

Mobile Connect for Cross-Border Digital Services

Lessons Learned from the eIDAS Pilot





Contents

FOREWORD	2
EXECUTIVE SUMMARY	4
1. INTRODUCTION: eIDAS AND MOBILE CONNECT	12
1.1 BACKGROUND: CROSS-BORDER INTEROPERABILITY OF NATIONAL eID	13
1.2 THE NOTIFICATION PROCESS	14
1.3 eIDAS-RELATED OPPORTUNITIES	15
2. AN OVERVIEW OF THE PILOT	20
2.1 MOBILE CONNECT AND THE eIDAS PILOT - PHASE I	21
2.2 MOBILE CONNECT AND THE eIDAS PILOT - PHASE II	22
3. ANALYSIS AND KEY FINDINGS FROM THE PILOT	26
3.1 TERMINOLOGY AND ARCHITECTURE DESIGN FOR TECHNICAL INTEGRATION	27
3.2 FINDINGS AND RECOMMENDATIONS REGARDING TECHNICAL INTEGRATION	31
3.3 DATA FLOW AND MINIMUM IDENTITY ATTRIBUTES	37
3.4 THE USE CASE AND USER JOURNEY	39
3.5 AUTHENTICATORS AND LEVEL OF ASSURANCE	42
4. BUSINESS MODELS: HIGH LEVEL CONSIDERATIONS	44
5. PILOTED COUNTRIES	46
5.1 FRANCE	47
5.2 NORWAY	51
5.3 SWEDEN	55
5.4 FINLAND	57
5.5 ESTONIA	59
6. CONCLUSIONS	62
ANNEX: HIGH LEVEL GUIDANCE FOR eIDAS NOTIFICATION	64
NOTIFICATION SYSTEM FOR IDENTIFICATION PROVIDERS	65
CASE STUDY: NATIONAL REQUIREMENTS FOR NOTIFICATION IN FINLAND	65
CONTRIBUTORS TO THE PILOT	68

Foreword

**Andrus Ansip**

Vice-President of the European Commission

“Building trust in the online world is crucial to accomplish the Digital Single Market. Coupling mobile authentication credentials, such as Mobile Connect, with the identity security provided by eIDs under the eIDAS Regulation, is the way towards this goal. This is a huge opportunity for European citizens and businesses: they will be fully empowered and benefit from the untapped potential of mobile, secure and accountable access to public and commercial services without frontiers. It also sets the starting point for extending, with the help of mobile operators, the use of trusted eIDs globally. Our ambition is widespread use of eIDAS services, helping people in their everyday lives, by allowing them to identify and authenticate themselves online in a secure, convenient and responsible way.”

**Mariya Gabriel**

European Commissioner for Digital Economy and Society, European Commission

“The cross border use of trusted eID under eIDAS gives EU citizens a new freedom: to rely on the eID they already use at national level to securely access digital public and private sector services provided everywhere across the EU. By giving citizens control of the personal data and attributes they want to disclose, this freedom also benefits online service providers who can now be sure about the identity credentials of their counterparts in digital interactions. This interoperability pilot between Mobile Connect and eIDAS shows how more and more digital interactions can take place through mobile devices. Mobile operators can partner with governments to provide trustworthy identification solutions, capable of meeting high security standards and that are easy to use. Partnering together on mobile trusted eID is key for Europe to be successful in seizing the full potential of the Digital Single Market and to securely and responsibly empower citizens and businesses in realising their ambitions in the digital world.”

**John Giusti**

Chief Regulatory Officer, GSMA

“Interoperability of digital identities across Europe represents a tremendous opportunity to bring cross-border e-government and e-business to European citizens. It will also help drive the development and commercial deployment of convenient and secure identification and authentication solutions, such as Mobile Connect. GSMA Intelligence estimates the eIDAS Regulation, adopted in 2015, will create an addressable market for authentication, authorisation and attribute services of more than \$2.47 billion by 2022. In the pilot highlighted in this report, mobile network operators demonstrated the value of working together with Member States and the European Commission to integrate Mobile Connect into the interoperability framework, defined by the eIDAS Regulation. This should help to accelerate the cross-border uptake of electronic identification by both the public and private sectors. The GSMA will continue to work with industry and government to deliver the benefits of digital identity solutions to citizens across Europe.”

