WHITE PAPER

DIGITAL IDENTITY 5.0

LEXING
ALAIN BENSOUSSAN AVOCATS

WHITE PAPER

DIGITAL IDENTITY 5.0

CONTENTS

FOREWORD **ALAIN BENSOUSSAN**

As the real and virtual worlds are merging, digital identity is a key issue.

As we know, the identification of a person is a vital technical and legal prerequisite to the trust and security of electronic transactions (such as message exchanges, contracts, procedures, internal workflows).

Guaranteeing the confidentiality and legal value of digital exchanges by irrevocably identifying the authors of the content, the senders, the recipients and all authorised third parties at each critical stage is therefore a major challenge.

This is all the more true given the increasing number of autonomous entities used to perform tasks for which they have been designed and "mandated", e.g. robots, artificial intelligence, connected devices[1].

These are all new actors that must be identified amid continually rising fraud and cybersecurity risks.

Digital identity is defined by the Karamanli, Hennion and Mis[2] parliamentary taskforce as *"the ability to securely use attributes of our identity in order to access a set of resources"*. On March 14th 2011[3], the Framework Law on Internal Security Enforcement (LOPPSI 2) enshrined such Digital Identity with the creation of a new offence regarding online identity theft.

Digital identity is by nature reserved for artefacts implemented in the virtual world; in other words virtual personalities, of which avatars are the first materializations. On the other hand, the success of social networks with their multiple forms of digital identity do multiply the risks of spoofing identities as well as risks for a business becoming a victim of data theft or disinformation campaigns.

Entitled "Digital Identity 5.0"[4], this White Paper first aims at simplifying and improving the legal understanding of the many papers and news on digital identity.

Let us cite a few examples:

- Enactment, under the impetus of the European legislator of numerous legislative and regulatory texts involving an electronic identification component; in particular the 2014 e-IDentity And Signature (eIDAS) Regulation;
- Creation in 2018 by the French Government of an inter-ministerial taskforce for the deployment of a secure digital identification journey;
- Launch of a digital identity project supported by the initiative 'France Identité Numérique';
- Implementation in 2016 of 'FranceConnect', an identity federator, and then in 2019 testing of ALICEM, the first secure government digital identity solution;
- Introduction of an electronic national identity card for French citizens by summer 2021, in order to bring France into compliance with European law.

This White Paper also aims to lay the foundation for the implementation of digital identities that are "interoperable and inter-enforceable in an ecosystem in which operators are no longer issuers but only guarantors of procedures".[5]

Questions about ethics, trust, security and privacy protection are critical in both the real world and the virtual world. This White Paper has the merit of directly addressing these topics, thereby contributing to the global emergence of a universal and irrevocable identity that is supranational and enforceable against third parties.

Alain Bensoussan
Lawyer
Alain Bensoussan Avocats Lexing

[1] By giving them a dedicated legal personality: See in this sense Alain Bensoussan et Jérémy Bensoussan, IA, robots et droits, Bruylant 2019.

[2] Joint taskforce by the Commission for Laws and the Commission for Economic Affairs of the French National Assembly chaired by Marietta Karamanli (Soc), with Christine Hennion and Jean-Michel Mis (LaREM) as corapporteurs, whose report was published July 2020.

[3] Law No. 2011-267 of March 14th 2011"Loi d'Orientation et de Programmation pour la Performance de la Securité Intérieure" (LOPPSI).

[4] Identity 1.0: seals and banners;
Identity 2.0: baptism registry, then civil register, which led to the national identity card;
Identity 3.0: digital revolution: email address, Google or Microsoft Live account, and many other "login ID";
Identity 4.0 cryptographic certificates and digital identity cards, which led to eIDAS.
Identity 5.0: irrevocable and supranational digital identity

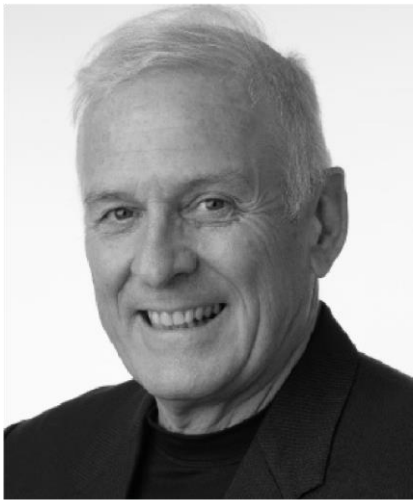
[5] See Chapter 7.

FOREWORD **PHILIPPE MOREL**

Civil registers were created in France in 1792. Since their creation, the control and management of identities have been under the sovereign responsibility of the French state.

The arrival of digital technology has disrupted our perceptions, in particular because anonymity is king and there are no borders on the Internet.

What happens to the concept of sovereignty in a digital world? Do we have new judicial territorialities? What about personal and national sovereignty?



As digital technology permeates all aspects of our lives, it challenges the rights we acquired in the physical world and invites us to rethink, or even recreate, the cultural and behavioural components from which our values were built. These same values that shaped our societal model – can we preserve it? These values are constantly, sometimes even unconsciously, challenged by new, ever-evolving and constantly growing digital behaviours.

It is a digital universality that disturbs the links and values that unite us to the point of questioning the principles of trust, respect for privacy, the secrecy of communications, and our trade secrets; in short, the nature of our free will. And that forces us to redefine WHO we are and for what common project.

The marketing pledge of the trust market insinuates that authentication would be sufficient to protect fundamental rights. In the same way, some people believe that a digital signature replaces identity, or that cryptographic certificates would be sufficient to create an identity. This is not legally true.

An identity is unique and constant.

The multiplication of identity thefts along with massive data leaks have destroyed the idea that businesses and citizens can trust public and private identity providers.

The rapid increase of these cases and modern means of mass surveillance vow with force and urgency the necessity to set a path for a legal and technological evolution at the service of a true digital identity. One that would be enforceable against third parties in a supranational environment. One that would protect our rights.

No industry can evade the law.

The Internet has become a tool of everyday life. An ever growing number of French businesses and citizens are using social media. Government services are going digital at high speed. The European Union is launching a 'Horizon 2030' investment plan in which New Tech is central. The digital identity market is estimated to be the biggest market in the digital world. It is therefore essential that all actors (natural and legal persons, robots and other automatons) be provided with a universally recognised identity offering everyone the legal means for the strictest protection of their privacy.

Can we do more business with less trust?

The freedom of each person and our sovereignty in general are questioned.

Philippe Morel
Digital identity specialist,
co-founder of Woobe

FOREWORD **BERNARD HAUZEUR**

“Remarkable!” This is what comes to mind when reading the latest information report on digital identity[6] by the French National Assembly; far from us the intent to plagiarize this public document, which we recommend reading as a preamble to this White Paper.

In addition to presenting the state of the art of digital identity in France, this report makes 43 recommendations for *“the rapid deployment of digital identity*” (sic). This large number of measures raises questions: if so many measures are necessary to reach my goal, shouldn’t I question either the goal I have set for myself or the path I am taking to reach it?

- Questioning the goal? This would mean questioning the aspiration to a reliable, universal digital identity; an identity at the service of citizens and honest commerce, safe from abuse and misappropriation; an identity clean from all the wickedness made possible by typical self-assigned avatars. This would be to deny its very existence: there is no such thing as a half-identity!

- Questioning the path? That is precisely the proposal developed in this White Paper.

Our “digital identity” boat is leaking on every side. Fact is, this boat has been assembled while already sailing the virtual ocean. Shall we then consider that we are too far from any harbour and thus have no other possibility than sealing off leaks by all possible means? … from the inside of the boat? … while embarking millions of passengers? Or can we not, instead, land somewhere and ask our naval architects to design the ship of the virtual century?

In the 1980s, when computers were just starting to be interconnected, it became more and more clear that it was also necessary to think about putting locks on the doors thus opened: computer security as we know it was invented.

At the beginning of the 1990s, with the multiplication of personal computers, local networks were invented, and then the network of networks: the Internet.

From the interconnection of computers, we moved to the connection of people to computers, and then of people with each other. We started to think that we could identify people with cryptographic certificates as we do to interconnect machines reliably. We remained focused on security issues (already so much damaged by a too rapid evolution) and totally missed something fundamental: the Law. In particular the Law that affects the "person".

Of course, since the middle of the 1990s, voices have been raised and attempts have been made to fix it by sticking Law on top of what was done. The result: eIDAS[7] which tells us: it may be you (at “low” assurance level), it is probably you (at the “substantial” level), or it is almost totally you (at the “high” assurance level, using a so-called “qualified” certificate).

The requirement for a proof, which was previously subject to an obligation of result, has been replaced by a risk with best effort duties. Is the protection of my identity just a question of economic means? Can I accept the risk that my identity provider may be hacked or bankrupt and leave me without compensation? Is there an alternative that would guarantee the result? At minimum, we must ask ourselves the question.

How can we go about it? Undoubtedly by considering what was initially forgotten: the Law.

Mathematics teaches that a few well thought-out axioms are enough to build coherent universes with infinite possible applications. So, the question is: what are the axioms of digital identity?

Bernard Hauzeur
IT architect, security and digital identity expert,
co-founder of Woobe

[6] Mission d’information de l’Assemblée sur l’identité numérique, National Assembly Report N° 3190, 8 July 2020.

[7] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014.

FOREWORD **DINESH UJOODAH**

The recent pandemic has incredibly accelerated the digital transition and our digital practices. More than ever, we want to find in the digital world via our remote interactions, the trust that we enjoy in the real world when we act everyday and carry out transactions.

If you closely look at it, the concept is obvious: in a digital world, how can we ensure that the person undertaking a transaction via their favourite mobile device or the internet is really the person who they claim to be? How can we give the other party the necessary guarantee and confidence required to close the transaction? If we cannot do that, then it is clear that the entire development and potential of remote services may be questioned.

Beyond the benefits in terms of law, citizens with a true digital identity will experience new and greatly simplified digital journeys because access to their data by foreign ecosystems would be carried out in complete confidence. Actors will be linked together by a federation of identities that can trust each other.

Ensuring the truthfulness of digital identity is vital! It is the key to accessing all the services upon which we increasingly rely, and where trust is central: identity enrolment and automated verification services (KYC/KYB), relevant and even personalized health services, access to administrative and public services, notary, succession, education and mobility. We shall not forget to cite the authentication of online payments, strong & simplified authentication of in-store payments, credit subscription services carried out with three authentication steps...

Digital identity is ultimately the basis of our freedom, precisely of our new Freedom in the digital age. And how would we ensure that every citizen can enjoy their digital identity for free?

Digital identity is the keystone of the new digital world. We have to lay down its fundamentals in terms of law. This is precisely the objective of this White Paper. It is one of the major challenges we face. What if the next global virus was not biological but digital? What if our identity in the digital world gets stolen?

It is in this spirit that A3BC (Anything, Anytime, Anywhere Biometric Connections), a private actor of the French Tech, complements the French state's digital initiatives to provide private businesses and individuals with a universal digital identity and strong authentication. We offer solutions that are extremely secure, relying among other things on (local and centralized) biometrics to simplify their use, as well as on patents for data storage.

Our platform is of course compliant with the European General Data Protection Regulation (GDPR) and, in order to meet the challenges of User-Centric Identity, we are now starting the eIDAS certification process by integrating new technological advances such as blockchain (self-sovereign Identity).

The aim is to give back to each individual the mastery of their personal data, the control on its use, the necessary trust to choose the services they prefer, and ultimately allowing everyone to control every aspect of one's life!

Dinesh
Ujoodah
CEO, A3BC

THANKS

1. Sincere and warm thanks to Lucien Pauliac, Director of SCRIPTUM-Archives, for his technical support. Lucien's expertise in the preservation of evidence was of great help to us.

2. Thanks to Anthony Sitbon, consultant, Head of the Security Department of Alain Bensoussan Avocats Lexing, who coordinated all the technical and human resources required for the creation of this White Paper, and without whom nothing would have been possible.

3. Thanks to the lawyers of Alain Bensoussan Avocats Lexing involved in the preparation of this White Paper:

- Éric Bonnet, lawyer, Head of the Legal Communication Department;

- Isabelle Pottier, lawyer, Head of the Studies and Publications Department.

1.PREAMBLE

This White Paper lays the foundation for the implementation of digital identities that are “*interoperable and inter-enforceable in an ecosystem where operators are no longer issuers but only guarantors of procedures”*.

4. The year 1792 marks the creation of the civil register in France. Since then, the management and control of identities have been under the sovereign responsibility of the French state.

5. It was not until the 1990s that the inexorable rise of the Internet called into question many certainties and achievements. The creation of a new, borderless world, in which anonymity is king, defines new sovereignties which are no longer held by states, but by the new technical and economic actors of the Internet.

6. The power of giants of the Internet is now considered more important than that of many states, obsoleting the very concept of state’s sovereign power, and of new non-geographic legal borders. As digital technology permeates all the aspects of our lives, the rights that we acquired and considered intangible are challenged: privacy for everyone, trade secrets for businesses, and trust between all actors of our society: public actors, private actors, and citizens.

7. These values are constantly, even if sometimes unconsciously, challenged by new, ever-evolving and constantly growing — and even uncontrolled —digital behaviours. The ability to track you everywhere at all times, and the continuous rating of your choices and activities against a “profile”, are these a tool of domination? Or just a nice commercial plus: “we’ll make you happy”? Or a national security issue?

8. This digital ubiquitousness disrupts the ties and values that unite us to the point of questioning our free will. It forces us to redefine WHO we are in this parallel digital world, and for what common project.

9. The marketing pledge of the trust market asserts that better computer security would be sufficient to protect fundamental rights. Similarly, many of us believe that a digital signature can pledge the identity of individuals and companies because linking a cryptographic certificate to a person would be enough to create an identity.

10. However, this is not legally true.

11. Back to origins: in our democracies, sovereignty is the expression of the collective will of citizens. And there can be no “collective” without a “community”.

- The first example of a “sovereign community” is the state, which is historically based on a territory. The Identity issued by the sovereign state is the cornerstone that makes each member of this community responsible towards others and the collective good. Identity provides us with control[8] over the extent to which we accept the personal and collective spheres to penetrate, thanks to the system of Law applicable in this “community”, and with which this community has sovereignly endowed itself.

12. The virtual world has created “digital identities” — that is a fact[9]. They escape our control, hover over our future, and are attached to NOTHING sovereign or collective, but to the service contracts of foreign commercial companies, the Big Tech's[10] notably, fully endowed with private interests.

13. The question of sovereignty is key to identity. If identity is not linked to a community in which there is a sovereign system of rights and obligations, then we are not free, but enslaved.

[8] ... or severe supervision, in the case of authoritarian states! Personal control = freedom, state control = authority.

[9] Clearly stated and reviewed in depth by Blandine Mallet-Bricout and Thierry Favario ("L’identité, un singulier au pluriel", Dalloz 2015) and Nicolas Chambardon ("L’identité numérique de la personne humaine: contribution à l’étude du droit fondamental à la protection des données à caractère personnel", Thèse de doctorat en Droit public, 27-09-2018).

[10] Google, Amazon, Facebook, Apple, Microsoft, and all the others by extension such as Tencent, ByteDance, Snap, Uber, Baidu, Alibaba.

The "digital identities" by Big Tech companies are not sovereign at all: they are bound to the opaque lines of code of their apps and unilateral user agreements.

14. The question of identity is closely linked to the concept of sovereignty; both individual and collective sovereignty (community). But there is no Internet sovereignty: "*States are places, the Internet is a link. Sovereignties are defined in delimited physical spaces, the Internet is a dimension that connects all territories without being one itself*"[11].

15. The digital world has broken down the borders of states and Big Tech companies have taken control, much to our dismay! However, it is the states that are the custodians of the sovereignty of a system of Law capable of protecting businesses and citizens on their territory. States are neither in a position, nor do they have the means to impose themselves as the "communities" issuing a universal "identity"[12] unless they transform themselves into a "digital territory"[13]; Big Tech companies have largely preceded them and have taken on this role.

16. Today, industrial companies stick to their strict needs, namely to IAM (Identity & Access Management) systems that are part of their IT infrastructure. These systems focus on mutual recognition only between local employees.[14] Then, they use cryptographic certificates supplied by some PKI[15] for securing exchanges with the external world and ensuring mutual authentication between remote systems, between remote people, or between people and systems.

17. This is not enough to create an "identity" on the web. On the other hand, these legal persons — the companies— are attached by nature to a system of Law. They form natural legal communities issuing mandates (employment contracts, representatives) which govern a large part of our identity and our life: our work time. Moreover, companies have means and speed of action that the state cannot afford.

18. In fact, Microsoft, Google, Facebook and a few others have shown the way: companies can issue digital identities[16]; however such identities are in the hands of companies whose purpose is to monetize our private lives. We must instead allow the companies that employ us (and not only big Tech's) to become issuers of digital identities[17], which can be legally enforced[18], on a universal and sovereign basis, and allow mutual recognition.

19. This would enable a partner of a company to accept the identity assigned by a third party (e.g. to temporarily hire a third party's consultant, to negotiate with a new partner) and have the guarantee that this recognition is based on the foundations necessary for the legal protection of its business.

20. The IAM investments and personnel management work of all private companies would earn added value as the identities thus issued become useable outside the company walls for business purposes.

21. This.is.me@SomeCompany.com would no longer be a presumption, but a source of certainty.

[11] Pierre Bellanger, "La souveraineté numérique", Édition Stock, January 2014.

[12] Very few states in the world currently provide their citizens with an "electronic" identity, which in any case does not relate to any identified "digital community", and has no legal status of its own. It is just a technical means of authentication recognised by a number of service providers, including state administrations. And as it is a preformulated standard contract, the quality or weakness of this means is only binding on its issuer, the state, unless a fault from the user is proven. Credit cards issued by banks are subject to the same scheme. There is nothing bilateral between two partners (I identify you, you identify me), neither balanced, as must be the case for trade.

[13] For example, China, for whom an overly open Internet endangers its political system and authority.

[14] What's worse, with the cloud, more and more companies are enslaving their IAM systems to the online collaboration and desktop applications of the same digital giants. Not only have these giants access to all personal identities, they are also taking control of business identities, and - icing on the cake – they are offloading the costs of administering and maintaining these identities!

