Committed to Europe

Orange views on the review of the electronic identification Regulation and the new European Digital Identity

Executive summary

Orange, as a multi-service operator, welcomes the Commission's initiative to revise and expand the electronic identification and trust services for electronic transactions (eIDAS) Regulation. We support ambitious initiatives in this domain such as the extension of its scope to the private sector, new rules for authentication on digital devices and the introduction of a European Digital Identity (EUid) scheme to access online public and private services.

Achieving a review addressing those three targets would be beneficial not only to the digitalisation of, and trust in, official digitalised documents (e.g. driving license, health insurance, etc.) but also to secure transactions in a hyper-connected digital world. Mobile device solutions have a great potential as such devices are widely used by European citizens, but need a favourable framework to be massively deployed within the single market so as to avoid fragmentation or lock-in proprietary solutions.

To trigger the potential of digital ID and trust services on digital devices, Orange suggests the following changes to the Regulation:

- eIDAS services should be available to all citizens and extended to the private sector and to the digital devices;
- Implementation of eIDAS services on digital devices (smartphones) should be based on interoperable solutions independently from any specific type of actor with a security-by-design approach;
- eIDAS-compliant solutions that use secure hardware such as secure elements in mobile devices should be supported by policy makers and standardised;
- eIDAS-compliant service providers should be able to deploy interoperable standardised solutions made available on all kinds of digital devices (smartphones).

Our society is becoming increasingly digitalised, but digital identity solutions remain fragmented, with a risk for EU digital sovereignty

With the first eIDAS Regulation, the European institutions laid the foundations and a predictable legal framework to safely access services and carry out transactions online and across borders. After this first step, Orange welcomes the European Commission willingness to review this Regulation with the objective of providing all citizens, private companies and public administrations secure digital identity solutions.

Digital identity solutions are becoming key, especially on mobile devices. More and more European citizens use services on their mobiles; they expect and need secure identification systems, for instance to access digital secure services, being public (e.g. e-Government, e-Health) or private (ex: banking services, transport). There is therefore a great role to play for mobile devices' solutions.

However, service providers in public or private sectors cannot easily deploy their secure services on mobiles in the EU for the following reasons:

- They are unable to address all smartphones;
- It is not possible to provide a sustainable level of security to all devices; it will depend on the solutions deployed by each and every operating system or device manufacturer, i.e. the service providers have no choice than to adapt to their solution;
- The situation is currently complex in terms of legal framework (contractual, technical…);
- Market fragmentation is high; there is a strong dependency on key global players, like device manufacturers or OS vendors who are deploying their own technology and tend to promote their own services.

This creates a situation where competitiveness and sovereignty of the EU are at risk:

- Risk for the EU players to lose ground on the development of secure mobile services;
- Risk of dependence for Member States on technological solutions and identification systems not defined in the EU.

The revision of the eIDAS is therefore a timely occasion to implement an ambitious strategy on digital identity solutions and boost the European digital market.

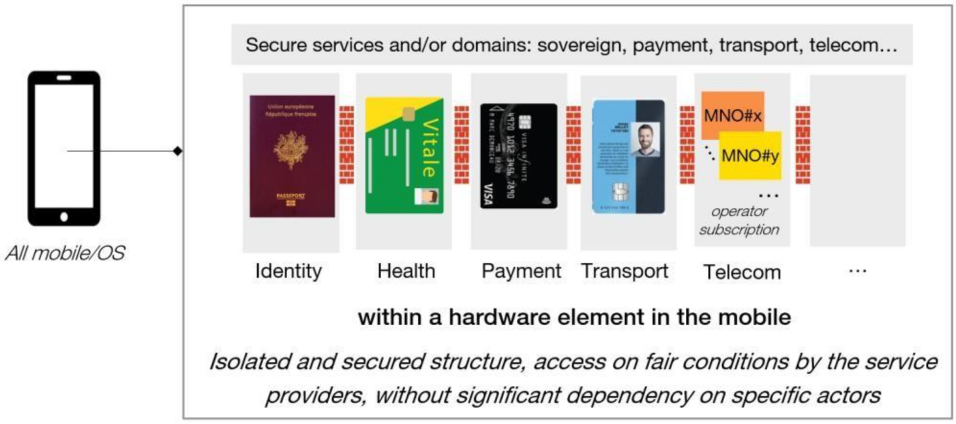
A new solution for an interoperable and highly secured identification system on mobile devices

Hosting secured services in a hardware element of mobile devices

The mobile industry has already worked extensively to develop standardised and easy to use solutions for clients' authentication online. This is the case for instance with Mobile Connect.

To complete those initiatives and ensure a wide accessibility for services that deserve strong authentication requirements and independently from any type of provider, Orange has initiated together with the mobile industry and manufacturers, the standardisation of a core solution for hosting secured services and sensitive data (attributes, credentials, attestations…) in a hardware element of mobile devices. This GSMA standardisation work is named Secured Applications for Mobile – SAM.

Such a highly secured element in the hardware of the mobile device will be divided into several "domains" (ex: identity, health, transport, etc.) where all corresponding service providers could be hosted.


All mobile/OS
Secure services and/or domains: sovereign, payment, transport, telecom…
Vitale
MNO#x
MNO#y
…
operator subscription
Identity
Health
Payment
Transport
Telecom
…
within a hardware element in the mobile
Isolated and secured structure, access on fair conditions by the service providers, without significant dependency on specific actors

With such a solution, only the end user will be able to manage his sensitive data, ensuring data protection and privacy in line with the GDPR. It means that online identification and authentication will be made independently from any specific type of actor.

This hosting solution should be interoperable and accessible to any accredited service provider from their back-end(s) via standardised interfaces; security and certifications for service providers will be developed according to the specific needs of the different hosted services and/or domains and delivered by competent authorities.

Standardisation work in progress

The standardisation work started in February 2020 in a dedicated GSMA working group gathering many key actors such as device manufacturers, operating system makers, chipset vendors and mobile operators worldwide. GSMA has defined use cases that include identity services supporting the eIDAS level "substantial", as well as the digitalisation of official documents (e.g. driving license on mobile).

The requirements should be completed by Q4 2020 and the technical specification by H1 2021, in close cooperation with relevant standards bodies (e.g. GlobalPlatform, ETSI).

Implementing the standardised solution

This standard solution for secured services builds an interoperable and secured framework for the deployment of digital ID and other trust services on secure element on devices. It should be made available by all smartphone manufacturers to service providers and all citizens without any kind of discrimination.

This is the only way to cover a wide range of smartphones and to prevent isolated solutions from individual manufacturers or service providers, which have previously prevented broad market dissemination. Furthermore, this solution could also be considered to implement a EUid scheme on mobiles, as a way to reduce the current fragmentation.

Such an ambitious approach would ease the deployment of secured applications on mobiles in the public and private sectors offering many advantages:

- Simplification and dematerialisation of services including sensitive services, especially public ones, for a large number of users and citizens;
- Innovation and competitiveness in public and private sectors with increased trust services reach in the mobile environment;
- Cybersecurity, with a certified security solution meeting the expectations of national and European public authorities;
- Digital sovereignty, with the ability to deploy services without significant dependency on proprietary solutions;
- Administrative processes in European Member States should continue to be harmonised and adapted to the digital age.

For more information: https://oran.ge/in-Brussels , or follow us on Twitter: @Orange_Brussels