**Stéphane Richard**

Chief Executive and Chairman, Orange

“As identity goes digital, it’s also increasingly going mobile. This trend is especially pronounced in Europe, where 53% of all digital transactions are conducted using a mobile handsets. As one of the pioneer operators launching Mobile Connect alongside the GSMA and other leading mobile operators worldwide, Orange is making mobile phones the key to electronic identification and authentication enabling Mobile Connect for any service and any device. 2017 was pivotal year for Orange, and I am proud that Mobile Connect is now helping the French government in its digital transformation. We are making Mobile Connect available for government services to every citizen connected on the France Connect portal. This live service will help spread digital identities in the context of eIDAS, with the aim to create a Digital Single Market that simplifies access to public administration, improves user convenience and makes the trust and authentication services market more transparent and accountable, while preserving citizens’ privacy.”

**Bjørn Ivar Moen**

Chief Marketing Officer, Telenor Norway

“Norway is a leader in the development and adoption of electronic Mobile ID systems. Today, over a quarter of Norway’s adult population uses Mobile BankID at least 15 times a month, underlining its key role in the country’s digital economy. The strong uptake is due to its ease-of-use combined with robust security available across a wide range of online services; Mobile BankID is readily available on any mobile device and is interoperable between Norway’s network operators. Telenor sees benefits in applying these principles on a supranational scale, whereby European operators offer their customers Mobile Connect to gain access to key services, irrespective of their country of origin.”



Executive summary

Consumers, regulators and companies all recognise that robust digital identity services are required to enable safe, easy and efficient online interactions.

By assuring the identity of parties engaged in an online relationship or transaction, digital identity services can reduce the uncertainty inherent in remote transactions, thus fostering trust and helping to reduce fraud, while preserving individuals' privacy. In Europe, the implementation of the EU Regulation on electronic Identification, Authentication and Trust Services (eIDAS) and the mandatory recognition of notified electronic identity (eID) systems by all Member States as of September 2018, is set to facilitate the roll out of electronic identification solutions for public sector online transactions. With 84% of mobile penetration in Europe, the use of mobile identity services for eIDAS will drive usage and support further adoption across many sectors of the digital economy, from banking, corporate services and domestic utilities. Designed to enable citizens to carry out secure cross-border electronic transactions, such as university enrolment, bank account opening, filing tax returns and authorising access to electronic medical records, the eIDAS Regulation will create an addressable market for authentication, authorisation and attribute services of more than \$2.47 billion in 2022, according to GSMA Intelligence.

Mobile Connect is a multi-purpose identity solution that uses the inherent trust, security and ubiquity of mobile networks.

Mobile Connect was launched in 2014 by the GSMA and many of the world's leading mobile operators. When a consumer logs into a service using Mobile Connect, they receive a message on their mobile device asking them to either confirm the action, or input a PIN or a biometric, such as a fingerprint, in the case of more sensitive applications. To date, Mobile Connect is supported by more than 60 mobile operators and in over 30 countries worldwide and is available to more than three billion people. Designed to meet the technical and regulatory requirements of eIDAS, Mobile Connect enabled an eIDAS-compliant pilot in late 2015, making it the first private-sector cross-border public service authentication solution compatible with eIDAS. Building on this success, Mobile Connect was employed in a second phase of the pilot lasting 12 months.

There is great value in combining cross-border eIDAS recognition with the convenience and security of Mobile Connect for users and online transactions.

The second phase of the pilot was a collaboration between several public and private sector organisations seeking to accelerate the uptake of trusted and secure digital authentication in response to the eIDAS Regulation and its implementing acts.