[15] Public Key Infrastructure (PKI), who issue cryptographic certificates.

[16] Visa, MasterCard, Amex and others have also shown the way by distributing credit cards, a substitute for a digital identity, with a system of recognition by third parties (the banks), but in a field closed to their business and a single type of trade: payment.

[17] This is a claim far from the case of a company outsourcing issuances of cryptographic certificates for every employee, as we will later see in this White Paper.

[18] Big Tech companies do not care about a "legal" identity. They only need monetizable traces; self-assigned identity is more than enough. Safe behind their contractual clauses, they don't feel responsible for the wrongdoings of their members. Worse: a strong digital identity would be a hindrance and would involve them legally. It is in their interest to maintain weak but economically viable digital identities.

2.OBJECTIVES

2.1 Background

22. This White Paper proposes a basis for building digital identities in the context of sovereign communities, whether they be at the level of a state, a commercial company, or a simple interest group.

23. Communities both in the real world (companies, institutions, administrations, associations) and in the virtual world would be invited to implement interoperable and inter-enforceable digital identities in an ecosystem in which operators are no longer issuers[19] but only guarantors of procedures.

24. This basis will also reconcile the need to identify any autonomous, acting and legally accountable entity: robots, connected devices, and even artificial intelligence algorithms with whose decisions we are increasingly confronted.

25. This digital identity recognises the pre-eminence of mandates in the execution of any task:

- In business, you rarely act on your own behalf, but on behalf of your company or your employer. The professions — take a doctor — have an equal need to isolate their family from their medical liability.

- You cannot self-declare your identity or function and then obtain effects under Law. There is always a third party who confirms your attributions (e.g. a human resources director), your citizenship (civil registrar), or your status (register of legal persons). You are mandated in your functions, and the person who assigns such mandate to you must of course themselves be mandated to do so on behalf of the community (institution, legal person, state) that such person represents.[20]

- Mandates are the key to grant legal personality (together with the related liability) to our intelligent artifacts: vehicles, connected devices, robots, and algorithms that bear a decision-making autonomy and a capacity to act in the real or virtual world.

- Legal entities have a legal existence and an identity, but no capacity to act directly but through their duly mandated representatives.

- People who are in physical difficulty (handicaps) or financial difficulty (lack of necessary computer equipment) can naturally mandate a third party to act on their behalf, subject to the scope of the mandate.

26. A person's identity cannot be reduced to their signature alone, whether in the real world or in the digital world:

- A person's identity is found in all the acts of that person's daily life, e.g. when carrying out administrative procedures, giving consent (order, electronic signature), accessing a service or an account, publishing a document, obtaining a diploma or a professional certification, managing (intellectual, industrial, commercial) property, and ensuring the smooth running of both personal and business affairs (e.g. buying, selling, hiring, authorizing, sharing, producing, paying, delivering).

- For a robot, the issue is generally to identify it in order to enable it to perform the tasks for which it has been certified (autonomous driving, medical prescription, handling) within the scope of action (road, city, care facility, warehouse) for which it is mandated.

27. Identity is the basis of mandates, and thus of the capacity to act (what can I do, to which extent, on whose behalf), both for persons and for intelligent artifacts. It also affects archiving (my documents, those of my companies, the memory of a robot) and storage (land registry, publications, assets, public registers, traces of a robot in public places).

28. This White Paper is politically neutral. It does not advocate the obligation to use a digital identity or the disappearance of anonymity on the Internet. It places no limits or restrictions on the applications or exclusions of the digital identity it proposes.

[19] In contrast to PKI (Public Key Infrastructure).

[20] A PKI does not represent any professional community and therefore does not have the sovereign power to assign identities to members of a community it does not represent; it needs to change its role from issuer to provider of the means for each community's rights holders to exercise their sovereignty, starting with the creation of digital identities.

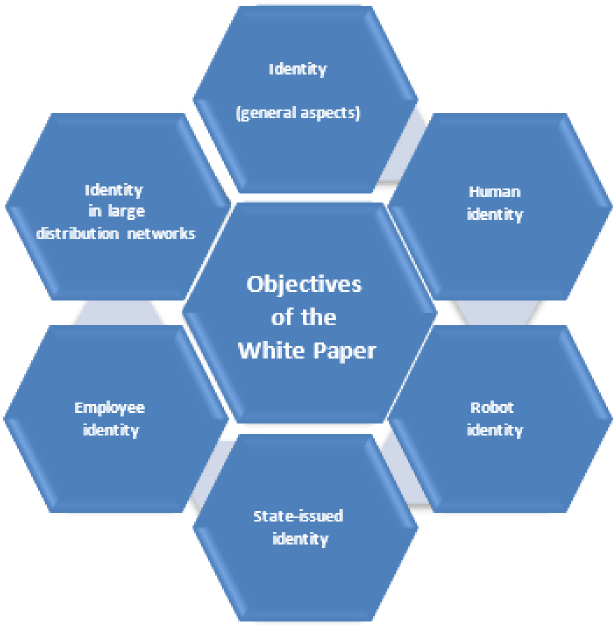
29. It proposes an ecosystem of sovereign communities, which will be autonomous and free, like individuals, to express their choices, their wills, and their own rules and limits in a transnational framework that allows for legal inter-enforceability.

30. It leaves open the possibility of imposing a single state-issued identity at the level of the State, or accepting the multiplication of mutually recognised identities at the level of sovereign associative, commercial or even individual communities.

31. This White Paper is based on the system of Civil law or Roman law as opposed to Anglo-Saxon law or Common law, and focuses more specifically on the European scope. Beside, authors do believe that if used in a Common Law system, this white paper contains all the elements to create the necessary jurisprudence.

32. This White Paper is technologically neutral. It does not evaluate or recommend any technical solution, as these are in constant development; it formulates the functional and structural requirements necessary for the effects of the Law.

33. In this document, each structural or functional requirement derived from the logic and/or principles of Law will be clearly marked with the following symbol: ⚠



2.2 Who is this White Paper for?

34. This White Paper is aimed at professionals of private or public structures and is designed to help them solve the problems they may face as a result of legal and technological constraints when they implement a digital identity solution: any solution applicable to the relationships between natural persons, legal persons, and intelligent artifacts (autonomous vehicles, AI, connected devices) as the latter play an increasingly important role in the functioning of the society as a whole.

35. This White Paper is intended to be educational, to support studies in this field, and contribute to the academic and/or normative debate.

3.BIRTH AND IDENTITY

Digital identity is defined by the Karamanli, Hennion and Mis parliamentary taskforce as *“the ability to securely use the attributes of one’s identity to access a set of resources*” (Ass. Nat. Report No. 3190, 8 July 2020).

36. “A person’s identity can be seen as a set of components through which it is established that a person is indeed who they say they are or who they are assumed to be”.[21]

37. “Digital identity is defined as a technological link between a real entity (individual, organisation or company) and virtual entities (its digital representation(s)). It allows the identification of the person online and their connection with all the virtual communities on the Web[22]. The digital identity is not only built by the real entity, or the “Subject”, but also greatly influenced by the relationship that the latter has with others and with society[23]”.[24]

38. For a very complete analysis of all the aspects of identity in Law (and its consubstantial counterpart: anonymity), reference is made to the proceedings of the colloquium on identity organised by the University of Lyon.[25]

3.1 What do our institutions say?

39. If you search on the Internet for “digital identity Europe”, you immediately come across the European regulation known as “eIDAS”.[26] This regulation, adopted in 2014 by the European Parliament and the Council of the European Union, came into force in France the same year.

40. It primarily concerns public sector bodies and trust service providers established in the territory of the European Union. The objective of eIDAS is to establish a suitable legal framework for enhancing trust in electronic transactions related to electronic identification and trust services within the European Union market and thus fostering the emergence of the digital single market.

41. Its objective is to create a common basis for interoperability that the previous electronic signatures directive 1999/93/EC had not succeeded in creating; hence, it does not call into question any of the existing practices that consist in assigning a cryptographic certificate to a person as an identity. A cryptographic certificate is the minimum basis for the technical creation of an electronic signature; one signature = one person, so one person = one certificate.

42. This is the implicit reasoning held for decades and by eIDAS as well. This application of cryptography is widely standardized, and concomitant with the rise of public key infrastructures (PKI). An eIDAS implementing Regulation (2015/1502) specifies how to implement the related technologies in order to promote interoperability, and even proposes open source software.[27]

43. The eIDAS regulation contains no definition of identity and is limited to the identity of natural and legal persons. It refers to the attributes of an identity without defining them.

44. The French National Assembly’s report[28] on digital identity is more detailed. In its introduction, it refers to the multiplicity of definitions and introduces the concepts of identifier and “pivotal identity” *(identité pivot)*, which form the basis of the FranceConnect project.

45. Regarding the concept of identity, the report contains a reminder of history and recalls that written documents replaced face-to-face commitments, leading to the creation by the French state of civil registers. These replaced the “registers of baptisms” made compulsory by François 1st.

[21] Serge Guinchard, Gabriel Montagnier, Lexique des termes juridiques, Dalloz 16e éd. June 2007.

[22] Cited by Fanny Georges, « Représentation de soi et identité numérique. Une approche sémiotique et quantitative de l’emprise culturelle du web 2.0 Réseaux, vol. 2, no 154,2009, pp. 165-193.

[23] Cited by François Perea, « L’identité numérique : de la cité à l’écran. Quelques aspects de la représentation de soi dans l’espace numérique », Les Enjeux de l’information et de la communication, vol. 1, 2010, pp. 144-159.

[24] fr.wikipedia.org

[25] Blandine Mallet-Bricout and Thierry Favario, L’identité, un singulier au pluriel, Dalloz 2015.

[26] Regulation (EU) No. 910/2014 European Parliament and the Council of the European Union of 23 July 2014.

[27] Digital Signature Services DSS https ://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/DSS.

[28] Mission d’information de l’Assemblée sur l’identité numérique, Rapport Ass. Nat. N° 3190, 8 July 2020.

It was the French revolution that took the registers out of the hands of the Catholic Church and entrusted them to the state, thus creating the state-issued identity, so-called sovereign identity *("identité régalienne")*.

46. A book is therefore used to record the information that allows each individual to be identified: last name, first name, place and date of birth, the identities of the father and mother, sometimes accompanied by their occupations, their signatures, and the name plus signature of the civil registrar who records this information. A reference number is assigned to each entry in the register.

47. Today such information is communicated electronically to the public administration by the maternity doctor as soon as the birth takes place. A national identity number is assigned.

48. At birth, a new being[29] is given a first identity linked to their legal personality; it is as simple as that for natural persons.

49. For legal entities, it is very similar: the court's registrar records the identification information in the Trade and Companies Register: company name, company type and tax scheme, address of headquarters, type of activity, articles of incorporation, representatives.

50. With a few variations, the principle is the same throughout Europe.

51. What about robots and other intelligent artifacts? Nothing; although a lot of work is being done on the subject by Europe (e.g. eu-Robotics), states, and private consortia.[30]

3.2 The identity of artifacts: robots, AI algorithms

52. Our world is no longer limited to natural and legal persons. Robots are becoming increasingly intelligent and autonomous. The digital world is populated by Artificial Intelligence algorithms that are making decisions that are already impacting our mobility, our careers, our health, our encounters, and even our opinions, with impacts in the real world. The coming robohumanity cannot be excluded from the question of digital identity.

53. The book "*IA, Robots, et Droit*"[31] (AI, Robots, and Law) makes a very comprehensive analysis of the issue. The authors note that the idea of a legal personality for robots is accepted even if its status is not finalized or if the registers of "electronic persons" are not implemented. The book proposes a Charter of Robot Rights whose article 3 defines a legal personality "consisting of rights and obligations exercised by its legal representative". "A robot person has its own identity, an identification number, and a capital whose sole purpose is to repair any damage caused by it".[32] This remains a proposal, but it clearly gives a direction to follow.

54. In the case of intelligent artifacts (robots, algorithms) forming complex assemblies — such as an autonomous vehicle — the question of the number and boundaries of identifiable entities may be raised. The vehicle operator can legitimately subcontract the driving to an intelligent "co-pilot" software[33] maintained and operated by a third company, and opaque to the vehicle operator. The "pilot" software detects the state of the road, the existence and nature of obstacles and continuously informs the robot-vehicle which manages speed, direction, and the roadmap.

55. According to their respective intelligence, one could assign 1 or 2 identities (with their associated liabilities) in the same way as a pilot plus co-pilot, or zero if the will is to focus on a transport operator responsible for the whole. The operator is thus in charge of organising with its subcontractors the respective responsibilities of the manufacturer (mechanical failure), the maintenance company (maintenance failure), and the vendor of the driving software (navigation failure).

56. The digital world makes copying easy and even necessary for the different stages of production, for backups, or for the distribution of the data processing load. What do we do with copies of the same AI algorithm in several environments? Do they have multiple identities or just one? What if a hacker hijacks a copy to enslave it to his own purposes? Is this copy still the same entity?

57. The Law already deals with the case of kidnapped persons acting under duress. The multiplication of

[29] The Law recognises the existence of an identity before birth and after death, see Blandine Mallet-Bricout and Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015.

[30] A detailed inventory of all these initiatives can be found in "IA robots et droit" of Alain Bensoussan and Jérémy Bensoussan published by Bruylant, Editions Larcier, collection Théorie et pratique, July 2019.

[31] Alain Bensoussan, Jérémy Bensoussan, « IA robots et droit », cited above.

[32] « IA robots et droit », annex 19, cited above.

[33] We are talking here about AIs capable of dealing with new situations and whose experience determines their response. Even a very sophisticated GPS that plans the route remains a technical component.

legal copies of the same algorithm does not avoid the question of the liability of each "copy": one viewpoint is that these "copies" are just technical elements in the architecture of a single logical entity; alternatively these copies can be considered autonomous when, for instance, they are in the hands of different operators and therefore form as many independent, communicating, and accountable entities.

3.3 What does the law say about identity?

58. Let's now leave aside philosophical debates on identity, and nuances such as *ipse* or *idem*[34], to focus on the most reduced identity, the one that is strictly necessary to the creation of a digital identity carrying legal effects.

3.3.1 Legal personality and digital identity

59. The Law recognises the biological identity of an individual, their physical and mental autonomy, their capacity to act[35]. Now, if we extend the field of entities to be taken into account to legal persons, robots, AI and digital avatars, then the aspect of an identity at stake is that which confers legal personality and related rights and obligations.

60. In practice, such identity is the one that arises from an inscription in a register of the attributes necessary to its univocal identification. Such inscription establishes the existence of an entity legally responsible for its acts. It may be accompanied by indications of property (owner of all natures), physical integrity (mechanical for the robots), digital integrity (algorithms and metadata), and tangible plus intangible assets (such as reputation, works, authorisations, contracts, capacities, expertise, customers, memory, knowledge, digital data, and capital[36]).

61. We are perfectly aware of the risk of falling into what Professor Grégoire Loiseau denounces as a drift towards a "techno-personalism favouring the colonizing of human rights for the benefit of entities that are nonetheless totally devoid of any sense of identity and of perception of themselves".[37] It is not our intent to reduce the human person to an "organo-mechanical" entity. It will never be said here that the Law applicable to a human person cannot take into account many other factors than those applied to a robot. Our purpose is to bring together humans and non-human entities only on the question of the assignment of an accountable digital identity.[38]

62. Outside this field, nothing is called into question; on the contrary, as explained in the Preamble (Chap. 1), it is urgent to give back to humans the control of all manifestations of their identity in the virtual world; it is urgent to establish a form of sovereignty in the virtual world.

3.3.2 Features of the digital identity

63. Whether one is a natural or legal person, or a robot, algorithm or other intelligent artifact, we can discern three features:

- The establishment by a third party of the existence of the entity in question, at its birth or at its creation,
- The recording in a register of the attributes that characterize this entity as a unique person, and, pragmatically,
- The assignment of a unique identifier in that registry.

64. It should also be noted that the register in question is always linked to a community; e.g. for state-issued identities, the community is the state, but there are many other communities that carry an identification system[39]: the acronyms of securities (and by extension the identity of their issuers) on the stock exchanges, the DUNS, SWIFT or BIC codes, the two- or three-letter IATA Airline-Codes, the enrolment number of the armed forces, and even the declared identity of the French Foreign Legion, which appears to be a very old precursor in the real world of the multiple "identities" that we assign oneself in the virtual world.

65. ⚠ It is therefore clear that my digital identity will be expressed in practice through a digital identifier. In addition, such digital identifier must be assigned to me by a third party linked to the register of the legal community that I am joining. The same goes for legal persons, robots, algorithms and other intelligent artifacts.

[34] "idem" = what I am objectively/biologically; "ipse" = who I am in my self-perception and the image I project to others.

[35] What about will? Do artificial entities have a will? It is not necessary to decide this debate here; the concept of capacity to act is sufficient for accountability.

[36] Digital assets today have as much meaning for a natural person as for a legal person, a robot person or an AI. The ability to link these assets to an identity in this same digital world and capable of applying to natural persons, legal entities, robots, algorithms and other intelligent artefacts is an obvious necessity.

[37] Blandine Mallet-Bricout et Thierry Favario, L'identité, un singulier au pluriel, Dalloz 2015.

[38] The ability of attributing liability for an act to a person.

[39] Of course, most of them only have legal effects through the "official" identities to which these systems are attached.

66. ⚠ Note that we cannot exclude the registration of the same person in several registers[40] of different communities. The law recognises the multiplicity of uses, but at the same time affirms the uniqueness of identity. We cannot elude the fact that an identity transcends an inscription into a register.

3.3.3 Identity and digital communities

67. In Law, identity is a concept that is both singular and plural. Singular because of its uniqueness, plural because of its uses: “I” can at the same time be a director of a company, an employee in another company, the treasurer of the community tennis club, the father of a family (and as such the head of the tax household), a member of the association of grower-distillers of the city of Montferrand Le Château, and the driver of a van collecting food for the charity "Restos du Cœur". Accountability will vary for each of these assignments.

68. There is thus a single “I”, which does not change, and an infinite number of “communities”[41] within which I exercise “functions” with associated responsibilities (we shall return to the question of capacity to act below).

