) control and supervision body, called the Digital Identities Monitoring and Management Commission (CSGIN), with the following remit:** – *Upstream* assessment of requests from service providers to access the "Tell Us Once" or France Connect services and evaluation of the legitimacy of their requests. – *Downstream*: o Assess independent audits o Update educational programmes for citizens o Set up citizen forums to question civil society on the subject and encourage citizen participation (see 1.2.2. below) o Refer cases to the CNIL to sanction identity or service providers who do not comply with the previously established framework
18	Societal governance – Citizen forum	Assign the body a specific remit to query and bolster digital citizenship based on the principles of citizen participation. The ability to take part offline should be included. In addition, the CSGIN could support the local leadership of discussions by helping regional stakeholders such as the Maisons France Service.
19	**Agreement for private identity providers under a public service delegation and users' consent**	**Bind private identity providers** (in conjunction with public service providers) **to an agreement that defines the delegation of the public service they are performing according to the type of action they take** (e.g., physical enrolment, activation of state certificates) and the tools they use to certify citizens' identities. **This agreement should be guided by a principle of fairness in the general interest and in the interest of users, which is more broadly part of the**

		principle of fair business relations. The public service delegation contract should therefore contain: – An obligation to implement inclusive means of enlistment – Training for staff tasked with enrolling populations in the service of digital identity in ethics and inclusion – Definition of standards for the legibility and clarity of the general terms and conditions according to criteria that include legibility, understandability by the general public, legibility testing by panels, use of French that is easy to read and understand, complete and unambiguous information on the destination, uses and recipients of the data. – The type of data transmitted and stored as part of the relationship between the identity provider and a public service – A reminder that there may be spontaneous controls of the identity provider by the CNIL – Introduction of ex-post controls by the Interministerial Directorate for Digital Technology (DINUM) and the ANSSI
20	Open data	Make available, as open data, the metadata resulting from the connections of individuals, in an anonymous, aggregated manner, so as to: – Prevent one single structure (larger than the others) from benefiting from the positive externalities of a system created by the State without redistribution – Encourage innovation and research
21	**Legislative oversight**	**Submit a reform bill that defines digital identity and its purposes and ensures respect for citizens' rights by recalling the frameworks for using digital identity data to prevent abuses (surveillance, records, etc.).**
22	Regulatory framework (1) misuses	Establish a regulatory framework that allows for the rapid penalisation of misuse, particularly by persons in a position to abuse their professional prerogatives. To deter all forms of misuse, the Council recommends that strong sanctions (fines, penalties, etc.) be strengthened and specified.
23	"Tell Us Once" and data sharing	Building on the Council's 2015 recommendations, i.e. : – "Enable each user to visualise the data exchanges between administrations for the provision of a service, as well as how long they are kept on file – Provide for default user consent as regards the exchange of personal information between administrations, subject to the cases of unauthorised exchanges provided for by law or decree."