The GSMA managed the delivery and execution of the project in collaboration with:

- Orange, providing Mobile Connect in France
- AriadNEXT, a technology partner, providing remote identification built on top of Mobile Connect in France
- Telenor, providing Mobile Connect in Norway
- Clayster, a technology partner, providing a digital entitlement management platform for the Internet of Things
- France Connect, as the National eID system authority and single point of contact for the eIDAS Node in France
- The Norwegian Agency for Public Management and e-Government (Difi), as the National eID system authority and single point of contact for the eIDAS Node in Norway
- The Swedish e-Identification Board, as the National eID system authority and single point of contact for the eIDAS Node in Sweden

The European Commission services of DG CONNECT and DG DIGIT also supported the pilot by providing guidance on the architecture interoperability requirements and other regulatory issues.

The pilot demonstrates the value of interoperability achieved through collaboration between private sector players and Member States. Supported by the Connecting Europe Facility (CEF) eID building block, the eIDAS infrastructure, together with the deployment of reliable mobile identity services, will be able to manage the complexities and the opportunities arising in the EU Digital Single Market.

Focusing on the delivery of healthcare services enabled by the Internet of Things, the completion of the pilot is an important step towards developing a strategic action plan to employ mobile operators' assets to accelerate the development of a secure and trustworthy digital identity ecosystem.

The broader goal of the GSMA and its members is to drive adoption of Mobile Connect for trusted digital identities both within the EU and internationally. The pilot highlighted how leveraging Mobile Connect and the eIDAS Regulation, together with European Member States' investment plans for identity initiatives, could drive large-scale take-up of secure and reliable digital identity management solutions beyond username/password and smartcard-based approaches. This will:

- benefit citizens and businesses, increasing digital inclusion and drive economic growth;
- enable the widespread use of multi-factor-based identity management solutions, through the flexibility of Mobile Connect to use and combine different authentication factors and meet different eIDAS requirements at different level of assurance;
- enable efficient and secure customer authentication and remote identity verification by integrating mobile operator solutions into national and cross border eID systems, through the interoperable and decentralised federation layer offered via Mobile Connect and the API Exchange for the discovery service;
- deliver a user and device-centric approach to identity for Internet of Things applications;
- increase confidence in Mobile Connect, opening up commercial opportunities in other regulated sectors.

The execution of a successful rollout of Mobile Connect and eIDAS will depend on collaboration among key players, particularly governments and mobile operators.

To that end, the GSMA makes the following recommendations to Member States in Europe:

- i. Pursue greater cooperation with the private sector, in particular, to enable private sector identity and authentication providers to use the eIDAS infrastructure, thereby contributing to the emergence of an increased number of notified eID schemes with private sector stakeholders.
- ii. Consult with industry on the chosen eIDAS architecture, as its selection has important implications for the technical infrastructure deployed by private sector identity and authentication providers.
- iii. Publish guidance to help companies to comply with each eIDAS Node's specifications, including identity and authentication providers' service level specifications and service providers' on-boarding process.
- iv. Standardisation of the interface exposed by the eIDAS Connector Nodes to the service providers via the OpenID Connect framework.
- v. Collaborate with the industry on the standardisation of domain specific attributes to be shared across borders, including mapping of domain specific identifiers, on top of the identity layer established by the eIDAS minimum identity attributes.



The GSMA also makes the following recommendations for mobile operators and private sector service providers:

- i. Promote Mobile Connect as a key enabler to deliver secure identification and authentication in different sectors (e.g. banking, utilities) and as a valuable solution for their service providers, so that the increased demand can drive governments to adopt it.
- ii. Foster and encourage the synergies between the government-verified identities (which can provide a high level of trust in the identification) and Mobile Connect (which can provide a high level of trust and convenience in the authentication). One approach has been implemented in France with Mobile Connect, which combines a SIM based two-factor authentication with a secure KYC mobile application process for identity verification based on government issued credentials. Mobile Connect in France provides secure and convenient access to both public and private sector services.
- iii. The business model behind eIDAS requires further attention. Stakeholders should be consulted about a potential single contractual and commercial model, similar to the technical federation. There is potentially great value in bringing a commercial model that works and allows for scale for all parties in the technical federation. One possible commercial solution could emerge from the ongoing work by the GSMA and several EU mobile operators in forming a commercial federation service called Mobile Connect Link (MC Link).