69. In Law: civil identity is constant[42] and permanent[43] and plural[44] in its daily applications.[45]

70. In the digital world, there is no reason to see the Internet as a single community in which I would perform only one function. It must therefore be possible to create as many “digital” communities as desired, and to assign them an identity according to their legal personality. Like individuals, these “digital” communities can have an existence in the real world, e.g. as a commercial company, an institute, an association, an interest group.

71. ⚠ My digital identity must also be permanent, constant, and plural in its applications. This leads to 2 possibilities:
- My digital identity is linked to an identifier that is only linked to my person, and the function that I perform at a given moment in a particular community is only reflected by the context in which I use this identifier;
- My digital identity is made up of as many identifiers as I have functions.

72. The second possibility is much more interesting because it allows a person to be designated by the function they perform within a community[46] and to manage the lifecycle of this function with full sovereignty[47]. Moreover, it does not exclude the first.[48]

3.3.4 Digital identifiers

73. ⚠ Therefore, there is no reason why I should not have multiple digital identifiers in multiple registries.

74. ⚠ As in the real world, I must be able to “navigate” or “express myself” in the digital world without being systematically identified: I remain free to use the identifier I wish, or not to use one.

75. There is no link of Law between a certificate and its user; it becomes clear that a cryptographic certificate cannot serve as a digital identity:

- It is neither constant nor permanent:

- I can lose my “identity”/certificate, and take steps to recover it;
- It needs to be renewed (typically every 2 years);
- The life cycle of a cryptographic certificate and that of my digital identity have nothing in common and associating them appears as a nonsense;

[40] Not only people with several nationalities, but also: who among us does not have both a passport and an identity card?

[41] This term is used here to designate both companies - legal persons, institutions or organisations, professional associations, non-profit organisations (NPOs), interest groups, constituted bodies, and any form of grouping with a legal personality.

[42] It is identical, unchanging, through all moments of its existence (but it may appear and disappear).

[43] It exists continuously, uninterruptedly (but it may change during this continuous existence).

[44] Plurality of identity may refer to variations in gender, ethnicity, religion, culture, or the nature of the entity identified (human, robot, AI). Here, it refers to the exercise of an identity.

[45] Blandine Mallet-Bricout et Thierry Favario, L’identité, un singulier au pluriel, Dalloz 2015.

[46] Like legally addressing a document to the “Director of Company XYZ” without naming them and without any context.

[47] There are many other advantages as we will see later.

[48] As an employee of company W (= FW function assigned by the HRD) I can be a member of two online forums, as well as of a professional community related to this function, leading to the 3 “uses” FWa, FWb, FWc of the same “identity”. But I am also treasurer of a club (= Fclub assigned by the management committee), and subscriber to the railway company SNCF (= F0 = in my own name).

- My “identity”/certificate has an expiration date: nonsense for an identity;
- It can be revoked: absolute nonsense.

- A cryptographic certificate is an effective security tool; it is a key, just like the key to my car, my house, a safe. Identity is not a key, nor can it be reduced to a security problem.
- The issuing certificate authority - and all the intermediate operators between me and the issuing authority - have nuisance power if my certificate renewal fails when it expires. I might not be me anymore![49]
- Outside the field of electronic signature, the private key associated with my cryptographic certificate must be coupled with a “key escrow” mechanism, which implies that a “copy of my identity” is in the hands of a third party.
- Appropriating a person’s cryptographic certificate is not only appropriating their identifier, but their entire person in the digital world.[50]
- When quantum computers can break public key encryption systems, they will not only break encrypted communications, but all identities.

3.3.5 Digital identity and cryptographic certificates

76. ⚠ It is therefore imperative and urgent to dissociate digital identity from cryptographic certificates.

77. Of course, cryptographic certificates must be used, and even abundantly, to secure all the applications of my digital identity. But my digital identity must be able to go through all the diversity, renewal, and multiplication of security mechanisms needed today in the digital world without binding me to these mechanisms.

78. If my identity is tied to a cryptographic certificate, I have only one mechanism to protect myself, and I cannot multiply it without multiplying my identity.

79. The same is true for the digital identity of legal persons, robots, intelligent entities.

80. At this point, we leave two important questions unanswered:

- How am I going to detach this identity from a certificate or other cryptographic object without exposing it to abuse? In other words: how can I retain exclusive control over my digital identity if it is reduced to an identifier?

- How do I reconcile the uniqueness of identity with its plurality, or more specifically, with the multiplicity of qualified uses in relation to the functions performed within different communities?

- This question raises a double challenge:

(a) the segregation between these multiple uses: when accessing documents, how can I enforce a clear separation between my business documents (or even, in this group between different potentially competing customers for whom I work), and the documents regarding my private life;

(b) the independent and intertwined life cycle of each of the functions legally linked to the same identity: I am appointed as a board member, I am elected president of a club for two years, I am an employee, I resign as a board director, I work for a customer, I complete my mission, I become a director, I am fired, my term of office expires, and so on and so forth. It can already be seen that those who will legally have the authority to appoint and revoke me in each of these capacities cannot be confused with a single PKI operator.

●

[49] Of course, it can be argued that the certificate is issued to me by a company in which I have a function and that it is logical to withdraw this function when I am fired. But this then means that I would have as many certificates as there are pluralities to my identity! Which of these certificates would be my true identity in its uniqueness?

[50] One will not only be able to impersonate this person, but also to access all their historical data: their digital existence.

4.MODEL AND DEFINITIONS

Whenever necessary, we will use a capital letter to distinguish a term defined by our model from its other uses. For example, “Identification” with a capital letter refers to the word as we define it here, and identification without a capital letter refers to the multiple uses that this term has elsewhere (see Section 4.4).

81. A taxonomy is essential, and we already have the material to draft a model.

82. There are many legal, functional, and technical constraints. Rather than attempting an exhaustive inventory, itself preceded by an abundant catalogue of definitions, it seems to us much more effective to propose a reference model:

- To visualize each definition;
- To identify and understand each constraint;
- To convert the principles of Law into functional requirements;
- To provide information technology specialists with a conceptual model that complies with the Law, which they can in turn map to logical and physical implementation models; or
- To methodically evaluate how an existing system would or not be compliant with the Law.

4.1 The draft

83. The initial plan contains five elements that are self-evident:

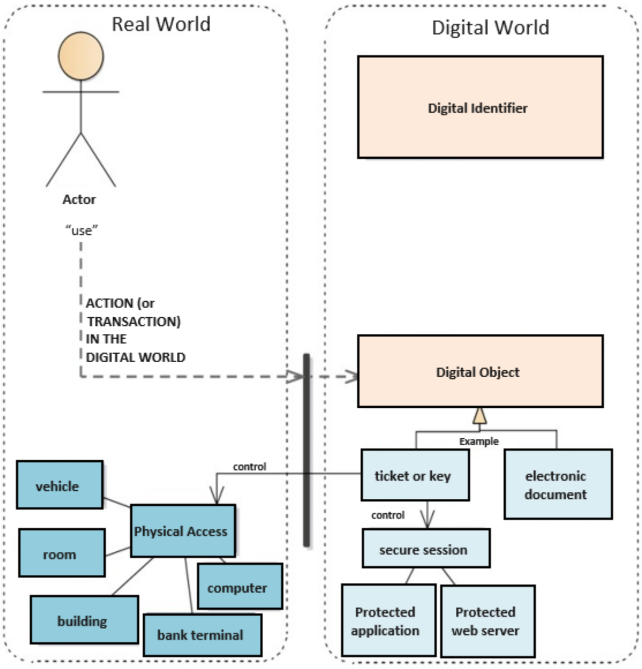
- The real world;
- The digital world;
- The entity of the real world[51], which has legal personality (a person);
- The digital identifier of such entity (as discussed above);
- The Object in the digital world on which the entity wishes to carry out its action.

84. The entity in the real world, the one that acts on the digital object, is by definition the Actor, such as represented in the figure opposite.

85. In the digital world, the Object of its action is very general, such as marking one's identity on a transaction or a document, exercising access to an application or data, executing an operation (calculation, addition or modification of data).

The Object is therefore represented in the digital world although the action triggered may have effects in the real world. Note that the examples of digital objects shown in the figure below under the Digital Object and their artifacts in the real world are by no means exhaustive.

86. The thick vertical bar through which the Actor’s action on the Digital Object is carried on, and through which passes the possible feedback or effects from the Digital Object on the real world, represents the Human-Computer Interface and/or the application interface (e.g. keyboard, mouse, screen, sensors, electric motors, buttons, switches, antenna).

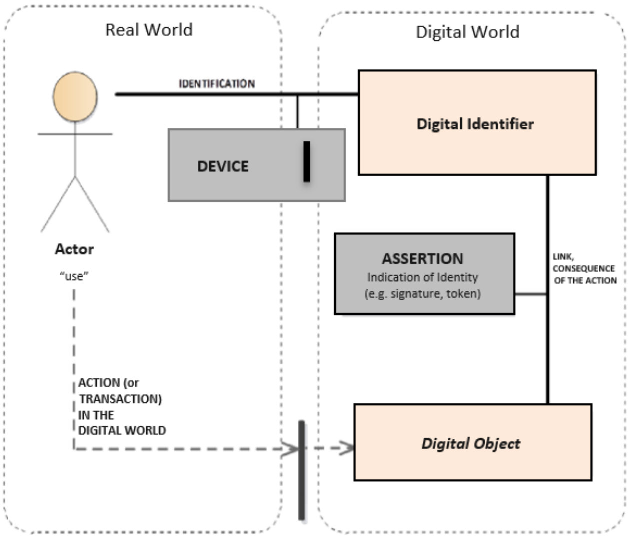


[51] The case of entities existing only in the digital world will be resolved later.

87. The Identification then designates the association between the Actor and their digital Identifier, as represented by the horizontal line in the figure below.

88. This association crosses the barrier between the real world and the digital world. It is by nature ephemeral and must therefore be accompanied by a Device at this interface. This Device shall be capable of renewing and re-validating the link between the Actor in the real world and their Identifier in the digital world, on every use of the avatar of our Actor in the digital world (i.e. its Identifier).

89. In other words, it is, by definition, the Device - usually composed of several elements - that makes our Actor the master of its digital Identifier. And since the Actor and the Identifier are in different worlds, there has to be an Interface.



90. Here are 4 examples (without giving our opinion at this stage on their respective qualities with regard to the Law).

91. Example 1:

- Actor: me;
- Device: smart card and biometric reader;
- Identifier: digital data sealed in the smart card;
- Digital Object: a document that I want to sign.

92. Example 2:

- Actor: me;
- Device: the keyboard of my computer and the access management software component (login ID + password) of an email server;
- Identifier: my email address;
- Digital Object: the application that checks my incoming emails.

93. Example 3:

- Actor: me
- Device: a payment terminal and my credit card;
- Identifier: my account number;
- Digital Object: a payment order.

94. Example 4:

- Actor: me;
- Device: my computer keyboard, my cell phone equipped with a one-time code generation application, a 2-factor authentication web application, and a remote identification server with its user database;
- Identifier: a user number;
- Digital Object: a SAML assertion[52] that will give me access to a document sharing workspace in a document management application.

[52] SAML (Security Assertion Markup Language) is a standard published by the industry consortium OASIS which defines the content of encrypted messages allowing an Identity Provider (IdP) to transmit authorisation information to Service Providers (SP). In concrete terms, when a user U tries to access an application A, application A contacts an application X specialised in user identification (or only user authentication). If application X sees that your previous identification is no longer active, it will ask you to give your password, or a code generated by your mobile phone, or data sealed in a USB key or smart card, or your facial image or fingerprint (in short, whatever process it has decided to implement to identify/authenticate you) and, upon verification, it will build a SAML message with your identifier, an indication of positive verification, and sometimes a list of your access rights, all cryptographically sealed between X and A. The identifying application X passes this message to application A, which validates the cryptographic properties, decodes the content, and opens the access requested from A by user U. In case user U's previous identification with X was still active, application X will cut red tape by exempting the user from the whole procedure and directly generates the ad hoc SAML message. The user has the comfort of accessing application A directly without being (re)identified. If the user then tries to access another application B, the user can also be exempted from the above-mentioned procedure: this is the Single Sign On (SSO) system.

95. Of course, there are an infinite number of variants, standards, mechanisms, digital objects and associated technologies. But we can always determine the Actor, the Device, the Identifier, and the digital Object targeted by the action or transaction in question.

96. We can immediately understand all the issues and the difficulty of this Actor-Identifier link so that it is unique, irrevocable, and ensures exclusive control of the exercise of its Identifier by the Actor. This link must cross the boundary between the physical world and the digital world, in other words between the material world and the virtual world.

97. The applicable legal constraints are detailed in chapter 5, section 5.1 related to the rules of evidence.

98. In the model shown in §89, there is a vertical association: the link between the Identifier and the digital Object. This link expresses, in the digital world, the indirect[53] relation between the Actor and the Object of its action.

99. This association only exists in the digital world and is expressed by an Assertion, i.e. a digital affirmation[54] of the relation between the Identifier and the Object. In the digital world, the assertion is the equivalent of a writing.

100. The vertical association embodies the Actor's will with respect to the digital Object at a given moment, such as an access token to a secure application, the mark of the Actor's consent on a document (electronic signature) or the issuing of a payment order (Object) from the Actor's account (Identifier).

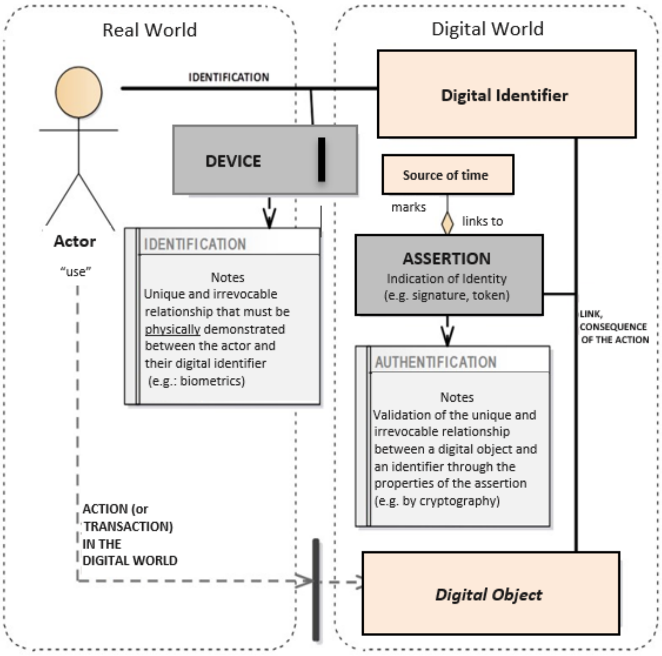
101. Here are some practical examples of Assertions:

- An ephemeral memory state (cookie) such as the session context[55] between your browser and the web application you logged in with.
- A PAdES[56] compliant electronic signature on a PDF document as prescribed by the eIDAS implementing regulation.
- The validation information attached to the electronic payment order issued by the merchant terminal to the payment operator.
- The validation information of your identifier inside a SAML message (a digital object already mentioned that serves as an access token to a computer application).

102. Like Identification, which revalidates the Actor-Identifier link at each operation (action or transaction) performed by the Actor, Authentication is the operation that consists in validating an Assertion.[57]

103. By an ellipsis that assimilates the identifier to the actor, authentication is often confused with identification.[58] While our Authentication validates the link between an Object and an Identifier, it is clear with this model that it does not know the Actor behind the Identifier.

104. We can therefore Identify without Authenticating, and (unfortunately in most current systems) Authenticate without Identifying.


Real World
Digital World
IDENTIFICATION
Digital Identifier
DEVICE
Source of time
marks
links to
Actor
"use"
IDENTIFICATION
Notes
Unique and irrevocable relationship that must be physically demonstrated between the actor and their digital identifier (e.g.: biometrics)
ASSERTION
Indication of Identity (e.g. signature, token)
LINK, CONSEQUENCE OF THE ACTION
AUTHENTIFICATION
Notes
Validation of the unique and irrevocable relationship between a digital object and an identifier through the properties of the assertion (e.g. by cryptography)
ACTION (or TRANSACTION) IN THE DIGITAL WORLD
Digital Object

[53] Direct between the Identifier and the Object, indirect (via the Identifier) between the Actor and the Object.

[54] We are talking here about data structures or even a structured electronic message designating or containing the digital object, the identifier, and generally a date, all of which is sealed, most often using cryptography, so as to be able to subsequently validate the association thus "written" in these data.

[55] Cookies are often referred to in the case of web servers. These are small packets of data, sometimes encrypted, exchanged at each request between your web browser and the online application. These cookies are either "anonymous" (in theory!) with the sole purpose of tracing your repeated accesses to the site on the basis of an identifier generated by the server, or they contain in addition data that convey the identifier that has been assigned to you (login ID) and the indicator of your successful login (e.g. with login ID and password).

[56] PAdES: PDF Advanced Electronic Signature, a set of standards published by ETSI (European Telecommunications Standards Institute), see "EU eSignature" documentation: https ://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Standards+and+specifications.

[57] Warning: this is the taxonomy used in this document. It is far from being universally accepted. For variants of meaning, see section 4.4.

[58] See section 4.4.

105. While one can easily understand the fragility of the Actor-Identifier link, which must cross the physical-digital barrier, it is quite different with the Identifier-Object link, which is entirely located in the digital world: cryptographic techniques have long made it possible to build robust and irrevocable Assertions.

106. But does this protect the right side of the model from any difficulty?

107. No, unfortunately not: first of all, it is necessary to guarantee the autonomy and durability of assertions[59] in order, for example, to benefit legally and over time from the enforceability against third parties. Except where special measures are taken (e.g. blockchain), it remains possible in the digital world to erase all traces of an assertion if this serves the interests of its author and their accomplices... or to claim that there is a forgery when the mechanisms of calculation of the Assertions are easy to reverse.

108. Moreover, the mark of time counts in the validity of an assertion, and the sources of time used to create an assertion are too often falsifiable, or under the direct control of the author (e.g. the clock of the author's personal computer).

4.2 Nested models

109. The legal value of an act is linked to the system of proof.[60] The model clearly shows the nature and fragility of each of the two links necessary for an act to be legally enforceable against third parties, i.e., one that can be proven independently of the assertions of the person concerned, in accordance with the legal principle: "No one can set up their own title by themselves"[61]

110. This demonstration can quickly become complex, because our model can be nested on several levels like Russian dolls through a hierarchy of Devices. And this is very often the case in practice.