Line of action 4 - Ensure security for all

24	Sovereignty - Presence in supra-national bodies	Bolster French representation within European and international standardisation bodies, which are a strategic place of influence and standard creation around digital identity. It is critical for the Ministry of Foreign Affairs to monitor these issues and to allocate the necessary resources to carry out informed monitoring and influence, with the support of other ministries concerned.
25	Sovereignty - Capacity for technology assessment	Use norms from European standards institutes (ETSI, CEN) which are nationally recognised as proposed by the European Commission. Indeed, "as part of Mandate M/460, the goal of which is to provide a coordinated response concerning the deployment of a single European digital market, ETSI (European Telecommunications Standards Institute) and CEN (European Committee for Standardisation) have been entrusted with the task of drawing up standards relating to the trust services provided for by eIDAS." In a second stage, certification should be carried out by bodies operating under the same legal rules as the companies seeking validation and the bodies promoting standards.
26	**Amendment of the eIDAS Regulation**	– **Standardise the peer review process, particularly in terms of documentary reference and methodology, and clarify its purpose and scope.** – **Define a set of documentation containing the information to be automatically communicated by the Member States on their electronic identification schemes.** In this respect, the Council agrees with the recommendations made by the ANSSI on the amendment of the eIDAS Regulation to unify security practices within the Member States and thus promote mechanisms for mutual recognition and interoperability of electronic identification schemes. It should be noted that this is not the Agency's top priority for the amendment of the Regulation, which considers that **it should start by clarifying the Regulation's requirements concerning substantial and high levels of security.**
27	Amendment of the eIDAS Regulation	Define the minimum criteria for remote identification in the eIDAS Regulation. Harmonisation and means for assessing the reliability of remote identification methods (e.g. the number of steps to accomplish by the user in terms of facial recognition, or standardisation of the false positive/false negative rate impacting the percentage of identification) would be welcome for the purposes of harmonising practices implemented in the Member States.
28	**eIDAS - interoperability point**	**Issue more information about the implementation of the French eIDAS point. Moreover, this point should not be supported solely by the department in charge of France Connect within DINUM; specific resources should be dedicated to it. Finally, it must be constructed in close collaboration with ANSSI and CNIL.**

29	eIDAS - interoperability point	Adjust the substantial guarantee level with a corresponding public digital identity solution (after determining the typical use cases for this level). Cf. Recommendation 30) Moreover, it would be appropriate to encourage States that already have a high-level solution to produce a substantive solution. France could begin to move in this direction.
30	**Homogenisation of security levels of procedures**	**Define, under the leadership of the government departments concerned, the levels of guarantee required for each online service and create guidelines to enable departments to easily establish the level of guarantee for new public services. These guidelines could then be proposed at European level with a view to possible harmonisation between Member States.**
31	Technical skills	Ensure that skills outsourced by the government are also mastered internally, to prevent dependence on subcontractors, which puts the system's sustainability at risk and loses the system's technical history (errors, correction of errors, reasons and choice of architecture, etc.). Technical skills need to be sourced on a massive scale with a career plan enabling staff to join the administration over the long term, and these new staff need to be integrated into DINUM's appropriate digital identity mission.
32	**Expert assessment**	In addition to the recommendations concerning involving the scientific community in the standardisation process (cf. 1.1.), the Council would like to put a recommendation from its opinion on the TES file back on the agenda. The Council believes that **the scientific community should be consulted, in support of the governance body, on the security choices for technologies deployed by the government, in particular through:** – **Evaluating the solution** – **Risk and cost assessments** – **Creation of the system architecture**
33	Sovereignty	Earmark budgets for certifying digital identity technology, and/or technology building blocks related to digital identity. The needs of companies in the community that do not wish to offer a complete digital identity scheme but only a building block need to be assessed. In fact, existing funds would make it possible to foster certification under the principle of peer review, in connection with the national academic centres of excellence, ANSSI and CSGIN.
34	**Audits of the Secure Electronic Documents file (TES)**	**Carry out both regular and unscheduled audits and controls of the Secure Electronic Documents file (TES) and the uses made of it by the ANSSI and the CNIL.**

35	National Digital Identity Card (CNIe) - certificates to allow the continuation of the "Tell Us Once" initiative via multiple channels	Insert into the National Digital Identity Card (CNIe) an authorisation certificate for administrative staff, allowing them to access information already known to the administration at the counter without the user having to bring his/her documents. Some form of explicit consent to this transmission via the government pathways needs to be put in place (e.g. on-screen signature).

About the French Digital Council

The French Digital Council is an independent advisory commission with a remit to produce and publish independent opinions and recommendations on any questions relating to the impact of the digital transition on society, the economy, organisations, public action and France's regions.

The Council reports to the Minister of State with responsibility for Digital Affairs. Its articles of association were amended by the Decree of 8 December 2017. Its members are appointed by order of the Minister of State with responsibility for Digital Affairs for a two-year term.

Media contact

Charles-Pierre Astolfi, **CNNum General Secretary**

presse@cnnumerique.fr / +33 1 44 97 25 08 / +33 6 81 69 07 21