- iv. Online service providers need to make the mobile industry and governments aware of their needs and expectations about eID.

Ready and able to support cross-border identification and authentication, Mobile Connect could play a central role in bringing about the EU's vision of a Digital Single Market. Through the CEF Programme, the European Commission is making funding available to help mobile operators and other private sector organisations to integrate their services into eIDAS Nodes. Mobile operators and other companies can learn more here <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom>



“Trust is the most basic, and yet most fundamental, of building blocks of business and the combination of trusted cross-border digital services and the convenience of end user authentication is key to a successful digital economy.”

Simon Wood, Ubisecure CEO

“We are honoured to participate in a project that we believe is of the greatest importance for the future of digitalisation and our Internet. Without trusted digital identities, the transition into the digital world will be halted. With a robust eID infrastructure in place, we enable people to claim digital ownership of what they previously could only own physically. In order to control who and when someone has the right to access our IoT device’s data, a hard-digital identity is essential. By securing our integrity while connected, trusted digital identities can be attained – allowing for an exponential growth of new services and applications. But this is only possible if we direct the consent decisions towards the rightful owner, rather than third-party delegated owners acting on our behalf. This is what we call the Human-Centric Internet.”

Rickard Strid, Clayster CEO

“eIDAS is a big leap forward in EU digital single market – and a global benchmark outside of EU. But to really drive volume, private sector use cases require further work on business models and public / private cooperation.”

Janne Jutila, MD, Internos Partners

“Digital identification is essential for the development of our economies and modern democracies. The eIDAS Regulation states nothing else.

In just a few years, mobile phones have become indispensable to our existence. They are already being used to pay, it is natural that they are being used to identify us. Mobile Connect brings authentication, a key element of digital identity. By combining an innovative recruitment method, we have given France Connect, the French digital identity hub, the trusted identity it needs for everyone.

We were thrilled to participate in this pilot. Seeing a French citizen connect to a Swedish service using Mobile Connect et moi has been an experience that we want to become a habit for all European citizens.”

Marc NORLAIN, CEO and cofounder AriadNext



Glossary of terms

Digital Identity	<p>The terminology used throughout this document to refer to the combination of self-declarations and third-party assertions about an individual. Digital identities can be anonymous, self-asserted or verified and the degree of verification can be tailored to match the level of liability associated with the intended use.</p> <p>It is best practice that a verified digital identity is based upon a minimum set of unique identity attributes, which may include a unique identifier defined by the state.</p>
Mobile Identity	An extension of digital identity provided via mobile networks and devices
Mobile Connect (MC)	<p>Mobile Connect is a global open and common framework developed by the GSMA in cooperation with leading mobile operators. Through a single consistent interface, Mobile Connect supports authentication, authorisation, identity and attribute sharing or verification for service providers, and puts the user in control of their data.</p>
eIDAS Regulation (eIDAS)	EU Regulation No 910/2014 on electronic Identification, Authentication and Trust Services (eIDAS) for electronic transactions within the EU

eIDAS Terms (Ref: eIDAS Interoperability Architecture v1.00)

Member State (MS)	State covered by the eIDAS Regulation, i.e. a Member State of the European Union and/or the European Economic Area
Sending MS	The MS whose eID scheme is used in the authentication process, and sending authenticated ID data to the receiving MS
Receiving MS	The MS where the relying party requesting an authentication of a person is established
eIDAS Node	An operational entity involved in cross-border authentication of persons. A Node can have different roles: eIDAS Proxy Node or eIDAS Connector Node
eIDAS Node single point of contact (SPOC)	Member States single point of contact to help service and identity providers connect to the eIDAS Network.
eIDAS Connector Node	eIDAS-Node requesting a cross-border authentication
eIDAS Proxy Node	eIDAS-Service operated by the Sending MS and providing personal identification data
eIDAS middleware Service	eIDAS-Service running middleware provided by the Sending MS, operated by the Receiving MS and providing personal identification data
Middleware	Software provided by a MS notifying a middleware-based scheme which is used by the Receiving MS to operate eIDAS-middleware-services