111. Let's take the example of the increasingly common two-factor authentication (2FA).

112. With an ad hoc application, your smartphone becomes an identification device whose link to the Actor is only guaranteed by the personal nature of the phone. Incidentally, protecting your phone with a PIN code (or a pattern lock or the integrated fingerprint sensor) is no longer an option, even if the robustness of these mechanisms is quite relative (technical hacking or phishing).

113. We thus have a first Device — with its qualities and its defects — used to activate the phone (digital Object) by the Actor who holds it in their hand, and the Assertion: "I am the owner".

114. The Actor can then launch the "2FA app" (2nd Device) on their phone which will ask them to re-identify themself (e.g. another PIN code, facial recognition) before issuing a single-use code (Assertion: "it's me, it's my phone and it's now") allowing our Actor to confirm (factor 2 of the "2FA") an identification process already initiated "online" with a Web application typically with login ID and password (factor 1 of the "2FA") via a 3rd device, made up of the Actor's Internet browser and the identification subsystem used by the remote application that will authenticate the single-use code.

115. The 3rd Device integrates the 2nd Device, which itself depends on the 1st Device.

116. It is clearly very complex technically speaking, and even more so legally speaking. In case of fraud or simple failure, what are the responsibilities of the phone manufacturer? of the 2FA application vendor? of the provider of the identification subsystem used by the remote application? of the communication network operators? of the service provider of the application you have (or have not!) accessed? and of the operators hosting all the intermediate hardware and software components involved?

117. The quick answer is that all of these stakeholders are now absolving themselves of any responsibility by hiding behind a best effort obligation and that the eIDAS regulation, despite the hopes raised, has done nothing more than promote the interoperability of "means" (the Devices) and select existing standards (which are also "means") for the mutual recognition of Assertions.

118. ⚠ It is already clear that, in order to produce evidence, we will have to return to much simpler, compact, and above all autonomous devices... with no compromising on security.[62]

[59] Chapter 5.

[60] Chapter 5, section 5.1.

[61] Civil Code, Art. 1363.

[62] See Chapter 6, sections 6.1 and 6.2 on Compact and Biometric Devices.

4.3 Composition of an identifier

119. Important question: can the Identifier be anything?

120. The Law provides the answer.

121. We have already spoken of the multiplicity of forms: identity is unique in law, but multiple in usage. In the business world, the Actor rarely acts on their own behalf. Whether they are an employee, director, administrator, representative, agent or member of a regulated profession (e.g. doctor, notary, lawyer, auditor), this Actor acts on behalf of a third entity, most often a legal person (company, state, organisation), or a business community:

⚠ We call a **Community** any grouping of individuals (the members of this community) that generally has legal personality, but that is in all cases attached to a system of Law, or in other words a jurisdiction. The concept of Community thus designates not only any form of industrial enterprise, institute, administration, association, or interest grouping, but also sovereign entities such as states or their subdivisions (e.g. regions).

⚠ We call **Function** the role - with rights and obligations - exercised by a member of this Community within such Community and/or on its behalf, as assigned to them by a third party (and not by themself) duly mandated by this Community.

122. The capacity to exercise a Function on behalf of a third party becomes even more meaningful when the entity (the Actor) is not a natural person, but a legal person: like a natural person, a legal person has legal personality; it can be sued. One cannot therefore prohibit a legal person from existing (and thus from being properly identifiable and accountable) in the digital world, but one cannot either let its identifier(s) "float" without control by the absence of any physical identification device.

123. The Law clearly states that a legal person is liable for all representatives and officers (e.g. employee, director) acting on behalf of such legal person (through a function, a mandate, or statutes). It is therefore through the Device of one of its representatives or officers that a legal person will be able to identify itself and act legally.

124. And for robots? They clearly have a capacity to act on the real world; but what about their legal personality?[63]

125. If a robot identifies itself as acting on behalf of a third party, whether a natural or a legal person, it then inherits the latter's legal personality and becomes an entity legally accountable for its acts in both the real world and the digital world.

126. In this digital world, an artificial intelligence algorithm becomes accountable if it is given an identity as the agent of a natural or legal person, such as an autonomous AI that delivers an automated diagnosis for several hospitals and that will be insured in the same manner as for a doctor.

127. An autonomous vehicle properly identified and mandated by a transportation operator will make the operator liable for the accidents of such vehicle.

128. The Law will allow to properly organise and supervise the investigations on the condition that the participating entities (natural person, legal person, robot) are irrevocably[64] identified, that their actions are traced (keeping of assertions / logs[65]), and that these identities are qualified (as explained below) (167 to 173).

129. Figure §131 generalizes all types of identifiable entities on the basis of combinations of legal personality and capacity to act. Clearly, the non-autonomous objects in the left-hand column need no identification. They fall into the category of movable property. This will also be the case for the vast majority of robots whose action is deterministic and invariant to experience.

130. The model is flexible: if one fears a move towards "techno-personalisation"[66], a community that uses AI robots can decide to keep them all in the category of movable property, or on the contrary to give them legal personality and an ad hoc numerical identifier, or to create a separate category in the system of Law that this sovereign Community uses and/or inherits.

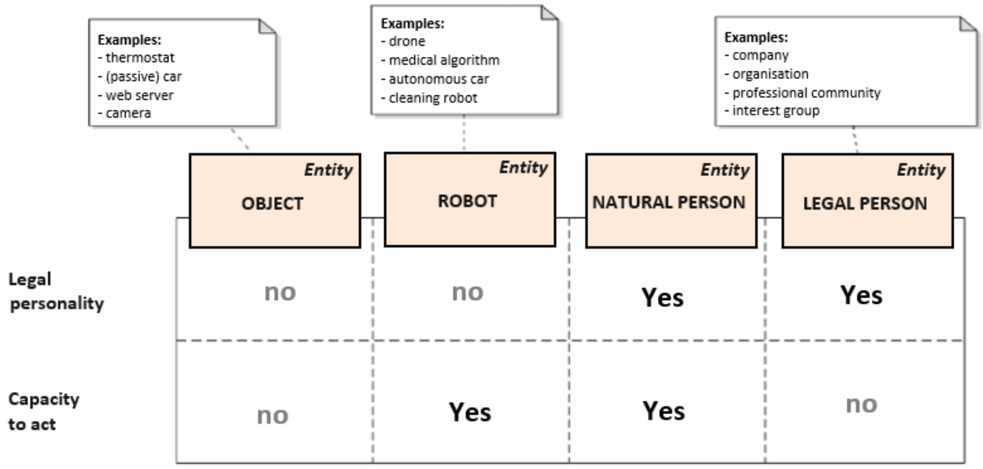
[63] For an in-depth discussion of the issue: « IA, robots et droits » (Bensoussan & Bensoussan, 2019).

[64] We must not resort to a useless and meaningless multiplication of digital identifications, like assigning one to an aircraft engine or a car wheel. Any failure of these objects to have an identity: the nature of movable property is perfectly regulated by law; it applies to animals and currently to robots, for the vast majority of which this poses no problem; only robots equipped with an AI capable of autonomous decision-making based on their own "experience" as robots raise the question of a legal personality both to protect them and to make them accountable.

[65] See Chapter 5, section 5.4.

[66] See above 61.

131. The case of natural and legal persons is obvious: their intrinsic legal personality calls for the creation of digital identifiers capable of carrying it.

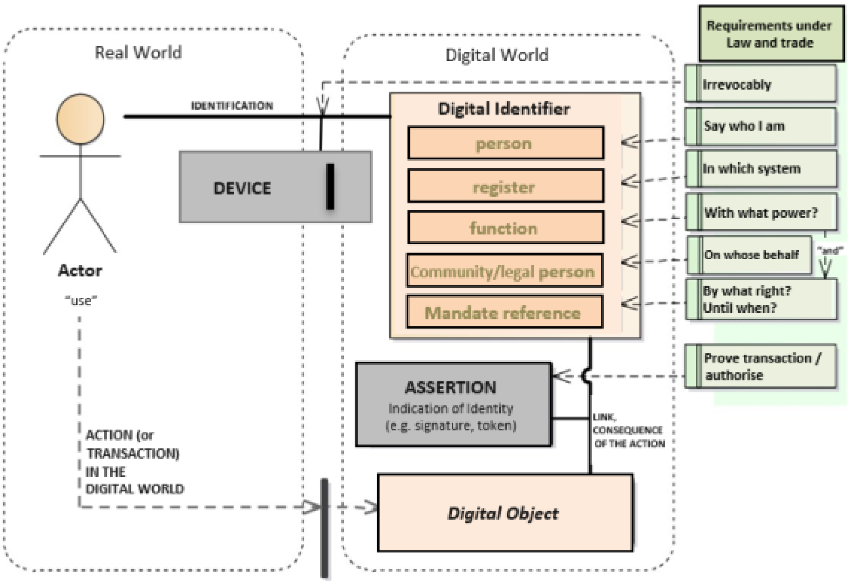


	Entity OBJECT	Entity ROBOT	Entity NATURAL PERSON	Entity LEGAL PERSON
Legal personality	no	no	Yes	Yes
Capacity to act	no	Yes	Yes	no

132. As "No one can set up their own title by themselves"[67], any Function emanates from a Mandate which thus assigns a Function to a Person in a Community whose reference must be part of the digital identifier:

- A Mandate has its own life cycle: it often has a deadline, it can be renewed or repealed in advance.
- Whereas the Function is essentially a title, its content (prerogatives, limits, rights, obligations) is determined by the Mandate. The Function can remain identical in its assignment, but change in its content with the renewal of the Mandates.
- While the 4 other elements of our digital identifier (person, register, function, community) are essentially declarative, it is the Mandate that gives the whole a legal value.
- We could actually be satisfied with the only reference to a Mandate as a complete digital identifier, but operational requirements and the requirement to avoid any central file of personal data, invite us to attach the first 4 elements to our digital identifier.

133. ⚠ This 5-elements digital identifier is represented in the figure below. It supports by construction an identification of the Person as such.



[67] See above 109.

134. The requirements that cover both the composition of a digital identifier and its relation to the Actor (horizontal association) and the Object (vertical association) of its action are illustrated on the right of figure § 133.

135. What happens then when I act on my own behalf? Is there no mandate? Yes, there is: the civil registrar who enrolled my civil identity as a citizen of a country, with rights and obligations. Of course, we are talking here about a digital identity: there will therefore be a Community (a digital one, which could be "Digital France" as much as, for example, a syndicate of Bailiffs) within which my first digital identity will be assigned.

136. Let us suppose that I am the employee of a bailiff, who is also a civil registrar. They can thus enrol my Function of employee in their service at the same time as my Function "in my own name" attached to my civil identity.

137. In contrast, if my first digital identity is assigned to me by the human resources manager of an industrial company, I could decide to add my Function "in my own name" later by going to an enroller duly authorized to confirm my civil identity. Or, why shouldn't the HR manager be able to verify my civil identity, as this is also in their interest? Every digital identity in this model has a mandatory reference to a mandate, and the "in my own name" function is no exception.

138. A mandate is a document, a Digital Object, with at least the signature of the enroller (irrevocable assertion of the enroller's commitment to the enrolment process) and the signature of the enrolled person (irrevocable assertion of the enrolled person's consent to the assigned Function), thus tying up all the legal requirements of an ex officio identity and allowing any identification fraud to be prosecuted.

139. In line with our call[68] to separate digital identities from the security mechanisms intended to protect them (e.g. a cryptographic certificate), the security of a digital identity must be attached to the life cycle of the Mandate, which is revocable and renewable without calling into question the Function of the person. This is obvious!

140. We can then go even further by having certified digital identities – with a Mandate – coexisting with non-certified (and without legal recourse) digital identities – without a Mandate, even if it means having them certified later. Of course, these digital identities would also be protected with an adequate level of security, but unlike the identities formally assigned by a Mandate, the user takes full responsibility[69] for the security of their self-assigned identities. These identities are by construction devoid of any legal recourse, as they cannot prove the real identity of the Actors.

141. The field of possibilities becomes colossal, and it will be up to the Communities to determine their applications and their limits.

142. All the legal requirements that follow[70] will reinforce this model.

143. Admittedly, one could argue that it is enough to enclose this digital identification proposal in a cryptographic certificate and return to the practice of PKIs. Big mistake! The multiplicity of functions for the same person, multiplied by the life cycle of the Functions, multiplied by that of the Mandates, will telescope with the life cycle of the cryptographic certificates, resulting in an unmanageable magma for PKI operators.

144. The solution developed below is much simpler, more robust, and more transparent.

4.4 Identify vs. authenticate

145. These are two terms whose semantics vary greatly.

146. If we start from a "stricto sensu" [71] definition of authentication — an operation that validates the correspondence between an observation and a proposition related to this observation — then, identification would be the proposition ("this person is linked to this digital object" [72]) that is the object of this validation. In our model, the proposition is reduced to "this identifier is linked to this digital object" and the path from the identifier in the digital world to the individual in the real world (the Identification in our model) remains out of reach.

[68] See above 76.

[69] However, constrained by the procedures, mechanisms, and security policies that the Community accepting these self-assignments would choose to put in place as part of its sovereignty.

[70] See Chapter 5 on the Legal Framework.

[71] Different from the ones found in the dictionaries. The *Littré* does not know this recent word. The *Larousse* is direct: "Process by which a computer system ensures the identity of a user". *Le Robert* piles up the definitions: "action of authenticating" -> "[...] to recognise as authentic" -> "Which is truly from the author to whom it is assigned / Whose authority, reality, truth cannot be disputed / [...]". The *Dalloz* lexicon sticks to the certification of "authentic instruments".

[72] This can be easily proven by cryptography.

147. For the authors of the National Assembly report[73], the identification takes place only when one goes back to the civil identity and thus to the registers of the state. It is established by the act of enrolment and confers a persistent quality on the identifier thus enrolled; this identifier is precisely what the authors call the "pivotal identity", namely the basis of one's civil identity: last name, first names, date and place of birth, sex.

148. The person's control over this identifier is made, for example, through facial recognition (ALICEM), and where the latter is a purely local operation (the cell phone compares the person's image with a locally recorded mask), one continues to speak of authentication but not identification. Authentication is then the dynamic part: providing proof (sic) of one's digital identity during an act in the digital world thanks to various means whose security level can vary... which - we note in passing - is in contradiction with the strict concept of proof: proof is established or not, without any gradation.

149. For other authors, any distinction between identification and authentication makes no sense: it perpetuates the confusion, knowing that one cannot go without the other unless doubt is introduced. These are two inseparable sides of a single operation, which consists in proving who is the person behind a digital act.

150. In this sense, authentication is the implementation of identification. Identification is the purpose of authentication operations; the words are therefore interchangeable depending on whether one wants to emphasize the means (authentication) or the objective (identification).

151. As far as this White Paper is concerned, for the purposes of building a digital identity 5.0, we need to clearly distinguish 2 concepts:

1. The ability of a person to keep exclusive control of their digital identifier, and thus to irrevocably indicate that any trace[74] of their identifier on any digital act emanates from their will[75], or from their explicit consent before or at the time of the act[76], and therefore that it cannot result from either accidental or abusive use.

It is a dynamic operation that consists in proving the link between the person and their digital identifier each time such identifier is used (or before a series of uses[77]) on a digital medium.

2. The ability to prove the link between a digital identifier and a digital object (e.g. electronic document, activity log, transaction, authorisation, certification, intellectual, industrial or commercial property on intangible or digital assets). This proof must obviously be persistent. Its creation and subsequent verification[78] are carried out in the digital world with means that, by construction, must exclude any falsification or misappropriation. Today, this implies almost systematically the use of applied cryptography.[79]

152. Unless we invent new terms, we speak of identification in the first case and of authentication in the second case. This usage is simple (person <Identification> digital identifier <Authentication> digital object/medium) and appropriate to our context (see the proposed model). Most importantly, it is relevant, as will be demonstrated later.

153. Simply put: to Authenticate is to validate who you claim to be; to Identify is to validate who you are.

154. The definitions given in § 151 are not incompatible with those given in § 149 and § 150. Firstly, if a person's control over their identifier is not certain, one cannot speak of Identification within the meaning of § 151 1. Secondly, there can be no proof unless the conditions listed in § 151 have been met: to identify implies being able to (re)Authenticate subsequently; to Authenticate implies having Identified, unless one introduces doubt, and therefore invalidates the authentication within the meaning of § 146 or § 148.

155. It is clear that in order to demonstrate the link between a person and a digital object/medium, one cannot dissociate identification and authentication. This is why in common parlance an authentication operation is often equated with an identification.

[73] Mission d'information de l'Assemblée sur l'identité numérique, Rapport Ass. Nat. N° 3190, 8 July 2020.

[74] In our model, we use the more precise term "assertion", see section 4.1.

[75] In the case of multiple traces such as the history of websites visited by the person, or the history of their GPS, the trace must be understood as referring to the group of elementary traces of the same nature, and the will of the person in relation to this group.

[76] Case of the electronic signature.

[77] See note 75.

[78] As many times as necessary for the exercise of the rights and obligations arising from this link.

[79] We do not wish to exclude digital microfiche, optical disks to a certain extent, or future technologies such as 3-dimensional micro-engraving in quartz blocks. Blockchains are also applied cryptography.

156. Identifying without Authenticating makes little sense[80], but Authenticating without Identifying is unfortunately the current prerogative of the Internet. Digital identity as used today is more often the result of self-declaration, accompanied by an extrinsic means of demonstration such as a "username" coupled with a password, and sometimes by a range of security measures such as two-factor authentication (2FA).

157. While it may be possible to reduce the risk of misuse of an online account, and thus improve the quality of authentication, it has still not been demonstrated who the person behind the self-assigned ID really is. To be admissible and enforceable against third parties, the user must be able to prove their identity by intrinsic means under their sole control; as it will be explained below, an identity worthy of the name[81] must be irrevocable, which implies the proof of Identification *and* Authentication.

158. Irrevocability implies keeping traces safe from any editing or erasing, both alterations that are technologically far easier in the digital world than in the physical one.[82] This question will be developed in Chapter 5, section 5.4 on the archiving of evidence.

