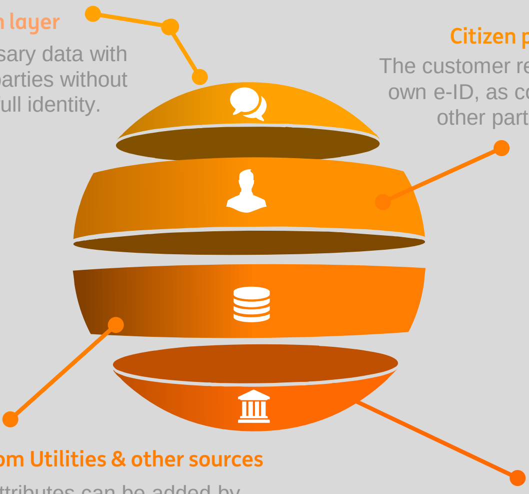
ING Viewpoint

February 2020

Electronic Identification

The Digital Single Market's missing link.



Consumption layer
Share necessary data with commercial parties without exposing its full identity.

Citizen provided consent layer
The customer remains in control of her own e-ID, as consent is necessary for other parties to access this data.

Attributes from Utilities & other sources
Successive attributes can be added by Utility, telco and other companies, who constantly verify & enrich user information, based on explicit consent of the user.

Attributes from government & banks
The fundamental identity attributes are added by government and banks.

> "Electronic identity (e-ID) should function as a passport for the digital world. It can considerably smoothen the customer journey across digital platforms while safeguarding online privacy and security. Moreover it brings efficiency gains for consumers and businesses alike.
>
> In an increasingly digital world, where most customer interaction happens online, a harmonised e-ID framework at the European level would considerably enhance the development of cross-border financial services and improve the customer experience. In that sense, it will be one of the key drivers to achieve a real digital single market."

Aris Bogdaneris
Member Management Board
Banking ING Group

Introduction

Cross-border electronic identity (e-ID) solutions are a missing link in developing the EU digital single market. Safe and efficient identification of remote counterparties is key in an increasingly digital economy, and by integrating the roll-out of both eGovernment and private solutions, synergies can be found. However, e-ID solutions are currently widely fragmented across the EU as operational and regulatory requirements differ per member state. To fully reap the benefits of this promising technology, policy makers should consider developing strong EU-wide e-ID standards, tackle the challenges of biometric data and allow cross-sectoral data sharing in a regulated environment.

The promise of a harmonised EU approach to e-Identity

The development of an EU-wide uniform, open, and secure e-ID standard would support the wider development of the EU digital economy, including eGovernment, and improve its competitive position in the world. Effective e-ID solutions would drastically reduce friction costs by among other things ensuring portability for businesses and individuals alike. Concretely, the EU's regulatory framework should encourage the development of cross-border e-ID solutions that allow European citizens and businesses to identify themselves to their public or private sector counterparties (e.g. tax authorities, e-commerce, banks) in a secure, cost-effective, and user-friendly way. These solutions should also include the possibility of verifying transactions and documents, which are in essence a form of identity check. Aside from convenience, one of the main benefits of e-ID is that it can help the financial sector to better fulfill its role in the fight against financial crime by improving its 'Know Your Customer' processes. The widespread use of e-ID could help diminish identity theft, phishing, money-laundering and fraud, while respecting the EU's strict privacy framework.

How can we get there?

In order to encourage the development of cross-border e-ID solutions, we recommend focusing on three main areas. These areas are also addressed in the recommendations of the EU's High Level Expert Group on e-ID/KYC:

1. **An EU Standard** – There should be a single EU standard for e-ID. To ensure critical mass, e-ID solutions that meet this standard should be accepted anywhere in the EU.
2. **A secure environment** - The cybersecurity and data protection frameworks need to be improved to provide adequate safeguards, particularly for handling biometric data.
3. **Access to data** – In order to build stronger e-ID solutions, certified providers of e-ID solutions should be able to access cross-sectoral data through regulated channels, relying on explicit customer consent.