Mobile Connect Terms (GSMA)

OpenID Connect	The standard protocol for identity services, including authentication and identity data exchange from the OpenID Foundation.
Mobile Connect API Exchange Discovery Service	The service that discovers the Mobile Connect provider (a mobile operator) and provides the technical information needed to make the Mobile Connect call to the discovered Mobile Connect provider (e.g. API endpoints, API credentials).
Identity Gateway	The component owned by the Mobile Connect provider, which exposes the OpenID Connect protocol and manages the secure authentication of the user
Authentication	<p>Authentication is the act of providing assurance that the individual presenting the electronic credentials matches the identity such credentials represent as authorised by a trusted entity. It is therefore a process of establishing confidence in user identities presented online to a service or resource.</p> <p>Digital identity answers the question ‘who are you?’, whilst digital authentication verifies that ‘you are who you claim to be’, based on one or more identity credentials (Something I Am, Something I Know, Something I have, Something I do).</p>
Credentials	<p>The means with which the user is able to authenticate themselves and lay claim to an identifier. Can take the form of a secret (username/password or PIN = something I know), a physical hardware token (something I have), a biometric template (something I am) etc.</p> <p>Essentially, a credential is bound to the identity to enable it to be asserted through presentation of the credential (authentication); in the digital space, the possessor of the credential is understood to be the identity owner.</p>
Authenticator	The mechanism used in the mobile device to challenge the user to authenticate and capture the response from the user. Mobile Connect uses the principle of “Pluggable Authenticators”, so that different authenticators can be plugged into the Mobile Connect system – based on the policy, needs and availability at the mobile operators and relying parties. Some of the popular authenticators used in mobile include: SIM Applet; Authenticator Network Initiated; USSD Authenticator; SMS+URL based Authenticator; Smartphone App Authenticator with network binding
Service provider (or relying parties)	The organisation (a public or private sector entity) that requires proof of identity and/or authentication of an individual in order to grant access to a service or resource. Service providers may themselves be digital ID and authentication providers, or they may outsource these functions.

1

Introduction: eIDAS and Mobile Connect



1.1 Background: Cross-border interoperability of national eID

Allowing citizens to access online services by reusing their nationally-issued eID is a key priority of the European Commission's Digital Single Market strategy. The eIDAS Regulation adopted in 2015 provides the legal framework, introducing the principle of mutual recognition of national eID schemes (including smartcards, mobile identity and BankID), ensuring interoperability and a high level of security and authentication assurance. As of 29 September 2018, all online public services requiring electronic identification assurance corresponding to a level of 'substantial' or 'high' must be able to accept the notified eID schemes of other EU countries. The technical infrastructure that connects the national eID schemes is called the eIDAS network (throughout the report also referred to as eIDAS infrastructure), and is composed of national eIDAS interoperability Nodes (eIDAS Nodes).

The eIDAS Regulation is designed to enable citizens to carry out secure cross-border electronic transactions, such as enrolment in a foreign university, filing of multiple tax returns, access to electronic medical records or authorising a doctor to access an individual's records. It also enables citizens relocating to another Member State to manage registration and other administration online with the same legal certainty as they have with traditional paper-based processes. In other words, whether you are a company or a citizen trying to complete an electronic transaction in another EU country, the eIDAS Regulation will ensure you can use your national eID to access public services in other EU countries where eIDs are required for such access at a national level. It also creates a EU-wide internal market for electronic trust services by providing legal certainty on the legal validity of trust services, namely for electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication.

A key objective of the Regulation is to reduce fragmentation, ensuring consistency of implementations across Europe. It is also designed to encourage the use of the eIDAS infrastructure for private sector services by defining a "legal toolbox" for market players, which includes, for example, reference guidance on key issues such as:

- Legal and technical interoperability requirements across different EU Member States' eIDAS Nodes (EC Implementation Regulation 2015/1501).
- Minimum technical specifications, standards and procedures to map level of assurance requirements of notified electronic identification schemes (EC Implementation Regulation 2015/1502).
- Person identification data and requirements on a minimum set of identity attributes available from notified electronic identification schemes and for which each Member State is liable.

