WHITE PAPER

The role of MNOs in electronic identification within the European eIDAS regulation

This paper explores digital identification, authentication and digital signatures within the framework of the European eIDAS regulation for the electronic identification and trusted services for electronic transactions. We will show that MNOs already possess the key assets to play a fundamental role in this nascent yet highly competitive digital ecosystem.
The context
The growth of the digital economy
The European Commission reports that:

- 72% of EU citizens regularly use the internet
- Half of EU enterprises provide mobile devices for business use
- B2C commerce saw €276.5 million turnover in 2012

More than 150 million eID documents are in circulation today, covering more than 30% of the total European population. The market penetration rate is close to 100% in some countries such as Belgium, and reaching half of the population in large countries such as Germany.

Source: Eurosmart, the future digital identity in Europe, Nov 2015

In recent years, digital identity solutions have become hugely popular across Europe: 21 European member states are now issuing national eID documents, and 20 of them are proposing secure electronic identification, authentication and digital signatures to hundreds of thousands of online service users via computers, tablets, and mobile devices.

This trend for the deployment of digital identity solutions is now ramping up, helped by several initiatives from both the EU and the private sector.

Private sector
A series of major initiatives have been launched by mobile telecom operators – such as the Mobile Connect secure log-in solution, and by web giants – like the Fast Identification Online (FIDO) specifications released in December 2014. Handset manufacturers are also involved in digital identity management, supplying phones with biometrics capabilities such as facial recognition and fingerprint sensors.

European regulation: eIDAS
The eIDAS regulation enables the use of electronic identification (eID) and electronic trust services by citizens, businesses, and public administrations to access online services or manage electronic transactions. It establishes the mutual recognition and acceptance of eID and authentication across borders with a legal status, laying down the groundwork for a single digital market for Europe.

However, businesses and citizens will only fully adopt eID for authentication for online services if they are confident of their legal validity. The eIDAS regulation will:

> Ensure that people and businesses can use their own national eIDs to access private or public services in other EU countries where eIDs are available.

> Create an internal European market for electronic trust services (eTS) delivered by trust service providers (TSPs). There are five trust services, all involving signature-based authentication, and they each cover the creation, verification, and validation of any certificates related to them:

- Electronic signatures, the digital equivalent to a hand written signature
- Electronic seals for proving the provenance and integrity of documents
- Electronic time stamps
- Electronic delivery services for acknowledgement of receipts
- Website authentication

Electronic identification (eID) and electronic trust services (eTS) are key enablers for secure cross-border electronic transactions and for building a single European digital market.

However, eIDAS does not define the technical means to achieve interoperability for eIDs and eTSs. Instead, eIDAS defines the levels of assurance (LOA) for trust service implementation.

1. Enrolment in trust services [remote or local]
   - Application, registration, identity proofing

2. eID credential management
   - Issuance, delivery, storage [in smartphones, secure elements, tokens, etc.]

3. Authentication procedures and protocols inherent to the trust services
The LOA covers the degree of overall security and the robustness of the enrolment, eID credential management, and authentication procedures. There are three levels: Low, substantial, and high, which apply to each of the steps described above.

For instance, qualified signatures for critical authentication can only be achieved if the three steps feature a high LOA. This translates into the physical presence of users with their ID during the enrolment process, the storage and management of eIDs in tamper-proof hardware containers such as secure elements (SEs), which also require Common Criteria (CC) certification, together with their operating system (OS) and their secure applications. Ultimately, this translates into end-to-end secure channels for authentication. Also, the certification scheme removes the need to evaluate security solutions as the same LOAs apply across all countries.

Potential cross-border use cases for MNOs
In this section, we will illustrate some typical cross-border use cases together with their typical LOAs. MNOs can act as eID and Trust Service Provider (TSP) for all types of industries and governments:

- **Education**
  - Students registering online with foreign universities [cross-border eID recognition]

- **Government**
  - Public calls for tender for foreign companies [electronic signature]
  - Website authentication

- **Private companies**
  - Mobile enterprises offering remote access to corporate resources

- **Healthcare**
  - Access to healthcare facilities while travelling, using an eID recognized by other EU states

- **E-commerce**
  - Companies wishing to sign contracts across borders [electronic signature]
  - Opening a bank account using eID while travelling abroad
  - Website authentication for eCommerce

- **Bank**
  - Business operations

Sizing cross-border opportunities in the EU:

- **EU citizens**
  - 14 million EU citizens are resident in another member state

- **SMEs**
  - 21.6 million SMEs in the EU, more than 40% of which do cross-border business

Sources:
1. EC memo of 25 November 2013 on “European Commission Upholds Free Movement of People”
2. Annual report on European SMEs 2013/2014

The eIDAS regulation entered into force on 17 September 2014, providing 500 million European citizens with a clear, legal and stable framework for eID, electronic authentication and the associated trusted services. The rules for trust services (eTS) came into force on 1 July 2016, ensuring that services work across borders and have the same legal status as traditional paper-based processes.
What’s in it for mobile network operators?

MNOs have a unique opportunity as eID and trust service providers. The market is now ready and there are many legitimate players in this digital ecosystem which is now starting to build up. Under the eIDAS regulation, eIDs must be recognized in all European countries by 2018.

There is a wide range of potential eID providers, including certification authorities (CAs), MNOs, banks, Chambers of Commerce, and financial institutions. It is a market full of opportunity and those who seize this opportunity first will no doubt be the market leaders of the future.

MNOs are ideally positioned to act as trust service and eID providers, for companies and governments, leveraging their five field-proven key assets.

MNOs can monetize these new interoperable services, enabling fast and easy cross-border digital solutions, focusing on those requiring high levels of assurance and security:

- **SOMETHING THE MNO DOES**
  - Mobile user enrolment
  - Establishing subscriber IDs

- **SOMETHING THE MNO KNOWS**
  - Customer habits and preferences
  - User segmentation

- **SOMETHING THE MNO OWNS**
  - Powerful cryptographic toolbox (already in the hands of consumers)

- **SOMETHING THE MNO CAN OFFER**
  - ID and authentication solutions for service providers
  - Trust that their subscribers have in them

CONTRIBUTORS

Rémi de Fouchier  
Vice President, Marketing Communications, Gemalto

Julien Baudouin  
Director of Marketing, Gemalto

Didier Benkoël-Adechy  
Marketing Communication Manager, Gemalto

GEMALTO.COM