Key elements of e-ID

- **Unique attributes** - E-ID is a set of unique attributes that represents the proven identity of natural or legal persons.
- **Convenient** – An e-ID solution should be clear and user friendly.
- **Secure** – An e-ID should make use of a secure infrastructure (with strong customer authentication), protected storage and data processing.
- **Reusable/Portability** – An e-ID should be reusable, acknowledged, and valid in all online ecosystems.
- **Trusted providers** – E-IDs should only be provided by trusted third parties that can deliver on security and convenience at the same time.
- **Storage** – E-ID should be centrally enabled but not centrally stored.
- **Empowering** – In line with GDPR, the individual owns its e-ID which means it can only be used based on consent. The individual has the right to keep identity information private and should have access to its identity data at all time.
- **Needs-based Identity**– An identity of needs can help prevent misuse of identities and safeguard privacy, as it allows customers to selectively disclose the identity data that is needed for a certain service or transaction online.
- **Verified data** - To enhance the trustworthiness and accuracy of e-ID an identity should be cross-referenced, and thus be based on multiple verified data sources e.g. ‘your bank’, ‘your municipality’, your utility provider’, etc.

1. An EU Standard

The EU’s 2014 Regulation on electronic identification, authentication and trust services (eIDAS) was a landmark development for e-ID. While eIDAS intended to ensure mutual recognition of e-ID schemes across the EU, a lack of operational standards, especially in the private sector, mean there remains significant barriers to developing cross-border solutions. A key problem is a lack of interoperability across borders. Maximum standardisation of e-ID solutions is therefore crucial. For e-ID solutions to really work, there needs to be certainty that they are secure, convenient, and ideally universally accepted and recognised. For this reason these standards should address data proportionality, data protection, security, authentication and connectivity. It is key that standards enable convenient solutions, but a careful balance between user-friendliness and strong security must be struck.

To facilitate the process of standardisation, EU policy makers could consider empowering a public-private scheme to help develop a set of rules, practices and standards to achieve interoperability for the provision and operation of e-ID. Mandatory acceptance of public/private e-ID solutions should be encouraged to allow for a swift up-take throughout society.

2. A secure environment

Biometric data like fingerprints, iris scan, and facial recognition, is one of the most secure sources to identify an individual. The use of biometrics as a means of verification strengthens security, while decreasing the risk of data breaches. In order to maintain trust in digital identities, clear rules on the handling and storage of biometric data are necessary. The downside of biometric data is that once it is breached, the data is compromised for life. Therefore biometric data deserves special attention when it comes to data storage and protection.

Under GDPR, biometric data is classified as sensitive data for which the collecting and processing is only permitted in limited circumstances. Therefore in our view, biometric data should only be stored by certain trusted parties under strict security requirements**.** We would recommend policy makers to consider developing a clear European regulatory framework to cater for the rising importance of this specific type of personal data.

3. Access to data

To minimise fraud and effectively verify the identity of the customer, identity data needs to be checked and confirmed from multiple sources. To achieve a system of multiple source identity checks, there should be secure communication lines between parties that are able to verify data, including public bodies and non-financial services corporates such as utility providers and online platforms.

The more data points available in an e-ID, the more secure and reliable electronic identification is. An EU-wide framework for allowing cross-sectoral data sharing in a safe and highly regulated environment would improve the effectiveness and reliability of e-ID solutions. This type of data sharing should always be subject to the data subject’s explicit consent and the GDPR’s overarching safeguards.

A domestic e-ID success story: itsme

In Belgium, ING is part of a private sector consortium (Belgian Mobile ID) that developed ‘itsme’, an e-ID app that provides a unique e-ID for individuals. Itsme, was launched in 2017 and is notified under eIDAS with the highest level of assurance and should therefore be accepted by public services in all EU countries. In Belgium itsme is accepted by both public and private institutions. Itsme is currently also being introduced in Luxembourg and will be added to LuxTrust (a qualified trust service provider) as authentication and signature means.

The rapid uptake of itsme shows e-ID has potential, but there are still limitations:

- It is a domestic scheme
- Itsme can only be used by natural persons and not business.

Conclusion

E-ID is a missing link for the EU digital single market as it can provide both natural and legal persons with a secure passport to the digital world. In order to optimize the current EU e-ID framework policymakers should consider developing EU-wide e-ID standards linked to the mandatory acceptance of eIDAS based e-ID solutions, creating a framework for the handling of biometric data, and by regulating cross-sectoral data sharing.