Keystones of digital citizenship. This report follows a letter of referral from the Secretary of State for Digital Affairs in July 2019. It includes 35 recommendations to guide the government in the development of French digital identities. The report deals with the need to make government digital identities a public service accessible to all and inclusive. It recalls the efforts that need to be made in terms of communication and training to create a digital citizenship that meets the challenges of the 21st century. It also addresses the issues of governance, security and sovereignty specific to digital identities, emphasising the need to create and provide the necessary safeguards for better control of this service.

In the context of the revision of the eIDAS Regulation and the consultations launched by the Commission, the Council would like to make a contribution to the Council would like to make a contribution to the "inception impact assessment". As mentioned in the paper, the three options considered: revision of the current framework combined with measures to speed up the process (option 1), opening up identification schemes to the private sector (option 2) to the private sector (option 2), and the establishment of a European EUid scheme (option 3) have advantages and advantages and disadvantages. A solution taking into account all three options could be the most ideal. ideal. Indeed, the Council would like to recall that it strongly values multiple digital identity solutions in line with the French model (FranceConnect), which leaves the choice to the citizen to use the identity they wish (public or private) depending on the procedure they wish to carry out.

Nevertheless, the Council would like to highlight several of its recommendations that could be of interest to the Commission regarding the different solutions.

Concerning option 1, the Council proposed five recommendations (from 26 to 30) concerning the revision of the eIDAS Regulation. In particular, it proposes to:
Standardise the peer review process, in particular in terms of documentation and methodology, and clarify its purpose and scope;
Define a body of documentation containing the information that must be automatically provided by Member States on their electronic identification schemes;
Start by clarification of the Regulation's own requirements for the substantial and high levels of Start with clarifying the Regulation's own requirements for substantial and high levels of assurance.
Specify in the eIDAS Regulation the minimum criteria for remote identification.
Harmonisation and assessment of the reliability of remote identification methods identification methods (e.g. the number of challenges to be made by the user in the case of facial recognition, or a standardisation of the false positive/false negative rate impacting the percentage of identification percentage) would be welcome in order to harmonise the practices implemented

practices implemented in the Member States.

Concerning the economic impact of options 2 and 3, the Council has doubts. While it is true that the digital identity solutions proposed in the two options will create added value and positive externalities, there is no evidence that citizens in the various countries will not take advantage of them. Indeed, the consultations carried out by the National Digital Council showed that individuals had difficulties in trusting digital identity: some of them would tend to favour the historical identity actors (States) while others would favour private actors (mistrust in States). Faced with these results, option 2 might not convince the majority and we would tend to think that Europe (option 3) is not a strong enough trustworthy actor. Nevertheless, option 3 seems extremely interesting for the identities of the legal persons and objects that gravitate in the single market.

Concerning the social impact, we have doubts about the realisation of the following proposal "The possibility for user to actively manage attributes, credentials and attestations [...] would empower user control of digital identity and enable personalised online services in a trusted environment where online privacy can be ensured and data is protected. While digital identities can indeed increase people's level of ability, control and management of their identity and personal data as well as the services they receive, we believe that the level of digital literacy is not yet high enough to encompass all European populations. As we suggest in our recommendations 12 and 13, we believe that it is necessary to provide training for all age groups before and in parallel with the development of digital identities. European funds could be earmarked for this with a view to improving digital citizenship. Moreover, the social impact must be considered from the design of design of digital identity solutions by ensuring that they are inclusive and accessible in their accessible in their design, pathways and functionality.

Regarding rights and freedoms, the Council maintains that it is important to let citizens choose the digital identity solutions they want to use, if they want to use one.

Regarding option 2, the Council considers in its report that it was necessary to oblige private services through a public service delegation if they were to provide digital identity services on behalf of the State. In addition, it considers that the control and monitoring and monitoring capacities of the bodies in charge of personal data protection should be increased. data protection.

As regards the environmental impact, the Council has not studied this issue in the context of digital identities. However, it has just published a roadmap for reducing the environmental impact of digital impact of the digital environment.