[80] For example, recognising a painting as being by Picasso without being sure that it is really by him.

[81] There is no need to add the qualifier "digital" here, it is universal.

[82] If blockchain technologies are of any interest here, it is to definitively and unalterably log all traces of transactions without recourse to an omnipotent trusted third party.

5.LEGAL FRAMEWORK

Guaranteeing the confidentiality and legal value of digital exchanges by irrevocably identifying the authors of the content, the senders, the addressees and all authorised third parties at each stage is a major challenge.

159. No industry can evade the law.

5.1 Rules of evidence

5.1.1 Law of obligations

160. Civil Code:

- Article 1353: "A person who claims performance of an obligation must prove it. Conversely, a person who claims to have been discharged must establish satisfaction or circumstances which have resulted in the extinction of the obligation".
- Article 1357: "The judicial administration of the proof of any matter, and disputes relating to it, are governed by the Code of Civil Procedure".

161. Code of Civil Procedure:

- Article 9: "Each party must prove, according to the law, the facts necessary for the success of their claim".
- Article 146: "A preparatory inquiry on a fact may be ordered only if the party who pleads it does not have sufficient material to prove it. In no case, a preparatory inquiry may be ordered for the sake of making up a party's deficiency to produce evidence."

162. ⚠ A problem arises with digital identity that did not exist with paper: I am concerned with the quality of the "arm and pen" of the other party. It is not enough that I am super equipped with a super Digital Identity and a super irrevocable Identification Device; if the other party uses only a weak Identification means, or if simply no third party (no Mandate) comes to confirm that the digital Identifier used is really that of the other party, I will not be able to prove anything.

163. ⚠ The Mandate attached to my digital identity is not an option. Example: I signed a document for my employer with a "personal" digital identity because it was the only one I have, but my employer thereafter withdrew and backdated my letter of dismissal to the previous day... In this scenario, the digital Mandate would have unambiguously established that I was acting for my employer and if there had been a revocation, the date of the revocation would have been certified by a third-party time stamp provider.

5.1.2 Perfect proof

164. Written evidence is one of the means of proof that are known as "perfect"[83] proof, i.e. proof that is binding on the judge, provided that it complies with the texts governing it; such texts include:

165. Civil Code:

- Article 1363: "No one can set up their own title by themselves."

166. ⚠ Who will risk using a digital identity only protected by a password or PIN code in important transactions? Either it is admitted as irrebuttable presumption of evidence (I was robbed of this code and I can't back out: too bad for me), or it is not evidence (that's the case! too bad for me). Not to mention all the disputes in between where I should try to convince that it was me, or not me.

167. No digital identity without a Mandate (third party ⚠nature) to confirm its assignment. Example: I self-enrol with a super Device. I could certainly demonstrate to the judge that this Device is under my control for the digital Identity in question, but who proves that I alone have such control?

168. Civil Code:

- Article 1364: "Proof of a juridical act may be constituted in advance by its being created in a publicly authenticated written form or by signature."
- Article 1365: "Writing consists of a series of letters, characters, numbers or any other signs or symbols with an intelligible meaning, whatever their medium."

[83] Which excludes by definition any presumption.

169.⚠ It is therefore necessary to stick to technologies (notably cryptographic technologies) capable of creating unfalsifiable Assertions and that these cannot (voluntarily or involuntarily) disappear over time. For archiving, see section 5.4.

170. Civil Code:

- Article 1366: “Electronic writing has the same probative force as writing on paper, provided that it is possible to properly identify the person from whom it originates and that it is created and stored in such conditions as will guarantee its integrity.”

171. ⚠ The irrevocability of the Actor-Identifier link must be ensured by all useful means[84]. The Devices must therefore prohibit any possibility of use by a third party of an Actor’s identifiers, even with the Author’s complicity (e.g. disclosing one’s PIN code). Any centralization of the identifiers and, worse, of the means of exercising them can lead to their misuse (potentially without leaving any trace) in the event of a breach of computer security. Any central electronic signature server should therefore be banned.

172. ⚠ The Article reaffirms the imperative need to ensure the sustainability of the media (assertions and associated digital objects, see section 5.4), and of the mechanisms for verifying the authenticity of these media; in order to prove 30 years later that it was indeed Mr M who had expressed his consent to such a transaction, the content of this transaction must also remain intelligible.

173. Civil Code:

- Article 1367: “A signature which is required in order to perfect a juridical act identifies its own author. It demonstrates his consent to the obligations which stem from that act. Where it is placed on the act by a public official, it confers authenticity on it. Where it is in electronic form, it must use a reliable process of identification which guarantees its relationship with the act to which it is attached. The reliability of the process is presumed in the absence of proof to the contrary where an electronic signature is created, the identity of the signatory is ensured and the integrity of the act is guaranteed on the conditions fixed by decree[85] of the *Conseil d’État*.”

174. This Article requires an explicit indication of consent. It cannot be a click or a keystroke; it must be an action that avoids any likelihood of confusion, unexpected ⚠ capture, or variable interpretation. In other words, the chosen Device must require an explicit and unambiguous gesture from the Actor, excluding any automatic or implicit repetition and any other actor. This clearly excludes confirmation clicks and text messages via SMS.

175. Moreover, there can be no consent without an equivalent facility to oppose. This was ruled by the ECJ[86] and is now clearly stated in a document[87] specifying the terms of the GDPR[88]. “Silence (…) or inactivity should not therefore constitute consent.”

5.2 Protection of privacy

176. “The mass of data collected from Internet users (Big Data) constitutes, as we know, “the oil of the 21st century” insofar as marshalling such data makes possible to predict - and even direct - the behaviour of consumers and customers.[89].

5.2.1 Personal data

177. Under the GDPR, personal data means “any information relating to an identified or identifiable natural person (...); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”[90]. This definition is also the one adopted by the French data protection authority, the CNIL.[91]

178. The amended French Data Protection Act reproduces the definitions set out in the GDPR and thus endorses the above definition of personal data.[92]

[84] See Chapter 6, section 6.2 on biometrics.

[85] Decree No. 2017-1416 of 28 September 2017 on electronic signature, referring to the eIDAS Regulation (EU 910/2014), itself followed by an implementing regulation (EU 2015/1502). Note that Decree No. 2010-112 of 2 February 2010, which imposes the RGS (General Security Referential – *référentiel général de sécurité*, published by the ANSSI), continues to apply to exchanges with the administration. The differences are minimal.

[86] Court of Justice of the European Union, 11 November 2020, C-61/19.

[87] Guidelines 05/2020 on consent under Regulation 2016/679 (= GDPR).

[88] Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[89] Pauline Türk et Christian Vallar, "La souveraineté numérique : Le concept, les enjeux", Ed. Mare & Martin 2018.

[90] Reg. 2016/679 of 27 04 2016, art. 4.

[91] www.cnil.fr/fr/definition/donnee-personnelle

[92] Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties *(Loi 78/17 du 06 01 1978 relative à l’informatique, aux fichiers et aux libertés)*, art. 2.

179. The collection and use of personal data must comply with the principles set out in the GDPR and soon with those laid down in the proposal for a regulation concerning the processing of personal data in the electronic communications sector, known as "ePrivacy Regulation"[93], which is intended to supplement the provisions of the GDPR and is currently being discussed at European level.

180. The identification of a natural person must be carried out with the strictest respect for the protection of the security and confidentiality of the personal data used for this purpose, with due regard for the privacy of individuals and their fundamental rights.

181. In the digital world, you leave many traces of your actions, or even of your mere passage. While your identity must be unambiguous for a small number of operators (service providers) or correspondents to guarantee the legal effects of your actions, it is desirable that you remain anonymous for all the other parties indirectly involved (e.g. infrastructure managers, telecommunication operators, intermediary software vendors, relay servers, traffic sensors, analysers of "clicks", advertising providers). The protection of your privacy will be enhanced by the use of digital identifiers that are as anonymous as possible and under the strict control of the designated person.

182. ⚠ In other words, we advocate the use of identifiers devoid of any meaning; this implies excluding the use of a surname such as "Dupont" or even a function such as "Director", and even more so all current uses of email addresses. A binary numerical field allocated pseudorandomly[94], combined with the person's ability to use several identifiers (multiplicity of uses[95]), is the best identifier. You can fully control the public information that you wish to attach to each identifier through a directory, or — depending on the needs — by including it in the envelopes (in clear) or the content (encrypted) of your exchanges.

183. ⚠ One could even advocate the replacement of implicit identification means (IP address, cookies correlated by multiple sites, profiling), by an explicit but anonymous identification under your control. We cannot deny the economic interest of marketing analyses, or even a positive contribution to the optimisation of resources, nor the potential interest for users of personalised services, but not without the knowledge of the person concerned.

184. Digital Identifiers can then be seen more as addresses, in the same way as a telephone number. However, the structure shown in Figure § 133 with the element designating the Mandate is required here; with the associated Function, it is a much more relevant identification tool than a telephone number, even if the latter, reduced to numbers, remain anonymous.

5.2.2 Identity theft

185. The digital identity provider must protect everyone against identity theft. The "LOPPSI 2" [96] Act created the offence of online identity theft, which is now inserted in Article 226-4-1 of the French Penal Code.

186. The Internet is special in that even if identity theft can be prosecuted under criminal law, the possible damage in terms of image or reputation may be irreversible. Fact is, the right to be forgotten is impracticable. Only the right to de-referencing is possible.

187. The digital Identity proposed in this White Pape⚠has several advantages.

- Digital Identity becomes much more robust by construction when self-assignment disappears "for everything that matters", when the problem of Identification is correctly dealt with in relation to the issues at stake, and when third parties – who are mandated by communities (legal entities) and identifiable (accountable) – are referenced in the identities that they assign.
- It establishes a system of multiple identities that are, by their very nature, compartmentalised to the communities within which they have been assigned.
- Any misuse can - by construction - only target a particular Mandate, which can then be revoked and renewed.[98]

[93] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy), Compromise text of 18 September 2019.

[94] Pseudorandomly as it must remain unique.

[95] See 66 to 71.

[96] Framework Law on Internal Security Enforcement *(Loi 2011-267 du 14 mars 2011 d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure)*, JORF of 15 March 2011.87.

[97] See 133, figure § 133.

[98] See§ 139.

-

5.2.3 Trade secrets and secrecy of correspondence

188. To find out more on this subject, see Annex 1 to this White Paper.

189. It is obvious that in order to be able to authorise or not authorise a person to access information, you must first identify that person, and thus have a reliable digital identity.

190. The identification proposed in this White Paper, which extends to the Function of an individual within a Community, clearly reinforces the quality of the identification needed to protect the intangible assets of companies/legal persons, which are themselves identifiable. It further compartmentalises my functions: the life cycle of function A and the associated access rights do not interfere with access to documents that I own in the context of function B.

5.3 Conclusion of contracts

191. Articles 1112 to 1171 of the Civil Code on the conclusion and validity of contracts leave the field of their conclusion by electronic means completely open. Electronic mail is mentioned by name, without referring specifically to Internet mail, thus leaving the way open for any system of the same nature. These Articles add an additional requirement over the obvious requirement for the quality of the identification of the contracting parties: the ability to know with certainty whether and when one party has received (or not) information from the other party.

192. In this respect, it should be recalled that the model proposed in this White Paper does not limit its scope of application to the signing of documents. The formal acceptance of an exchange (digital Object) may thus be covered by an Assertion (I accept — or I refuse[99] — an electronic exchange) between duly identified parties.

193. We define the Function, together with a Mandate, in the proposed digital Identities. Doing so clearly reinforces the legal quality of document exchanges when the submission and addressing of documents are tied to the strict framework of the Mandates of the persons involved. The contractual relationship between legal entities through their agents (representatives, employees, administrators) finds all its legal weight here too in the digital world.

5.4 Archiving of evidence

194. We have already mentioned on numerous occasions[100] the imperative need to archive the Assertions.

195. A very pertinent analysis of the question is proposed by Lucien Pauliac[101]. He notes the contradiction between Article 1379 of the Civil Code, which establishes the concept of “reliable copy”, and the implementing decree 2016-1673[102] concerning the possible modification of the copy deemed “unmodifiable” in the event that it is kept in electronic form and requires technical renewals for its preservation over time. The silver microform is essential for 3 reasons:

- The solution is proven and standardised by AFNOR;
- The evidence is irrefutable and cannot be modified by nature;
- It offers a net saving on the cost (energy expenditure, accommodation) of preservation.

196. The author draws the following conclusion with regard to electronic archiving: “Therefore, establishing or preserving one’s legal acts by methods that one knows in advance will arouse distrust is contrary to the purposes of pre-constituted evidence and, in a way, derogates from the requirements of the administration of evidence. When the law requires evidence of acts to be pre-established, the aim is to have effective evidence, not an enigma; the aim is that the resolution of disputes is simplified, not the contrary”.

197. It is up to the Actors to archive the Assertions and digital Objects that will contribute to the success of their claims, as is customary in law.

198. Depending on the nature of the Object and the action captured by the Assertion (access ticket to an application, consent to use my data on a website, invoice, contract, title deed), the duration of the archiving will vary from a few minutes to several decades.

199. It goes without saying that a strong digital Identity is essential both to control access to archives and to know who owns them.

200. With respect to the archives of businesses, public administrations, and all public or private bodies, the ability to provide legal entities with a digital identity, and to identify all the employees of these companies with an identity qualified by the Function carried out within these entities, has become an unavoidable necessity.

[99] The right to consent implies the right to renounce.

[100] See § 158, 169, 170.

[101] Lucien Pauliac, Le numérique, l’archivage, et la preuve.

[102] Decree 2016-1673 of 5 December 2016, JORF of 6 December 2016.

6. IMPLEMENTATION

Digital identity solutions must comply with the strict rules of evidence: evidence of the identity of the actors (and not of an IP address); evidence of consent; evidence of the constitution of agreements. They must be admissible and enforceable in court and irrevocably validate the right to act that links actors and actions.

6.1 The autonomy of evidence

201. There is a general principle in the rules of evidence: "evidence is not assumed; it must impose itself". In other words, there can be no ambiguity or residual doubt as to the observation that has been elevated to the rank of proof. This concept calls for another: the autonomy of evidence, i.e. the validity of evidence cannot depend on other elements, which are themselves unverifiable.

202. It follows that a simple and compact Identification Device (see section 6.2) will always be preferable to a complex Identification chain comprising many distributed subsystems.

203. A user confused by a cascade of menus, pop-up windows, badly clicked buttons or links, communication error messages, confirmation messages that are equally furtive or deleted by an unfortunate web page refresh, will always be able to claim in court: "Your Honour, my will has been altered by the complexity of the machine."

204. There is not even a need for a possible confusion: any programmable machinery, or with components distant from each other (a Web applet in your Internet browser, the input of the PIN code by the keyboard driver, and the calculation of the Assertion on the digital Object by the remote server) is an intermediate intelligence capable of altering the will of the Actor, whether by its possible failure or by malicious (re)programming.

205. Even the multi-windowing feature to which we are so accustomed on our computers and tablets, and our Web technologies whose page composition is by nature fragmented over multiple remote sources, do raise questions. It is very easy to substitute one content for another via the graphical overlay of windows without an outline; nor can a web page be guaranteed to be complete or intact, even without intent to harm, because of a communications mishap.

206. "Your Honour, my will has been altered by the complexity of the machine."

207. ⚠In other words, if there are electronic Devices that are:

- Non-programmable (frozen in their algorithms),
- Autonomous (they do not require any intervention from systems external to this Device),
- Under my control (the gesture[103] cannot be dissociated from the Device used to release the Identifier for the purpose of creating a new Assertion)
- Capable of making an Assertion linking the Identifier[104] I choose with the digital Object targeted by my action,

then it is clearly this type of Device that I must use.

6.2 Compact and biometric devices

208. We have understood that the difficulty lies in the irrevocable nature of Identification as defined in our model[105]:

- Having exclusive control over my identifiers;
- For the purpose of building Assertions linked to the digital Objects targeted by my action,
- Consecutive to the explicit expression[106] of my will (consent or renunciation[107]).

[103] See 174.

[104] That I choose from those assigned to me and associated with a valid Mandate.

[105] See 87

[106] It should neither be implicit (serial acts unless explicitly encompassing su

[107] See 175.

209. At this stage, the only currently reliable way to involve a specific real-world user in the autonomous making[108] of an Assertion in the digital world is to use biometrics in combination with a second factor[109], typically a removable physical token such as a key or a smart card that locks up the “secrets” necessary for cryptographic operations.

210. The requirement for autonomy argues strongly in favour of a local execution of the Identification; that is, a validation of the biometric captures and the generation of the Assertions within the Device and without any external agent.

211. Neither the remote validation using a central file of biometric masks (e.g. fingerprint, iris, face print), nor the calculation of Assertions by a central server is illegal. However, this raises security issues related to the transmission of these data through other systems that could intercept, alter or replay them without your knowledge. The calculation of Assertions by the central server further compounds these issues. What recourse will you have if a third party (the central system hosting provider, the server operator, the network provider) prevents you from expressing your identity at a critical moment because of a temporary unavailability?

212. All of these elements argue in favour of autonomous devices and, what’s more, these technologies already do exist.

213. Biometric technologies are evolving. They are diverse: fingerprints, facial recognition, iris, voice, micro blood vessels, neural electric fields, physiological microvibrations, and others based on implants, or even a combination of various means. We will therefore not discuss the reliability or merit of each of these techniques, or their resistance to attempts at falsification. The current rate of false positives [110] is under 1/1,000,000 in particular with fingerprints.

214. Proof is not a means; it is a result: what is to be done with the remaining millionth? The answer is found at the legal level: the supplier of the device must commit to achieve a certain result and not only to use best effort to achieve such result.

The residual risk will be covered with insurance; it’s that simple.

215. This is not so different from what is happening today for credit card operators, except that it concerns only one type of digital Object: the payment order. Operators are liable to compensate users for fraud, provided that users are not at fault. The operators’ commission includes insurance to cover a fraud rate (about 0.05%) that is much higher than the 1/1,000,000 of biometrics.

216. We must not forget the rules of proportionality, lawfulness, and purpose[111]. In other words, the implementation of means must be proportionate to the level of risks and stakes in addition to complying with the law.