1.2 The notification process

Under the eIDAS Regulation, Member States need to complete a notification process for their eID schemes to ensure the scheme is recognised by other Member States. At least six months prior to notification, the notifying Member State must provide a description of that eID scheme, as well as details of the responsible parties involved, to the Commission and the other Member States (pre-notification).

In February 2017, Germany became the first EU country to pre-notify the European Commission of the online ID function of its national identity card and electronic residence permit. In August 2017 notification was completed. As of December 2017, Italy

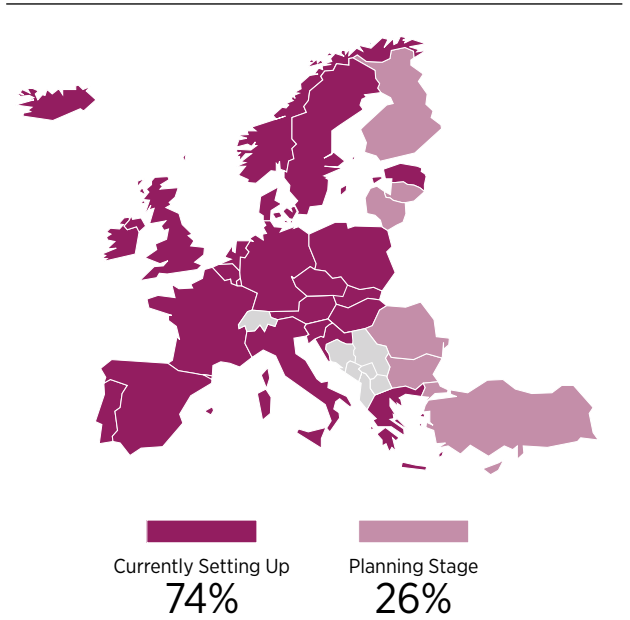
had also pre-notified SPID (Sistema Pubblico per la gestione dell'Identità Digitale)¹, its private sector-led electronic identification (eID) scheme, to the European Commission.

Five more countries are about to pre-notify their schemes, with others expected to follow. About 74% of EU countries are currently setting up and deploying an eIDAS Node, and 90% of the countries already have a national eID scheme issued, as described in figure 1. By September 2018, all the Member States should have a Node ready for eIDAS. A high level description of the eIDAS notification system is described in the annex to this report.

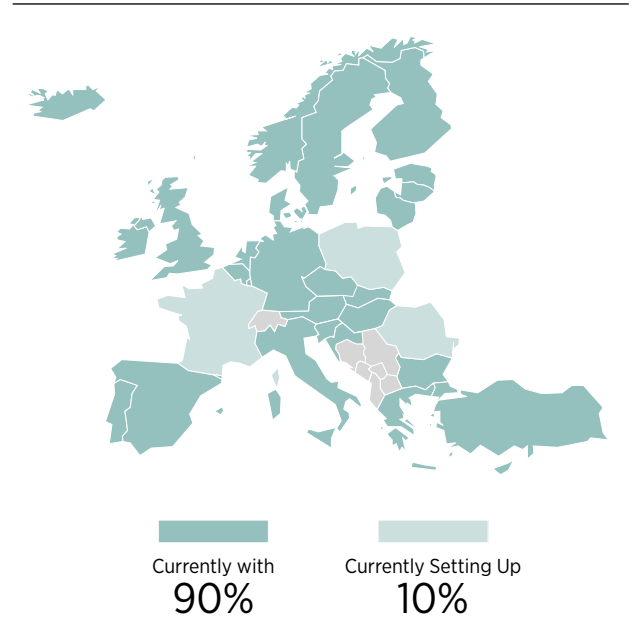
Figure 1

eIDAS-Node implementation plan

EU MS and associated countries implementing an eIDAS-Node



EU MS and associated countries with nationally-issued eID schemes



Please note that these maps reflect information published on the CEF Digital country page, based on the information publicly available (e.g. INEA grants, governmental web sites) and updates provided by the Member States experts of the Cooperation Network.

