

## Revision of the eIDAS regulation – European Digital Identity

The eIDAS Regulation (entered into force in 2014) introduced a first cross-border framework for trusted digital identities and trust services. However, its potential remains still underexploited. Only 15 of 27 Member States offer an eID to their citizens. One of these 15 Member States is Italy.

Italy notified 2 different means of electronic identification (eID): SPID and the electronic identity card. Both can be used cross-border. The former counts more than 10 million eID issued (as of August 31, 2020), growing by more than 1 million unit per month, the latter more than 15 million. SPID can be used to have access to the online services offered by almost 4,478 public service providers (as of July 31, 2020), and is open to be used by the private sector on a usage based tariff: currently 11 private service providers have been authorized by Italian Agency for Digital (as of June 30, 2020). In the first 7 months of 2020 the login with SPID **exceeded 40 million**.

The Italian models have proved to be virtuous and it is important that it continues to be promoted and encouraged, in order to represent an example for other European countries.

### COMMENTS ON THE POLICY OPTIONS PRESENTED

The first option, properly integrated, seems to be the only one effectively pursuable. The others, while presenting points of value, might introduce some critical elements, with potential economical and organizational impacts on the digital identity models currently in place (Identity Providers and public Service Providers), already used in a pervasive manner.

Any Commission intervention should be based on technological neutrality with a special attention to the eID models already in place and the interoperability node system currently used. Only in this way can the maximum efficiency with the widest dissemination be achieved. In this sense, a link with the Strong Customer Authentication (SCA) provided by the PSD2 might play an important role in the promotion of the application of eID under eIDAS also by the private sector.

#### **Option 1:**

The full enhancement of option 1 should include **amendments and additions to Regulation (EU) 910/2014 related to:**

- the definition of a model that ensures, also through the provision of specific obligations on private service providers, the application of the eID scheme to the private sector - starting from the one already implemented for the public sector. This eID scheme should ensure the mutual recognition at the European level based on the level of guarantee required. Then, considering the need to ensure a sustainability of the entire system, it is highly recommended that the application of the eID scheme to the private sector provides for a specific access fee defined at national level.
- the application of the identification model also on devices or applications used for the Internet of Things.

Only in this way can European online and e-commerce services be more effective and safer.

## **Option 2:**

The introduction of digital identity trusted services, other than the eIDs already implemented under the eIDAS Regulation, should not be pursued. As previously noted, if this were to happen it could undermine the massive efforts, organizational and economic, put in place by the Member States that have already developed notified digital identity systems. As already mentioned, the employment of already existing eID schemes would enable significant synergies to be easily exploited (especially in Italy where the eID scheme has been already adopted by some private entities); not to mention all the advantages for citizens who can use the same eID for public but also private services throughout Europe (One for All). All advantages that would not be possible with the provision of new trust services for identification.

Furthermore, the adoption of a new trust service for the identification in the private sector, other than the eID system already implemented, could risk not to respect the level of guarantee deemed sufficient for services that process personal and, in some cases, sensitive data. According to the GDPR, private trust providers must define the best way to mitigate the risks identified under the risk assessment, no specific rules are provided. The Data Protection Authorities intervene only after the breach. It is too risky in that case.

Similar problems could also occur with reference to the recognition of these possible new identification trust services, where the qualification and supervision procedures of the Member States were not standardized in order to guarantee the same levels of security.

## **Option 3:**

The introduction of a new European digital identity system (EUid) complementary to eIDAS for citizens' access to public and private online services does not seem to bring particular advantages; on the contrary it could jeopardize the investments made to date. In fact, the intervention might appear as a disincentive with respect to what has been developed up to now and to the schemes currently notified and with a growing adoption rate throughout Europe; schemes that are already interoperable thanks to the support of the EC itself through the Implementing Regulation (EU) 2015/1501.

The introduction of a mandatory notification of at least one eID scheme for each Member State (with the mutual recognition of notified systems) would instead have significant benefits.