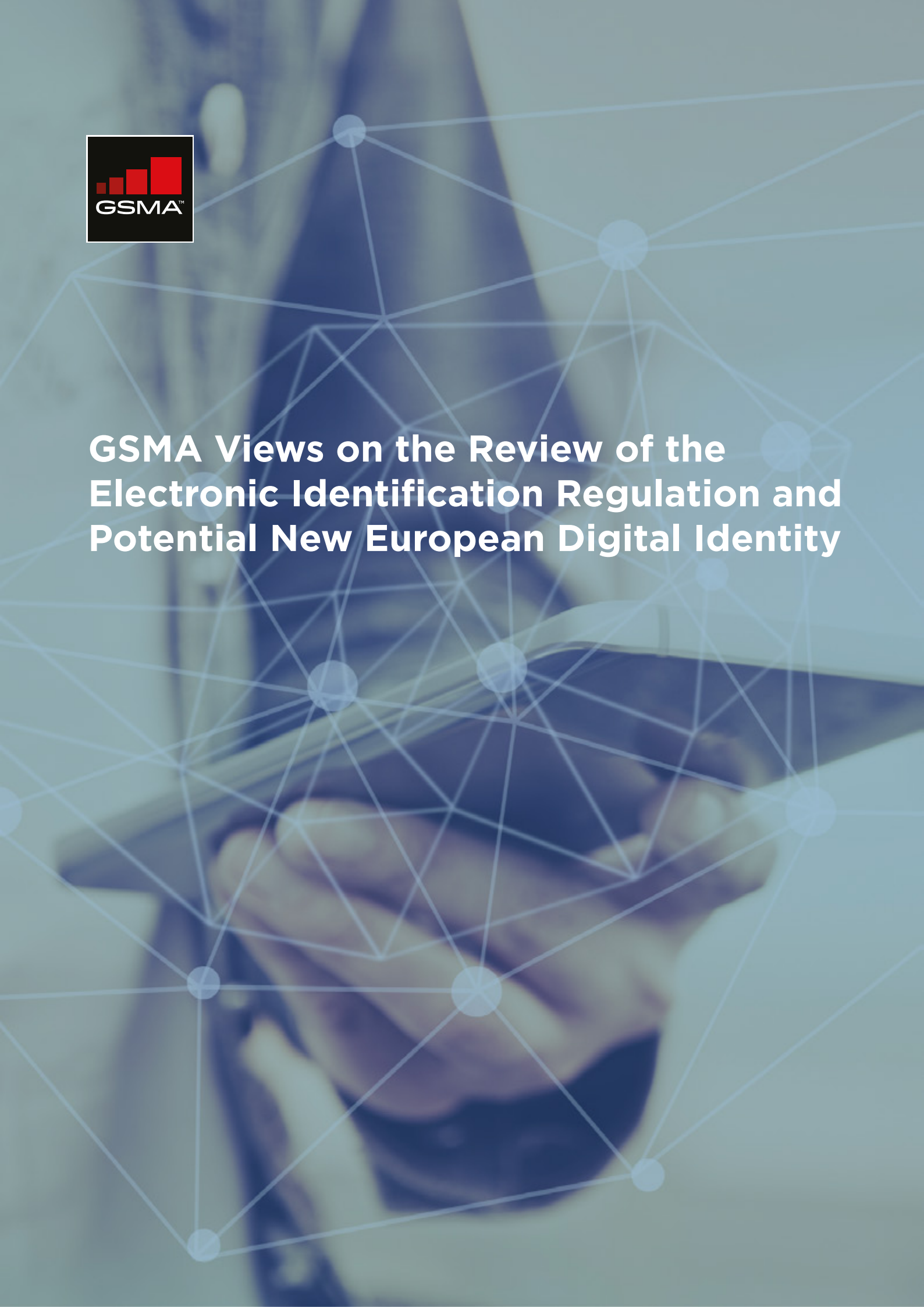

GSMA Views on the Review of the Electronic Identification Regulation and Potential New European Digital Identity

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at **gsma.com**

Follow the GSMA on Twitter:
@GSMA
@GSMAEurope

Contact:

Helene Vigue
Head of Go-to-Market, Personal Data, GSMA
hvigue@gsma.com

Andrzej Ochocki
Head of Identity, Deutsche Telekom and
Chair of the European Identity Group, GSMA
Andrzej.Ochocki@telekom.de

Executive Summary

The GSMA, specifically representing the European Mobile Network Operators involved in Identity Services in this instance, expressly welcomes the Commission's approach to revise and expand the eIDAS Regulation. We favour a combination of the three potential options described in the Inception document.

We support ambitious initiatives in this domain such as the extension of 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 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, GSMA 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 with guarantee of digital sovereignty and a security-by-design approach;

- eIDAS-compliant solutions that use secure hardware such as secure elements in mobile devices, SIM cards or eSIMs should be supported by policy makers and standardised;

- eIDAS-compliant service providers should be able to deploy interoperable standardised solutions made available on all kind of digital devices (smartphones).