217. This further confirms a necessity built into the model: namely about the plurality of identifiers, and the consequent flexibility for attaching means of recognition proportionate to the functional importance of each identifier.

218. You can also combine the use of digital identifiers without an attached Mandate[112], i.e. which are self-assigned and protected for example by a password. A structured identifier[113] is not without interest for managing your personal data associated with this identifier.

219. If we wish to integrate artificial entities (robots or AI) into our model, the Identification Devices will have to be sealed or possess unalterable physical characteristics such as an irremovable hardware chip that is indispensable for starting up processors. Such devices already exist.

6.3 With or without a central file

220. Personal data is “any information that directly or indirectly identifies a person”[114]. It does not matter whether this information is confidential or public.

221. In order for such data to no longer be considered personal[115], it must be rendered anonymous in such a manner that the data cannot be used to trace back to the subject. If it is possible to identify a person by cross-checking several pieces of information (such as age, gender, city, diploma) or by using various technical

[108] See 207.

[109] There are 3 factors maximum: (1) what I am (biometrics), (2) what I have (smart card or physical token), (3) what I know (a PIN code for example).

[110] Positive recognition of the supposed person, whereas it is someone else.

[111] Se GDPR, art. 5 and 6; French Data Protection Act, art. 4 and 5.

[112] See 139.

[113] As described in 133.

[114] Cnil definition: https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi.

[115] Subtle nuance: the legislation does not regulate the issue of personal data ownership.

means (IP address, cookies), then such information will also be considered personal data.

222. For ensuring strictly compliant use of personal data, it is imperative that any means used to produce a digital identity should guarantee that the person identifying themself retains control over the personal data associated with such identity (e.g.: “signed by Mr X, sales representative of company Y”). Once again, autonomous devices can ensure this function in the same way as a central identity file. The question of autonomy[116] is coupled with the question of personal data protection, which goes in exactly the same direction. And this second question is not limited to identity data: the calculation of Assertions by a central server uses even more personal data concerning who is doing what with whom and/or on whose behalf at what time.

223. ⚠ Therefore, choosing your device with or without the use of a central personal data file is important because the construction of a central personal data server or file is not necessary for the implementation of a digital Identity as proposed in this White Paper. The identity data (biometrics, full civil status, list of all attributes of the person) can remain within the Devices, the identifiers are digital, and the users retain full control over the information linked to those identifiers and published in directories associated with the above-mentioned Registries.

224. Nothing in the GDPR prohibits the storage of biometric data centrally on a dedicated server accessible remotely in a third party data centre (cloud), on the condition that appropriate security safeguards are set-up to address the risks.

225. Therefore, choosing whether or not to use a centralized file (and therefore any centralized generation of Assertions) will depend on the use case:

- Where the person with whom a transaction is carried out is the same as the operator of the central servers;

- In the case of a pre-formulated standard contract, where the Person to whom you must prove your identity is also the Person who has made the means of such identification available to you.

226. Electronic payment (by credit card or online banking) is a case in point. The debit or credit organisation provides me with the identification means that it has unilaterally determined (hence this so-called “pre-formulated standard contract”) to be adequate for the services it offers me. When I pay a merchant, it is to this organisation that I send my payment order. The merchant receives the proof of payment via its own payment processor and does not need to identify me[117]. Since this is a pre-formulated standard contract, any system malfunction or any fraud not attributable to me is the responsibility of the operator and entitles me to a refund.

227. Another example of pre-formulated standard contract is when you use state-issued identification means (i.e. made available by the state) with the authorities of the same state.

228. ⚠ In contrast, this is very different when it comes to setting up a digital identity that can be enforced against any person without any relationship to my supplier of Identification means, nor to the supplier of the opposing party: the operators concerned have no relationship either with the Object of the transaction, or with the opposing party systematically. In such case, it is therefore imperative to be a manufacturer of evidence (see Chapter 5, section 5.1), interoperable (see section 6.4) and inter-enforceable see Chapter 7, section 7.2).

6.4 Interoperable

229. Interoperability is an obvious legal necessity. Europe (in its regulations, such as the GDPR and eIDAS), standardization bodies, and United Nations bodies (such as UNCITRAL), impose that there can be no solution tied to a particular service or hardware provider. A digital identity solution cannot impose Android or iOS, nor depend on a particular provider; it must therefore work in all countries and on all networks, and be legally admissible in all states. Competition is the rule; it necessarily implies the definition of standards regarding data communicationand interfaces between the components of the solution.

230. ⚠ In our ecosystem of sovereign Communities, a community must be able to recognize the identity assigned by another Community/in another register, and in particular to be able to enrol the Functions of a person within a Community on the basis of identities already assigned elsewhere.

[116] See 210.

[117] Not for the payment itself, maybe for the services I buy, but then most probably not on the basis of my “bank identity”.

231. These issues and the list of data/interfaces to be standardized have been thoroughly studied but are beyond the scope of this White Paper. They will be published in future specifications.

6.5 Use cases: conclusion of contracts

232. Digital identity must create the conditions for ensuring the legal security of electronic, paper and other transactions exchanged between one or more natural or legal persons and between communicating objects. The service produced by this solution must be interoperable (independent of the operating systems), inter-enforceable (legally admissible in the 193 UN Member States), sustainable (constant over time) and supranational (no borders on the Internet).

233. Note that the modus operandi described here does not require any central file.

234. The system is based on an indivisible sequence of functions (or say functional kinematics) explained below and assuming a Device formed by:

- A smart card, which carries the user's identifiers, the encryption keys necessary for security, and the attributes of their identity;

- A fingerprint reader, where validation is a local operation[118] between protected data on the card and the fingerprint reader:

235. The systematic and indefectible linking of these points constitutes the necessary and sufficient elements of proof for the establishment of a contractual relationship that is enforceable against third parties, with a view to the formation of a contract or the expression of an obligation of any kind whatsoever.

6.5.1 Irrevocable identification of the signatory/sender of the document

236. Control – To be under the physical, moral and legal control of the cardholder.

- One of the first conditions necessary for the demonstration of proof of identity in a digital environment is that the actor has full and complete control over their physical and technological identification means. A local, compact, and non-reprogrammable Device is by nature not vulnerable to being controlled by others and remains under the exclusive control of the Actor who wishes to identify themself.

237. Autonomy – The ability to determine oneself.

- One of the complexities of the digital virtual space is the ability to dissociate several actions over separate system locations without any direct control over these locations although they may still look integrated. If all the operations take place on a sophisticated device like a computer, how can I be sure that the action I perceive is actually taking place on my computer?

- For the Device illustrated here, autonomy can be summarized as "the card reads the finger and the finger reads the card"; there is a technological imperative that guarantees that the pairing action between the Actor's will and the Device's capacity to link this physical particularity takes place without any possible external interference.

238. Autonomy guarantees the indivisibility of all activities that are needed to prove "Who am I?".

239. Quality – The fact of being formally empowered in a legal act.

- Beyond the validation of their identity, the actor must be able to indicate in what capacity they are empowered to act. It is necessary that the identity be legally qualified by the Function to which the identified person can refer, for example: director of company X, treasurer of association Y.

240. Capacity – The ability to enjoy certain rights and to exercise them.

- In addition, the actor must be able to validate the capacities to act that their Quality confers on them.

241. Corollary – Difference between the signatory and the sender.

- The devices intended to validate a digital identity must be able to distinguish the message signatory from the message sender, in order to preserve the rights and the capacity of each to act. This will also strengthen the rights of the addressee.

[118] Known as "Full Matching on Card".

6.5.2 Creating an unbreakable link between the signatory's consent and the subject matter of the consent

242. Consent – I am free to consent or object; I sign what I see and I see what I sign.

- As already mentioned, one of the complexities of the virtual space is the ability to dissociate several actions and lose any direct control. The Author can make a mistake and sign a document "B" instead of a document "A", just by confusing the various windows on the computer screen, without there being any fraud. With Web interfaces, what is seen is often the result of the assembly of many "pieces of a page" coming from different sources, and communication errors can alter their display without a visible impact.

- Otherwise, doubt exists about a true consent (or explicit objection); consent cannot be guaranteed and can therefore be challenged.

243. Causal link – Material warranty of the thing signed.

- This is the question of the causal link between the Actor and the Action. The Device generating the Actor's digital identity must, without any possible failure and with an obligation of result, ensure that there is a one-to-one and unbreakable link between the actor and the action, without any possibility of usurpation or copying.

244. Integrity – Guarantee of incorruptibility of the document.

- Upon the irrevocable identification of the actor, who has consented to an action, whose causal link will be definitively acquired, the result of the above-mentioned functions will have to be definitively encapsulated and encrypted in an act (final document) that is total, original, unique.

- The key here is to guarantee the technical modalities necessary to make the above-mentioned action immutable in time and space. Encrypted or not, the original form of the document must be guaranteed independently of the evolutions (updates) of the applications intended to read the said document.

245. Confidentiality – Only signatories and designated participants have access to the contents of the agreement.

- In strict compliance with the protection of trade secrets and the secrecy of correspondence. It is imperative that the communications formed from an identification and consent system (signature) guarantee the strictest confidentiality and protect the contracting parties from any dispersal of the information thus exchanged.

6.5.3 Irrevocable electronic signature

246. Irrevocability – An electronic signature must be irrevocable to be enforceable against third parties.

- In order to be enforceable against third parties, the consent (signature) given by the identity of the author must be irrevocable. Consequently, the system providing this service will have to be able to demonstrate both the sequence of functions and their indivisibility.

247. Supra-nationality – The Internet has no borders.

- In order to satisfy this criterion, the "identity-signature" service must comply with the legal constraints imposed by UNCITRAL[119] in this area. If so, the service will be admissible in the 193 signatory countries.

248. Pseudonymisation – The electronic signature does not require a central personal data file.

- By construction, the system described here does not need one. The intermediary exchange system can validate transactions using zero knowledge proofs (ZKP). These are protocols that allow an actor to prove that a situation is true without having to reveal information about it.[120]

249. Uniqueness – The signature is not reproducible. Each signature is unique and different.

- In order to guarantee the originality of each consented action, the mark of consent in its electronic form must be unique and exclusive to each action. Prohibiting the duplication and/or interception of any form of consent will protect the intrinsic quality of the consent linked to a specific action, which is essential for the demonstration of proof, and the security of the consented acts.

[119] UNCITRAL Model Law on Electronic Signatures (July 2001): 35 signatory countries.

United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005): 27 signatory countries.

[120] Guillaume Chanut, « Les zero-knowledge proofs (ZKP) : principe et applications », Cryptoast.fr 25 July 2020.

250. Non-corruptibility – The electronic signature must be protected.

- All of the component functions of the "identity - consent – contract" chain must be protected by cryptographic means that guarantee the end-to-end security of the exchanges carried out.

251. Multi-signature – The electronic signature must allow multiple signatures on the same document by several signatories.

- The ability to have multiple signatories is a necessity, especially for contracts. Moreover, each participant must be able to exercise their capacity without any interference with each other.

Note that the current signature standard (PAdES)[121] on PDF/A documents (PDF Archive) requires a strict sequence of signatures "stacked" on a single copy, which is either:

• (a) centralized, thereby raising the issues of central filing and autonomy (programmable remote server), or
• (b) circulated among the participants, thereby opening the door to obstruction or retention at the expense of subsequent signatories.

252. Enforceability – The electronic signature must be enforceable against third parties and legally admissible in the 193 Member States of the United Nations.

- Enforceability against third parties (where the first "third party" will be the judge) will be acquired on condition that the act is perfect, i.e. the parties involved are irrevocably identified, the consents are informed and indisputable, and that the terms and conditions under which the agreement is formed comply with the provisions laid down by UNCITRAL with regard to supranationality.

6.5.4 Creating an original document

253. Intervention of a third party – "no one can create evidence for themself".[122]

- According to the principle of the extrinsic quality of the formation of evidence, it is accepted that in a digital space where the means of making documents and signatures are accessible to all without leaving any trace, the intervention of a third party for the purpose of guaranteeing the legal quality of agreements formed online and/or the exchange of information in any form is necessary for the formation of agreements.

254. Note that current techniques (including "zero knowledge proofs"[123]) make it possible to guarantee this without having to know the content of or identify the participants in a digital transaction.

255. Exchange logs – Universal Time timestamp.

- Given the global scope of information transmission and the "borderless" nature of digital space, it will be agreed that, in order to be enforceable, time stamp must be based on universal time.

256. Validation of the signatory/sender – Right to act.

- In addition to the identity of the signatory, the system producing the consent (via a signature) must be able to indicate the rights to act of the parties involved in the agreements, in order to guarantee and protect the contracting parties as to the nature and amount of the commitments to which they mutually consent.

257. Original/Unique – The "identity-consent" service must be able to guarantee the originality of the document produced, throughout its existence.

- The Internet is by nature a system that favours the copying of information. It is therefore necessary to put in place a concept of "logical" original document independently of the copying of its media, rather than fighting against the digital copy that is always feasible, even with electronic "safes".

258. Integrity – Guarantee the incorruptibility of the document through suitable protection means.

- The integrity of the documents (information) exchanged must be guaranteed by encryption solutions that are necessary and sufficient to produce a unique original and ensure its uniqueness over time.

6.5.5 Irrevocable identification of the addressee

259. The requirements applicable to the control, autonomy, quality and capacity of the addressee are the same as those set out in 6.5.1 for the signatory who is the sender.

[121] PAdES (PDF Advanced Electronic Signature) is the format for electronic signatures included in PDF documents.

[122] See Clémence Mouly-Guillemaud, « La sentence « nul ne peut se constituer de preuve à soi-même » ou le droit de la preuve à l'épreuve de l'unilatéralisme », Revue trimestrielle de droit civil (RTD Civ.), Dalloz, 2007, pp.253 hal-02196195.

[123] See § 248.

260. Corollary – Difference between the addressee and the recipient.

6.5.6 Compliant delivery of the document

261. Integrity – Conformity to the above-mentioned original.[124]

262. Non-intrusive delivery – The document is fetched, not pushed.

- Considering that the digital space of a computer/PDA is a private space, any form of unsolicited delivery of data can be qualified as a violation of the private space. Furthermore, to be valid, the ability to accept must be proportional and reciprocal to the ability to refuse (you can refuse a registered letter). The email service provider must then:

- Ensure that the recipient can refuse delivery of an email,
- Ensure that emails are due at the address of the debtor and not of the creditor.

263. Confidentiality – Only the addressee can read the document.

- The service must guarantee the addressee the utmost confidentiality of the messages received.

6.6 User case: payment

264. The bill of exchange - With an irrevocable identity and more or less the same sequence of functions as the one just described above. The bill of exchange and, more generally, all commercial bills can be reinvented.

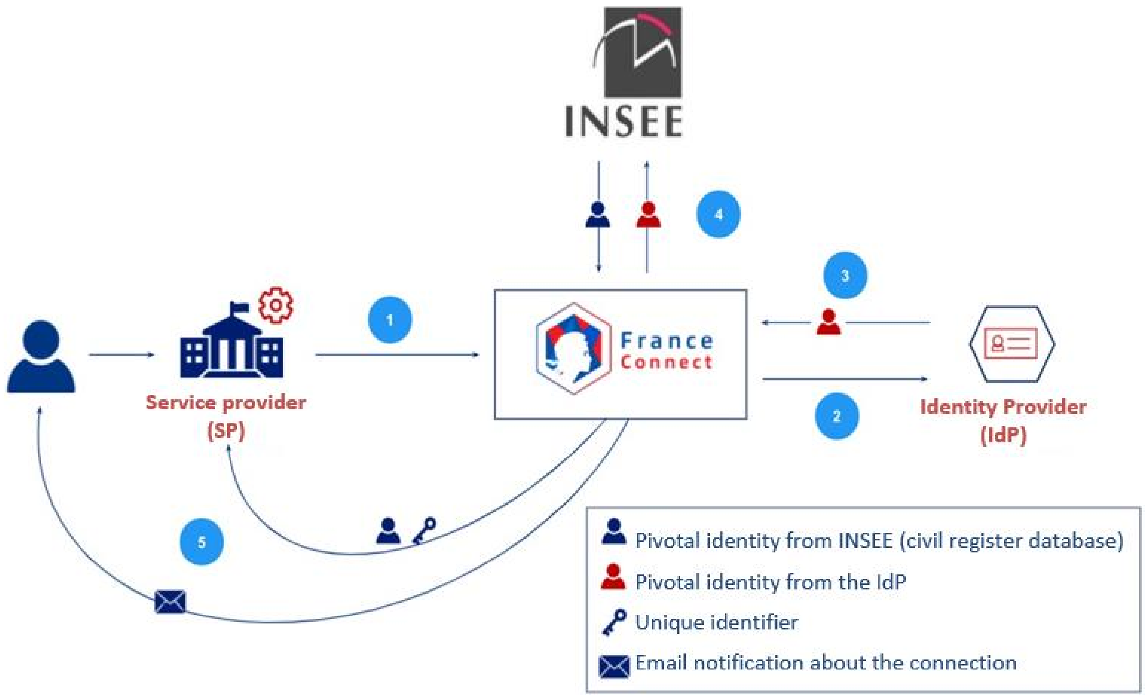
6.7 FranceConnect system

265. FranceConnect is a system designed by the government to facilitate and secure online procedures.

6.7.1 FranceConnect

266. The FranceConnect system is a federating system between Service Providers (SPs) and Identity Providers (IdPs) for the state-issued identity, also known as the "pivotal identity": last name, first names, date and place of birth, sex, and optionally an alias and email address.

267. The figure below and the related explanations come from the documentation available on the Partners portal of franceconnect.gouv.fr.


INSEE
4
3
1
France Connect
Service provider (SP)
2
Identity Provider (IdP)
5
Pivotal identity from INSEE (civil register database)
Pivotal identity from the IdP
Unique identifier
Email notification about the connection

(1) The Service Provider (SP) requests the Trusted Third Party (TTP) to send all or part of the user's personal data (pivotal identity) in accordance with the authorisation.
(2) The user selects an Identity Provider (IdP) and identifies themself using the identifiers of their account with the IdP.
(3) The IdP sends FranceConnect the user's pivotal identity (last name, first name(s), date and place of birth, sex), the preferred name if known to the IdP, and the contact email (the email may differ depending on the IdP chosen by the user).
(4) FranceConnect requests validation of the pivotal identity from INSEE, which rectifies it in the event of a small discrepancy. FranceConnect generates a unique identifier for the user, specific to the IdP.
(5) FranceConnect sends the pivotal identity and the unique identifier to the SP. The user is connected to the service and informed by email.

