The eIDAS Regulation, and notably the principle of mutual recognition, has been
a major step towards fostering a trusted Single Market for digital services.
step towards fostering a trusted Single Market for digital services.

The Regulation responded to a demand that has proved to be growing and much needed:
trust in electronic transactions, especially of the identity of the person behind the online activity.
of the identity of the person behind the online activity. In short, to promote the creation of one of the essential elements for the development of the Internet of Value.
for the development of the Internet of Value.

Subsequently, other standards have also stressed the need to apply secure identity tools in certain sectoral areas.
secure identity tools in certain sectoral areas. The closest example is PSD2 in the area of digital payments, which has meant the
of digital payments which has meant the requirement for secure identification by means of two-factor authentication (SFA).
authentication factor (SCA) to enable the development of the European single market for digital payments, reducing the brakes
reducing the brakes associated with fraud in payment transactions, i.e. the uncertainty and insecurity associated with the
uncertainty and insecurity associated with the identity of payers of digital payments.

The experience gained over the years allows us to reflect on the strengths and weaknesses of certain trust services, and to
associated with certain trust services, in particular their implementation and dissemination in certain specific areas.
in certain specific areas. It even makes it possible to point out a strategic opportunity for the
digital industry in Europe to play a key and central role as a guarantor of the necessary secure digital identity.
guarantor of the secure digital identity necessary for the development of the Internet of Value.
Seizing this opportunity would mean contributing to the advancement of the digital industry in Europe in the areas of secure digital identity, secure digital services, and secure digital services.
on the issues of secure digital identity, setting an example for other geopolitical areas.

And from the experience of these years of implementing the eIDAS Regulation, two aspects emerge:
on the one hand, the need for the European authorities to lead and finance the creation of the
the creation of user guides with the appropriate standards for European users on the solutions provided by the
solutions provided by the industry in Europe and, on the other hand, the need to pay more attention to usability and adoption of the
attention to the usability and adoption of secure digital identity technology solutions.
secure.

We will start by commenting on the need for pro-activity in guidelines at European level rather than the
current adaptation. The closest example is the recent developments related to the
the implementation of the SCA of the PSD2 in European digital payments, which have highlighted the difficulty for an industry such as the
the difficulty for an industry such as the financial industry to adopt, on a company-by-company level, a uniform level of
company level, a uniformly higher level of requirements in terms of identity security.

Probably the lack of technical knowledge in many financial operators and in some regulators has led to an evident delay in the adoption of a uniform level of identity security requirements at company level.
regulators have led to an evident delay in the EBA guidelines and, consequently, in the implementation of SCA technologies.
implementation of the SCA technologies required by the PSD2 regulation. As a consequence
of this lack of focus, the deadline of 14 September 2019 set out in PSD2 has been widely missed and has
and has forced the EBA to advise a period of "supervisory flexibility" until December 2019.
"supervisory flexibility" until December 2020.

It is a fact in October 2019 that technology is already available to ensure timely compliance.
compliance in a timely manner. In fact, financial institutions in some countries European countries (the Nordic countries) have already been implementing the required level of security in authentication through
authentication through technologies such as SIM-based technologies1. .

Such technologies that would enable the SCA requirements of the PSD2 to be met can be provided
immediately and interoperably (globally open standard). In particular through services based on the Mobile Connect standard, which has been developed by the GSMA globally and which is already
is already implemented in many European countries and therefore available to users with a mobile phone (e.g. in the UK).
mobile phone users (i.e. almost all European citizens).
European citizens).

However, the lack of guidance from the European institutions (the EU Commission, the EBA, etc.) in the
promoting the uptake of this type of technology has missed an opportunity to provide a better scenario in which
provide a better scenario in which European financial institutions could comply on time with the PSD regulation.
PSD2 compliance in a timely manner.

The European Commission would need to analyse the impact of the delay in the adoption of PSD2 solutions by the economic sectors.
of secure identification solutions by economic sectors and, in the light of the results, make the necessary proposals to
the results, make the necessary proposals to support the dissemination and adoption of secure identification solutions (SIM
(SIM Based such as those based on the Mobile Connect technology standard).

On the other hand, there is a need for roadmaps to take into account the usability of the solutions and, therefore, to make the necessary proposals to support the dissemination and adoption of SIM-based solutions.
of the solutions and, therefore, their ease of adoption. If solutions are very robust but not very usable, citizens will not adopt them.
If solutions are very robust but not very usable, citizens will not adopt them and the level of security will be lower than desirable.
In this sense, we have examples of sectors in which highly secure technological solutions have been developed for the services of
solutions have been developed for digital trust services, but are not very usable and therefore poorly adopted by citizens.
therefore poorly adopted by users. This is the case of identification services for eGovernment services such as the Spanish eDNI or the Cl@ve PIN system. Both are highly secure
very secure (certified as trusted services at EU level) but so complex to use (they require the installation of proprietary software and/or the
(they require the installation of proprietary software and/or the availability of a reader) that they are hardly used by citizens.

hardly used by citizens. In the case of public services, there is also the added
complexity of the co-existence of different
complexity of the coexistence of different geographic levels of public
authorities (in the case of Spain, there is a coexistence of levels of public
In the case of public services, there is also the complexity of the coexistence
of different geographical levels of public authorities (in the Spanish case,
there is a coexistence of state, regional and local levels of administration),
each sovereign in
the adoption of secure digital identification mechanisms (which leads to further
fragmentation and lack of interoperability).
fragmentation and lack of interoperability). To give a figure, according to the
website of the Ministry of the Interior, the eDNI can be used in the following
ways
According to the Ministry of the Interior's website, the eDNI can be used in a
few dozen local governments, whereas in Spain there are more than 8,000 local
governments.
there are more than 8,000 local governments in which it should be used in order
for it to really be a usable digital identity solution.
be a usable digital identity solution.

To solve these problems, it would be necessary for the European Commission to
carry out an impact analysis of the real
impact analysis of the actual use (not just availability) of digital trust
service solutions at the level of eGovernment services.
digital trust services solutions at the level of eGovernment services (not only
at the national, but also at the regional and local
and also at regional and local levels) and of the societal benefits that
European citizens would enjoy if they
would enjoy if they had a secure digital identification mechanism on their
mobile phone line based on an interoperable standard.
based on an interoperable standard. This is the case that the French government
has followed with
France Connect and could be rapidly extended to countries where mobile operators
already have such a standard in place, such as
have already implemented such a standard, as is the case in Spain.

In addition, the development of a secure digital identity solution based on SIM-
based technologies could have many applications in the following fields
SIM Based technologies could have many applications in fields that need
solutions such as the following.
following:

- Access control for minors to online adult content (e.g. gaming). The access of
minors to
of minors to content that may be legal but is intended for adults is an issue of
growing concern.
is an issue of growing concern. The requirement for a secure digital identity
(of which, while respecting anonymity, certain components such as the age of
majority requirement can be consulted) would bring
The requirement for a secure digital identity (of which, while respecting
anonymity, certain components such as the age of majority requirement can be
consulted) would bring security to the development of businesses such as gaming,
while respecting compliance with regulations on the protection of minors.

- Reducing levels of fraud in activities such as the online resale of tickets
for shows.
of tickets for events. The regulation of the resale of entertainment tickets has
become outdated in a context in which much of the
in a context where much of the sale and resale is done online. The combination
of
of the requirement for secure digital identity (easy, usable and universal) and
blockchain technology could provide a way out of the
technology could provide a way out for the smooth development of the business,
avoiding possible consumer fraud problems that may occur.

fraud problems that may arise.