Our Society is Becoming Digitalised, but Digital Identity Solutions Remain Fragmented, with a Risk for the 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, GSMA 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. An increasing number of 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 (e.g. banking services, transport). There is therefore a great role to play for mobile solutions.

However, service providers in public or private sectors cannot currently 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 manufacturers, i.e. the service providers have no choice other than to adapt to their solutions;

- Some existing eID providers in the market are limiting the use of their eIDs by case or geography (e.g. some Banking eID solutions);

- Some existing eID vendors impose contractual usage limitations in eID service brokering, thereby limiting service growth and complicating the entry of new competing eID solutions to the market;

- 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 defined abroad.

The EUid should go far beyond the previous approach of the eIDAS regulation and enable the use in both the public and the private sector. The revision of 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 secure element of mobile devices

The mobile industry has already done significant work to develop standardised and easy to use solutions for customers' authentication online. This is the case for instance with Mobile Connect, where eIDAS compliance has already been demonstrated in effective provisioning of cross-border services:

GSMA Report: Mobile Connect for Cross-Border Digital Services (Lessons learned from the eIDAS Pilot)

ENISA Report: eIDAS Compliant eID Solutions (March 2020) – Detailed description of Mobile Connect

To complete those initiatives and ensure a wide accessibility for services that deserve strong authentication requirements, independently from any type of providers, the European mobile telecommunication industry and manufacturers have initiated the specification of a core solution for hosting secured services and referencing sensitive data (attributes, credentials, attestations…) in a secure hardware element of mobile devices. This GSMA specification work is named "AM.01 -Secured Applets for Mobile Configuration" and is due to be published soon.

The issue of access to the secure elements in smartphones is currently open and should be regulated throughout Europe in connection with the eIDAS regulation. At present, most manufacturers use proprietary secure elements only for their own applications. We strongly recommend to create the legal and regulatory framework for standardised and non-discriminatory use of the secure elements already installed in most smartphones for service providers. This is the best way to implement the digital transformation and to maintain and strengthen the sovereignty of Europe, all Member States and each European in the digital world.

Levels of Assurance

The new eIDAS regulation should make it possible to derive an EUid from various underlying IDs such as an electronic identity card. A level of trust should be defined for eIDs, that indicates both the "level" of the underlying and of the derived EUid and can also underline the use of hardware security.

The eIDAS regulation is based on the three levels of assurance “low”, “substantial” and “high”, reflected in the design of the eID. In the opinion of the GSMA, the current technology openness of eIDAS leads to too much scope for interpretation and, for example, to an equalization of hardware and software solutions. From GSMA point of view, eIDAS compliant solutions that incorporate secure hardware, such as secure elements in smartphones, offer significantly increased protection e.g. against identity theft. Therefore, at least the introduction of a mechanism strength definition is favoured, in which the implementation on evaluated security hardware should lead to a higher value. The introduction of new intermediate stages (and potential equivalent branding) should be considered. In addition, it would be desirable to define an evaluation- and certification process according to eIDAS (at least in high and substantial levels) in order to guarantee a uniform level of assurance.

Ensure Interoperability and Integration Capability

The new eIDAS regulation is intended to enable integration in as many scenarios as possible and support an implementation rule and global device- and browser standards. An X.509 PKI, which is also used with Transport Layer Security, would be possible as a basis for this.

In addition to technical interoperability, legal interoperability is particularly important. This interoperability should be guaranteed across the entire range of EUid applications. In addition to these requirements, besides qualified electronic signature (QES) or qualified electronic seals e.g. qualified server certificates to be checked by a device application or a browser should also be addressed. Goals are uniform standards and legal requirements for the identification of natural and legal persons across all applications.

The acceptance of the guideline by citizens and ID providers all over the European Union and beyond is of crucial importance.

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 actors.

This solution should be interoperable and accessible to any accredited service providers from their back-end(s) via standardised interfaces; security and certifications for service providers need to be developed according to the specific needs of the different hosted services and/or

domains and delivered by competent authorities. Service providers should be able to purchase eID transactions from eID transaction brokers and integrators to simplify service provider integration and contracting.

Standardisation Work in Progress

The GSMA has specified the **Mobile Connect identity framework**, which has already been deployed by several MNOs across Europe. In addition to this, further specification work has been started in February 2020 in a dedicated GSMA working group gathering many key actors like 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" and "high", as well as 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 the secure element in devices. Currently, three such secure elements are available for this purpose: The secure element in the device hardware, the secure element on the SIMcard/ UICC and, relatively newly also, the secure element on the eSIM/eUICC. The task now is to create the legal and regulatory framework for standardised and non-discriminatory use of the secure elements. This is not currently possible as access to the device hardware secure element, already installed in most smartphones in the market, is controlled by the manufacturers. This should be made available by all smartphone manufacturers to the service providers and all citizens, free from 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 coverage. Furthermore, this solution could also be considered to implement the 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 coverage 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 harmonized and adapted to the digital age.

GSMA EUROPE
Regent Park, 1st Floor,
Boulevard du Régent 35,
1000 Brussels, Belgium
Tel: +32 2 891 8700
www.gsma.com/gsmaeurope

October 2020