[124] See section 6.5.4.

268. This platform's advantage is to isolate service providers and identity providers, based on the principle that identity providers do not know what service the user is requesting to access, and the service provider does not know the personal identity data used to authenticate (as they define it) the user.

269. From our point of view, FranceConnect is above all a technical system that allows the French state to confirm the state-issued identity of a person while relieving itself of the identification management and service operation, leading to substantial savings in effort and resources for all the actors.

270. The service provider (SP) is able to accept a new user without having to go through all the procedures for issuing a sufficiently secure identification to this user; the SP also obtains the guarantee of processing an official state-issued identity, without any responsibility for the quality of the ad hoc Identification (apart from requiring a minimum level of security, e.g. "substantial" or "high" under eIDAS).

271. The Identity Provider (IdP) offers each new user potential access to all FranceConnect service providers (SPs); it delivers eIDAS-certified identification means without having to worry about the nature or value of the services that will be used, and therefore without liability for any damage in case of misuse. The user also benefits from the system: the user only has to register once to have access to all the FranceConnect-related services.

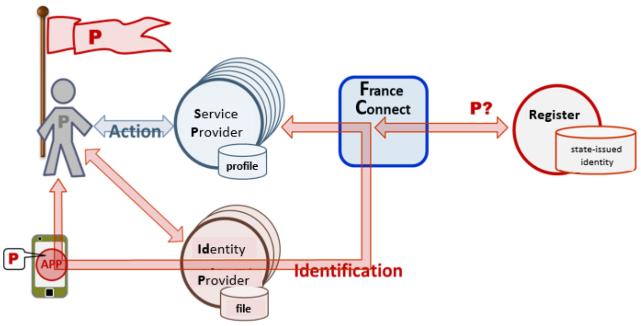
272. FranceConnect is based on the "Open ID Connect" and "OAuth 2.0"[125] authentication standards, which were designed to allow web service operators (SP) to share identifiers that are already registered with another operator (an IdP who is also often a SP as well).

273. Haven't you ever logged on to a service provider – for shopping, photos, blogs, press, forum, hosting services – that now accepts your Google or Facebook identifiers? At first glance, this is a nice simplification, but it makes tracking your activities all the more effective. Worse, as already mentioned in the Preamble, with this system cloud giants (SP role only) can offer access to their online services using the company's internal identifiers (IdP role). In other words, while being paid for their office services, they can observe the internal activity of each client company.

274. In the original architecture, "Open ID Connect" and "OAuth 2.0" are designed to directly connect SPs and IdPs in a fully meshed N-to-N architecture. FranceConnect has very cleverly extended these standards to act as a federating intermediary in an N-to-1-to-N star architecture so as to maintain its role as a repository for state-issued identities.

275. This is a defensive approach to the sovereignty of the state in the face of the digital flood[126]. The division of roles here is the result of a technical and pragmatic vision rather than a legal one; it is illustrated in the figure below. The banner floating above our user's head represents the digital identity that the user can exercise.

276. In this figure, a cell phone is part of the Identification Device used. Identity providers can of course propose other means under eIDAS certifications[127] or General Security Referential[128] applicable to administrations under the supervision of the French National Cybersecurity Agency (ANSSI).[129]



[125] OpenID Connect is an identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user. For more Information: https://openid.net/connect/.

[126] See Chapter 7.

[127] Certifications provided for in the "eIDAS" Regulation No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[128] Certifications provided for in the RGS (General Security Referential – *référentiel général de sécurité*) aimed at standardising administrative exchanges, under the terms of Order 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and in-between administrative authorities.

[129] For more information, https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/

6.7.2 Sovereign Communities

277. The legal approach to digital Identity that we propose leads to a much different, and — we believe — much more universal distribution of roles. This distribution is illustrated in the figure opposite: the system is very simple since the various — and all validated — digital Identities have been stored in the Device, with the agreement of its owner[130] and the confirmation of an enroller of the Community concerned. Since the Device is by construction under the exclusive control of its owner, the owner is then entirely autonomous to assert the identity they choose to exercise.

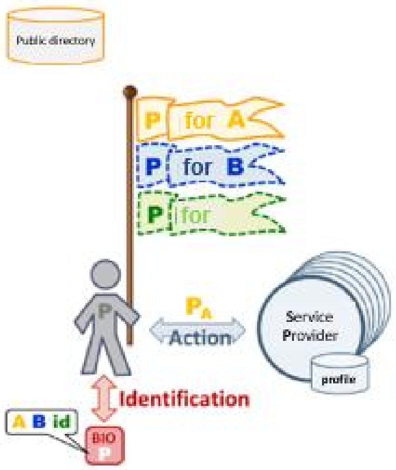
278. ⚠ This autonomy of identification (without interaction with a central system) is added to the autonomy of proof.[131] No third-party system can interfere with the user's desire to identify themself, nor can it substitute for it.

279. The initial enrolment phase is illustrated in the figure opposite for only one of our user's digital identities. This operation only takes place at the creation of an assignment (a Function in a Community), and at the creation of the identity "idem" / in the user's own name. Such enrolment is only repeated in the event of loss or renewal of Identification means (e.g. smart card), and when updating the biometric capture masks (to avoid any substitution of the person).

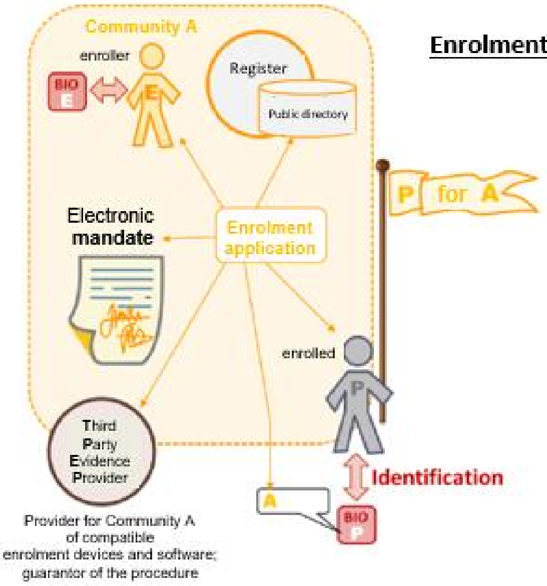
280. Here, the "Third Party Evidence Provider" replaces the Identity Provider (IdP). Its role is quite different from that of an IdP and the name "Third Party Evidence Provider" clearly indicates that this entity is only there to provide the Communities — and more specifically the persons legally mandated by these Communities to enrol members (e.g. the human resources manager in a company) — with the interoperable means necessary for the enrolment, without being able to interfere in the enrolment process other than as a guarantor of the procedure. The Provider will not be able to collect any personal data of the enrolled person.

281. ⚠ As identity and security properties[132] are separated, the periodic renewal of security variables (e.g. every 2 years on average for cryptographic keys, certificates) does not require any complicated operation: the user's Device management application identifies that the security variables will shortly expire and will simply request the user's agreement to the update. This agreement must be explicit: in order to ensure that the user retains exclusive control of the Device, there can be no change, even like updating community certificates, without the user's consent.

Exploitation Phase



Enrolment Phase



Provider for Community A of compatible enrolment devices and software; guarantor of the procedure

282. There would be much more to explain about the enrolment and operational phases, but that is beyond the scope of this White Paper. The necessary specifications will be subject of a companion document to this White Paper.

283. The proposed approach is not incompatible with FranceConnect. Communities can become Identity Providers (IdPs) in the FranceConnect architecture through Third Party Evidence Providers. They are able to validate the authenticity of an identification (precisely, of a Digital Identity thanks to the reference to the Mandate) without being able to identify the persons.[133]

[130] See section 6.2.

[131] See section 6.1.

[132] See above 76.

[133] This statement may seem contradictory; it is based on a lesser-known but well-tried technique in cryptography: "zero knowledge proofs" (ZKP). On this concept, see section 6.5.3.

7. DEPLOYMENT

The expression “digital sovereignty”, which is gradually spreading, was popularized by Pierre Bellanger, who received extensive media coverage first in 2008, before publishing *La souveraineté numérique* in 2014 (éditions Stock).

7.1 Creating an ecosystem of sovereign communities

7.1.1 Digital sovereignty

284. The intrusion into all activities of social and economic life of networks which are in the hands of a few private companies whose profits rival the GDP of many developed countries calls into question the sovereignty of states.

285. Even if we do not share all the predictions of Skyrock CEO and founder, Pierre Bellanger[134], concerning the future dependence of individuals, companies, and states on networked computer systems (the *“résogiciel”*[135]) in the hands of a few private and mostly American companies (Big Tech), we cannot deny that this movement is under way.

286. The traditional concept of sovereignty was introduced by Jean Bodin in the 16th century “to enable the king to free himself from both feudal lords and the power of the church”[136]. Today, the concept refers to the legitimate power of the (elected or authoritarian) state to govern a territory and a population without interference from outside powers for the purpose of retaining control over its destiny.

287. “There are few remaining areas in which the exercise of the state’s powers is not yet enslaved to digital networks and thus dependent on those who govern these networks: monetary and fiscal policies, defence, social systems, industrial policy, health systems, energy, culture, education, information and communication, transportation, and even the preservation of archives”.[137]

288. The concept of digital sovereignty, on which depend both the problem and its solutions, can be understood at different levels:[138]

1. “Claimed by states, digital sovereignty is not, however, conceived in the same way by all: according to an authoritarian and offensive conception, it establishes the right for the state to regain control of digital spaces in order to apply its laws and promote its interests there; according to a more liberal and defensive conception, it establishes the right for the state to protect its citizens against the surveillance and exploitation policies implemented in cyberspace by entities driven by their own interests.”
2. “But digital sovereignty can also be the sovereignty collectively claimed by groups of digital users, or even by more or less organized communities of Internet users who want to be involved in determining the applicable rules and to participate in organizing the protection of their data on the networks. Recognizing [this] right for communities [...] leads in a certain way to transpose to the digital world the traditional reflection on the formation of civil societies and the transition to political societies.”
3. “Digital sovereignty is also that of the individual from the point of view of their capacity for self-determination, for ordering for themself, for controlling their data”.

289. The concept can therefore be construed very differently, whether it is a question of extending the sovereignty of states or imagining new forms of non-state sovereignty. It has legal, economic, technical or functional meanings, and can be conceived at many levels: individual, collective (community of users), national (e.g. preservation of public records on a “sovereign cloud”), European (protection of personal data), or even international (network governance) level.

[134] Pierre Bellanger, La souveraineté numérique, Paris, Ed. Stock 2014.

[135] On the definition and mission of *“résogiciel”*, see https://pierrebellanger.skyrock.com/tags/cNtC2lXjcUw-resogiciel.html

[136] Pauline Türk et Christian Vallar, La souveraineté numérique: Le concept, les enjeux, Ed. Mar & Martin, 2018.

[137] Pauline Türk et Christian Vallar, cited above.

[138] Pauline Türk et Christian Vallar, cited above.

290. Rather than associating a new form of sovereignty with the digital world, Karim Benyekhlef sees above all a “competition of sovereignties” amplified by the Internet, and capable of redesigning the contours.[139]

291. ⚠ It is this model that is relevant in practice, because it does not exclude any mechanism of Law as long as one can identify the person in relation to one or more communities within which or for which the individual exercises their activity. This collectively begins with one’s own person and extends to the global scale, including companies, interest groups, states, and unions (e.g. Europe), each level having a form of sovereignty, nested within the others[140] and interacting with each other.

292. The emergence of an international law of the Internet or even a universal digital constitution would in no way upset our model; it would just add one more level to which it will be necessary to refer in order to determine the applicable law from the moment we know the individual and their Mandate (by what right can they exercise their Function). One can even imagine that the virtual world would come to interpose/superimpose its own transnational digital communities to those of companies and states, with a level of ad hoc legal rules.

293. ⚠ A digital identity cannot therefore be conceived outside of a community, but it can be attached to several communities, with the individual having an assignment in each of the communities, hence the (indivisible) model of the digital Identifier: <registry> + <community> + <personal identifier> + <function/assignment> + <mandate/capacity to act>.

294. ⚠ In our system[141] based on human rights and freedom, the individual is sovereign in their decision to join communities, and these communities are sovereign with respect to the systems of Law which they choose to endorse. They are also sovereign as entities protected from the potential interference of other entities to which they have not chosen to belong.

7.1.2 Legal approach: national sovereignty

295. National sovereignty is the principle that sovereignty belongs to the nation, which is an abstract, single and indivisible collective entity. Sovereign states make commitments and thus mutually safeguard their sovereignty and interests through numerous bilateral or multilateral agreements.

296. To identify irrevocably each citizen composing a nation, while safeguarding each of the fundamental rights, implies creating the necessary provisions for the preservation of a national sovereignty, even at the level of unions[142], on a solid and shared legal basis.

7.1.3 Political and economic approach: the sovereignty of economic operators

297. According to this political and economic approach, digital sovereignty would be that of economic operators who have the de facto power to impose rules.

298. Today, a few multinationals (Big Tech) exercise real command and regulatory power in cyberspace. They set the terms of use for online services that have become indispensable, develop algorithms, decide to delete content, close a user’s profile, keep or sell the personal data they store, and so on and so forth.

299. Some create their own virtual currencies (Bitcoin, Libra project), and have their own legal services for dispute resolution. Others are building projects for societies based on technological progress, in which they would provide services equivalent or even superior to those of the states, thereby replacing them.

300. ⚠ With the digital identity proposed in this White Paper, we could strongly restore order to this anarchy: the website user will be relieved from having to approve each time a bundle of opaque terms of use, whose primary purpose is to collect a maximum of the user’s personal data and whose mass of legal condi-

[139] Karim Benyekhlef, L’Internet : un reflet de la concurrence des souverainetés, Lex Electronica, vol. 8, n° 1, automne 2002.

[140] For example, in the company, the employment contract and the internal regulations are added to the collective bargaining agreements and then to the law applicable to the company, which is determined by the industrial sector to which the company belongs, the (potentially digital) territory in which it operates and finally its nationality (the state).

[141] Civil law system or Napoleonic law as opposed to Anglo-Saxon law or common law.

[142] The Court of Justice of the European Union struck a blow on 16 July 2020 by invalidating with immediate effect the “Privacy Shield” which governed data exchanges between the United States and Europe (CJEU judgment C 311/18, known as *Schrems II*). In so doing, the CJEU sent a message both to the American authorities, who were able to use the Cloud Act to access the data of all monitored individuals, whether American or non-American, regardless of where the data is stored, as long as these individuals are customers of an American company..., but also directly to Big Tech companies, which gladly collect all the personal data of their customers.

tions is only a counter-advertisement to the European institutions that are actually seeking to protect users' privacy

301. For example, the company (the Community) within which a person exercises a function that leads such person to use a Web service can predetermine the applicable rules of confidentiality, steering its employee clear of any error at the same time as ensuring the level of protection that it has chosen (as a legal entity) for its intangible assets.

302. Such employee can, the same evening, use the same Web service and this time — duly identified by their personal identity and not by their business identity — decide to take advantage of the personalized service by sharing their personal calendar (their identity not allowing them, for example, to access their work calendar). Or, the employee can also join a purely virtual "Do not track" community and identify themself through it to benefit from the ad hoc protection of their personal data without having to go through the service provider's terms of use.

7.1.4 Liberal approach: the digital sovereignty of users

303. A third, more liberal and individualistic approach is possible: the digital sovereignty of users. Inspired by the foundations of popular sovereignty, according to which citizens are the source of all power, it corresponds to the right of individuals to self-determination.

304. Users can make choices, express preferences, stop using certain applications, have a say in forums dedicated to technical standardization (e.g. the W3C, a non-profit standards organisation responsible for fostering compatibility of World Wide Web technologies such as HTML, XHTML, XML), or simply act as consumers.

305. The power envisaged here can be exercised collectively, in the context of user communities (transnational SW developer forums), in the context of a corporate function, or individually[143].

306. The concept of digital sovereignty is therefore not limited to the strict traditional legal perspective, attached to the power of states. In its broadest sense, it refers to the power of command and the right to self-determination in a digital world. Who sets the rules? On what basis and with what legitimacy? Who do we obey, and with what guarantees? Answering these questions means understanding who is sovereign on the networks and how this sovereignty is expressed.

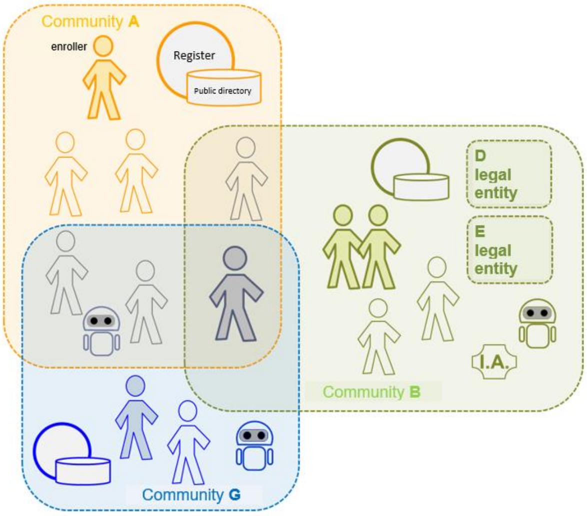
307. ⚠ How can one claim any kind of sovereignty without possessing an irrevocable, legally admissible (mandated), and supranational digital identity?

7.1.5 An ecosystem of competing community sovereignties

308. As a reminder, the Communities in our model may be private companies, professional associations, public institutes and organisations, the state, or purely virtual and potentially transnational communities. The state itself, depending on its size and administrative organisation, can opt for a mega sovereign community or a sub-division into departmental, provincial or regional communities.

309. As Communities are most generally legal entities, they will have their own digital identity (exercised through their legal representatives — mandated in this role, since a legal entity has no capacity to act in its own right), but they may also take a Function in other communities.

310. The integration of robots and AI in the model is just as easy as the integration of natural and legal persons (Figure below).



[143] In concrete terms, this translates into rights and guarantees that are in the process of being enshrined, such as the right to personal data protection, right to data portability, to be forgotten or to dereferencing, which could be included in a more general right to "informational self-determination" according to the German approach; Pauline Türk, « Le droit à l'autodétermination informationnelle », Revue Politeia, 2017, n° 31.

7.2 Supra-nationality and inter-enforceability

311. The growing use of New Information and Communication Technologies (NICT) has structurally modified the legal conditions for demonstrating the identity of Internet users. The providers of these technologies and related services have allowed the use of avatars to grow and have been satisfied with self-declarations of identity, which are often multiple and varied for one and the same individual. It is now clear that this situation has become impractical and is contrary to the interests of both providers and users.

312. To remedy the above, and although the demonstration of proof of identity is clearly explained above (perfect proof), the question of the territoriality of the applicable law now arises. Why should the law of one country prevail over that of another? It is the United Nations which, within the United Nations Commission for the Development of International Trade (UNCITRAL), has established the conditions of acceptability of the applicable law by imposing the legal principle of supra-nationality. This principle was accepted by the 193 countries making up the UN in 2005.

313. Supranational means something that is placed above national institutions and that is therefore enforceable against them in law.

314. It is within this supranational framework that UNCITRAL sets out 4 necessary provisions:

- It is essential that the person wishing to show proof of their identity has full and complete control over their identification means. This requirement excludes de facto all solutions that can be voluntarily or involuntarily manipulated by any person who can directly or indirectly take control of the means used to demonstrate proof: complicity of the software vendor, hacking, remote control of electronic tools by the infrastructure operators, or simply the enslavement of a central signature server!

- Interoperability requires, by definition, that each solution (software, smart cards, peripherals of any kind) be compatible with all of the systems in activity;

- Inter-enforceability is the ability for all identification solutions to comply with the legal provisions set out by UNCITRAL and therefore admissible in court before the jurisdictions of the UN;

- Durability is the ability to guarantee both the identity verification services and the elements of proof over time.

7.3 Towards a universal digital identity

315. We have seen above that an electronic document has the same legal value as a paper document as long as it complies with the same legal rules.
Regarding digital identity, we have seen that the law that applies is that of perfect proof in the context of a strict legal analysis; in other words, all interpretations and/or presumptions will be null and void.

316. Technological neutrality is therefore essential. Courts will focus on the technical sequences that prove identity only in a second stage; they will first and foremost ensure that the means used to prove identity comply with the key principles of the rules of evidence.

317. It is common ground that successive laws and regulations that regulate the formation of digital identity evidence set out the rights and obligations of individuals in a generic manner, without regard to the technological means by which the activities in question are carried out. The law is not concerned with the specific technological framework put in place. The law does not specify the technology that must be used to achieve and maintain the integrity of documents and to establish a legal relationship with a document. In this way, in the interests of neutrality, it neither favours nor disadvantages the use of one technology over another.

318. Technological neutrality means that the law should not discriminate between different technologies. The law must not favour the use of one technology over another. In other words, the law gives all technologies equal legal recognition on the basis of conditions that do not impose an obligation to act in accordance with any particular norm or standard.

319. It is important to understand that neutrality applies both to the distinction between paper and digital media and to the distinction between the technologies themselves. This is the universality of technologies.

320. There are no borders on the Internet. This raises the question of the legal territoriality that can be enforced in court in the event of a dispute. That’s when supranational law helps resolving the difficulties raised by territorial jurisdiction. As said above, it is the UN, and more precisely the UNCITRAL, that has set the conditions for the acceptability of applicable law by imposing the legal principle of supra-nationality.

321. UNCITRAL also examined the question of monopolistic control by a state over identity. It concluded that, as far as digital identity is concerned, no state should have a monopoly, thus leaving choice and competition in service offerings to the market.

322. A second step towards the universality of digital identity was taken. This is the geographical universality.

323. In the same spirit of universality, assuming that the irrevocable digital identity is acquired, its use will have to be required for all online digital services, with due account of interoperability and inter-enforceability. This is the universality of usage.

324. ⚠ The reference model proposed in this White Paper is therefore neutral in all these respects and is therefore specific to a universal identity. The implementation specifications (which are beyond the scope of this White Paper) remain just as neutral provided that they are limited to the interfaces necessary for interoperability: structure of the Identifier, interfaces of the Devices, structures of the Assertions.

7.4 Facilitating Cybersecurity

325. According to the working definition given by Wikipedia, cybersecurity means “the set of laws, policies, tools, devices, security concepts, mechanisms, risk management methods, actions, training, best practices, and technologies that can be used to protect the individuals and the tangible and intangible (directly or indirectly network-connected) IT assets of states and organisations (with the objective of availability, integrity & authenticity, confidentiality, proof & non-repudiation).”

326. If we go into a little more detail, we could complete this definition with the different contexts in which security is applied. For example, we can talk about:

- Network security, which includes the policies and practices adopted to control the data flow within the network and at access points, to avoid bottlenecks (denial of service attacks) and to protect its configuration in order to avoid address or machine name hijacking.
- Application security, which aims to protect software, devices and connected devices.
- Information security, which ensures the integrity, confidentiality and availability of data in transit or at rest in an information system.

327. Cybersecurity is adapting as cyber threats evolve. With the COVID-19 health crisis, the level of cyberattacks has significantly exploded across the globe: hackers took advantage of the remote connections of personal computers via insecure home networks, and phishing with COVID-19 related ads was greatly facilitated as everyone was affected. Crypto-currencies, which are anonymously traded, have made ransomware attacks very popular. The exfiltration of personal or sensitive data then resold on the “dark web” has become a very lucrative market for hackers.

328. Moreover, hacking no longer requires a computer expert: ready-to-use and regularly updated (to include the latest exploitable computer flaws) hacking tools can be purchased and phishing attacks can be launched using Trojan horses.

329. The risks are no longer individual: cyberattacks can bring a company down, cause damage to an entire state (e.g. disruption of electricity or water distribution infrastructures, attack on financial markets, attack on communication networks, disruption of air/rail/road traffic management, health systems), or even disrupt the exercise of democracy[144] (dissemination of fake news, influences and incentives, alteration of elections).

330. The problem in all this is not the lack of “identity” but the unreliability of identity. The ability to impersonate someone else is the basis of the vast majority of attacks: taking the identity of a person (email, mailing), a business (phishing, scams, malware), or more technically a system (IP addresses), or even a website (domain names).

[144] « Des utilisateurs de Facebook « manipulés » pour une expérience psychologique », Lemonde.fr, 30 June 2014 and William Audureau, « Ce qu’il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook », Lemonde.fr, 22 March 2018.

331. ⚠ The digital identity proposed in this White Paper makes it possible to identify individuals (natural persons), companies (legal entities) and connected systems or devices, and to know, for each of them, who their principal is (natural person or a legal entity). The reliability of these identities can then enable a considerable reduction in computer attacks.

332. It is not necessary to know personally your contact point (person, company, or system) if you know with certainty that they cannot escape their liability. You can trust an unknown person if you are certain that they can be held accountable, because the identity that will be given is irrevocable.

7.4.1 The case of electronic messages

333. It is unfortunate that this communication medium (e.g. email, tweets, chat, forums), which is so easy to use, so commonplace, a primary means of exchanging information and a tool for social ties, has become – because of electronic anonymity – the favourite playground for cybercriminals: it is time to rethink the law and create means of identifying the actors working on the networks.

334. What would the road network have become without license plates? Chaos. A brief experience in an IT support team in charge of the email gateways of a large company is enough to realize that chaos results from anonymity, and this chaos is rooted in the shortcomings of ad hoc Internet protocols[145] whose design — remarkable for the simplicity of their implementation — did not anticipate at all that these protocols could be hijacked in a desire to do harm or just for profit.

335. Filtering emails will be very simple: everything that is not attached to a verified Identification will be thrown into the trash can; no need to know the email sender, no need to filter names, no need to manage blacklists; any email becomes “enforceable” by nature and therefore liable to give rise to damages.

336. Why should we regress and accept electronic flyers that invade our mailboxes, whereas a majority of them are malicious? 60% of the emails entering the email gateways of companies is undesirable; 95% of these, or even more, are rejected by the anti-spam filters before even reaching their addressee, but there will always be some left to pass through the filters, especially those that borrow the identity — currently “unverifiable” — of your correspondents.

7.4.2 Identity + Security = Surety

337. A digital identity that is enforceable by law, supranational and that guarantees the total protection of personal data, is an absolute necessity from which the digital industry can no longer exempt itself.

[145] ESMTP et al.

8. BIBLIOGRAPHY

Bernard Benhamou (coord.), Internet des objets et souveraineté numérique: perspectives industrielles et enjeux de régulation, Institut de la souveraineté numérique-Afnic, 2021

P. Bellanger, La souveraineté numérique, Stock 2014

A.Bensoussan, V. Bensoussan Brulé et J. Bensoussan, Jurisprudence Données personnelles - Décisions tendances 2018-2020Lexing Editions, 2021

A. Bensoussan, Informatique et libertés, Editions Francis Lefebvre, 3e éd., 2020

A. Bensoussan et J. Bensoussan, IA, Robots et Droit, Bruylant, 2019

A. Bensoussan, A. (direction), Informatique Télécoms Internet, Editions Francis Lefebvre, 6e éd., 2017

K. Benyekhlef, L'Internet : un reflet de la concurrence des souverainetés, lex-electronica.org, Éd., 2002

N. Chambardon, L'identité numérique de la personne humaine. Université Lyon 2, Ecole doctorale de droit, 2018 https://hal.archives-ouvertes.fr/tel-02464483/document

M. Karamanli, C. Hennion et J.-M. Mis, Rapport d'information N°3190, par la mission d'information sur l'identité numérique. Assemblée Nationale, 2020

B. Mallet-Bricout et T. Favario, L'identité, un singulier au pluriel, Dalloz, 3, Éd., 2015

G. Montagnier, R. Guillien et S. Guinchard, Lexique des termes juridiques, Dalloz, 16 e éd., 2007.

L. Pauliac, Signature électronique : naissance du « faux faux » et du « faux conforme », 2017 https://www.linkedin.com/pulse/signature-%C3%A9lectronique-naissance-du-faux-et-conforme-lucien-pauliac/

L. Pauliac, Le numérique, l'archivage, et la preuve. https://www.scriptum-archives.fr/pauliac.html

P. Türk et C. Vallar, La souveraineté numérique : le concept, les enjeux, Ed. Mar & Martin, 2018.

9. ANNEXES

ANNEX 1: TRADE SECRETS AND SECRECY OF CORRESPONDENCE

1. Trade secrets and secrecy of correspondence

Provided that the identity of a natural or legal person meets the conditions detailed in this White Paper (perfect proof, data protection, supra-nationality), the identification that irrevocably identifies the authors of the information and those who access such information will be eligible for benefiting from the protection of trade secrets and secrecy of correspondence.

2. Definition of trade secrets

Article L. 151-1 of the French Commercial Code sets out three criteria for information to be a “trade secret”.

Information is protected by trade secret if it meets all of the following requirements:

- It is not generally known among persons familiar with this kind of information in these industry sectors, neither readily accessible to them; and
- Its secret nature entails an established or potential commercial value; and
- under such circumstances, it is subject to reasonable steps to keep it secret.

The usual information that may constitute a trade secret is about know-how, technological or technical knowledge, and commercial data. The information is protected only if it is held legitimately or has been obtained lawfully.

3. Judicial protection of trade secrets

A person who violates a trade secret is civilly liable. The expiration period is that of ordinary law, i.e. 5 years.

4. Secrecy of correspondence

“Correspondence” denotes any oral or written exchange between several people.

Legally, it is considered to be of a private nature. As a matter of principle, it is forbidden to make it public. This principle, known as the “secrecy of correspondence” is enshrined in various legislations concerning the protection of private life, including Article 9 of the French Civil Code, which states that “Everyone has the right to respect for his private life”, or by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, related to the respect for private and family life.

Under that principle, any form of transmission, including electronic messages, shall be strictly restricted to viewing by intended recipients. The law severely punishes any breach of the secrecy of correspondence. However, courts have held that there are degrees of confidentiality, which are assessed at the sole discretion of the judge.

The French Penal Code (Article 226-15) punishes the following by one year’s imprisonment and a fine of €45,000:

- opening, destroying, delaying or diverting correspondence sent to a third party, whether or not it arrives at its destination, or gaining knowledge of it by fraudulent or malicious means;
- intercepting, diverting, using or disclosing correspondence sent, transmitted or received by means of telecommunication, or setting up a device designed to produce such interceptions by fraudulent or malicious means.

ANNEX 2: ONLINE REPUTATION

If a company fails to implement sufficient technical security measures, its data may be stolen. With the implementation of the General Data Protection Regulation (GDPR) data theft can have important legal consequences.

The GDPR grants to supervisory authorities (in France, the CNIL), the ability to impose financial penalties up to 20 million euros or, in the case of a legal person, up to 4% of its total worldwide annual turnover.

Since then, the CNIL has issued several financial penalties against companies for proven breaches of their security obligations regarding personal data of their customers.

For example, in December 2018, a ride-hailing company was fined €400,000 following a data theft impacting 57 million accounts. This happened whereas the platform had been informed of a first attack the previous year and had agreed to pay the hackers the sum of 100,000 euros so that they would not reveal this flaw to their users and delete the stolen data.

It did not work... because a similar attack happened again a few months later, and the CNIL then rightly fined the company for not having taken sufficient security measures to protect the personal data of its customers.[146]

What were the security flaws exploited by the hackers in this case?

In its decision, the CNIL detailed how the attack took place.

It originated on the GitHub collaborative platform, a private work platform used by the ride-hailing company's software engineers and on which their identifiers were stored in clear text. The username was made of their personal email and accompanied by an individual password.

The attackers used these identifiers to connect to the GitHub platform, where they found an unencrypted access key that allowed them to access the hosting platform on which the personal data of the ride-hailing company's users was stored. This key also allowed the attackers to access the company's databases and steal the personal data of millions of users.

The CNIL's sanctions committee pointed out that access should have been subject to adequate security measures, including authentication and withdrawal of former engineer's authorisations, which the ride-hailing company failed to take.

The CNIL's sanctions committee highlighted that securing the connection to the "Amazon Web Services S3" servers was a basic precaution and that filtering IP addresses would have made it possible to avoid these unauthorised connections.

More recently, the CNIL issued a financial penalty against a real estate management company. In May 2019[147], the company was fined 400,000 euros for not having secured the personal data of its customers. An audit of the company's website had revealed that documents holding personal data of applicants for apartment rental was freely available, without prior authentication, to all website visitors. All that was required to access such data was to edit a part of the URL address displayed in their browser.

[146] For an analysis, see A.Bensoussan, V. Bensoussan Brulé and J. Bensoussan, Jurisprudence Données personnelles - Décisions tendances 2018-2020, Lexing Editions, 2021

[147] Cnil 28 May 2019, Délib. SAN-2019-005, upheld by CE 4 November 2020, req. n° 433311.

Outside France, some hacking cases have had a devastating effect on the security of personal data and even caused suicides. For example, the dating website “Ashley Madison” was hacked in the United States in 2015.

The 37 million customers database of this extramarital affair website, containing names, email addresses and even sexual preferences of users were disclosed on the Internet. Users received blackmail letters and a pastor even committed suicide.

An investigation by the Australian and Canadian privacy authorities revealed that the security and confidentiality measures were obsolete: lack of security updates for the various databases, lack of devices to detect computer attacks, non-expiring data records even in cases where the member asked to delete his account, to name but a few.

In another 2015 high-profile hack, the personal data (names, aliases, logins and passwords, some banking and medical data) from 80 million customers of the American insurance company Anthem was stolen. The hackers used login/passwords to authenticate at other sites and used the data to cast phishing campaigns.

All these cases demonstrate that the Login/Password authentication pair, however strong it may be, is no longer sufficient to ensure total digital security and privacy of users' data.

Even when Internet users choose complex passwords meeting the robustness standards recommended by the CNIL (8 characters minimum, use of upper- and lower-case letters and special characters, validity period of 6 months maximum), their data can still be stolen directly from the servers of operating companies.

Printing: Imprimerie Bialec SAS
23 All. des Grands Pâquis,
54180 Heillecourt December 2021

Image Credit
Fotolia - Adobe Stock

Lexing Alain Bensoussan Avocats
58, boulevard Gouvion-Saint-Cyr
75017 Paris France
Tel.: +33(1) 82 73 05 05
Fax: +33(1) 82 73 05 06
Mob.: +33(6) 74 48 13 25 / +33(6) 74 17 60 04
www.alain-bensoussan.com

A plea for a DIGITAL IDENTITY

This White Paper on “Digital Identity 5.0” proposes a basis for building digital identities in sovereign communities, whether at the level of a state, a commercial company, or a simple interest group.

It is a plea for a digital identity that will be able to:

- ensure “a flow of information enforceable in court”, allowing you to assert your rights and protect yourself from abuse, without escaping your obligations;
- guarantee the protection of your privacy, as any use of your identity in connection with digital information will result from your sovereign will;
- protect your intangible assets, as there will be — if you so decide— no more limbo as to the ownership and sharing of your data;
- defend democracy by clearly separating information coming from identified (and liable) sources by opposition to anonymous, altered, misappropriate or fabricated information;
- identify all actors of the economic and social life: not only natural and legal persons, but also autonomous robots and “virtual creatures” of the digital world (including AI with which we already interact), thereby ensuring that their mandators are accountable.
- establish a system of digital trust by and for the benefit of businesses, providing all public and private actors with the capacity for mutual recognition, in such a manner that it will create the trust that is essential for the smooth running of businesses.

Alain Bensoussan,
Lawyer, Paris Bar
Alain Bensoussan Avocats Lexing

Philippe Morel,
Digital identity specialist,
co-founder of Woobe

Bernard Hauzeur,
IT architect, security and digital identity expert,
co-founder of Woobe

Dinesh Ujoodah,
CEO, A3BC

Anthony Sitbon,
Consultant, Head of the Security Department,
Alain Bensoussan Avocats Lexing

Frédéric Forster,
Lawyer, Head of the Telco Department,
Alain Bensoussan Avocats Lexing