Source: European Commission analysis in 2017

1. <https://www.spid.gov.it/>

1.3 eIDAS-related opportunities

The eIDAS Regulation can benefit industries that need security, reliable identification, strong authentication and legal certainty (e.g. finance, banking, transport, insurance, health, sharing economy and trading). Rather than having to verify their identity in person, an entity can rely on an appropriate eID notified by a Member State to grant online access to their services. By providing greater legal certainty and making it easier to gain economies of scale, the Regulation will also bolster the digital identity ecosystem in general and mobile operators' solutions, in particular.

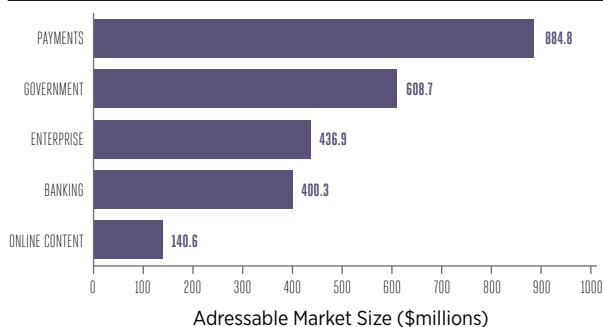
According to a recent study by GSMA Intelligence, eIDAS will create an addressable market for authentication, authorisation and attribute services of more than \$2.47 billion in 2022, accounting for direct revenues from government agencies and from the private sector (see Figure 2). The largest portion of this revenue is attributed to private sector use cases generated by the application of authentication, authorisation, and identity and attributes services in the banking, payments, enterprise and online content sectors.

Figure 2

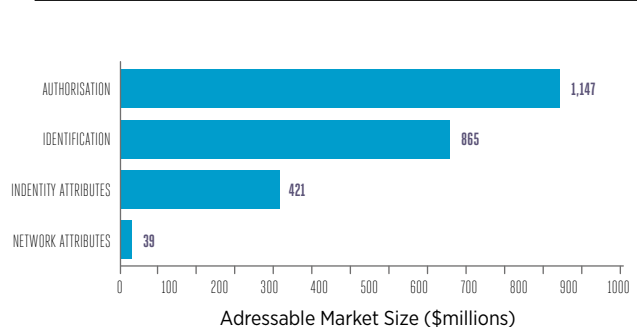
Addressable market for eIDAS in 2022



MARKET SIZE BY SECTOR (\$millions)



MARKET SIZE BY SERVICE TYPE (\$millions)



Direct market size sectors:
Government

- E-govt:** login, identification, digital signature
- Tax return:** filing, payment, authorisation
- National ID:** KYC, application, voting, age verification
- Govt services:** healthcare, education, welfare aid
- University:** application, financial aid, log-ins

Indirect market size sectors:
Payments, Banking, Enterprise, Online Content

- Login:** KYC verification & provision (registration), strong authentication
- Digital signature:** contract, tender, annual reports
- Payments:** 3D secure (authorisation), payee setup, age verification, expense approval
- Service applications:** new bank accounts, insurance cover, background checks
- Corporate login:** (VPN)

Source: GSMAi analysis February 2017

As noted by a study commissioned by the European Commission on a marketing plan to stimulate the take-up of eID and trust services in 2017, the involvement of the private sector will enable a broad number of eID-enabled applications to emerge, thus creating more frequent usage. Member States, in cooperation with the European Commission, could further lower the barriers experienced by the private sector, notably with respect to building business cases.²

The role of private sector is also highlighted in the eIDAS Regulation, see, for example, Recital 17 where states: *“Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means.”* Recital 17 and Article 7(f) also make it clear that Member States can set conditions (for example, a charge) for private sector re-use of authentication capabilities. The Regulation also includes provisions on liability for notifying Member States, which private sector service providers could consider as they begin to rely upon digital identities under notified schemes. However, it does not address some of the other key questions, such as the question of commercial models - it makes identification and authentication free to a service online provided by a public sector body, but leaves it to Member States to decide how the commercial model for private sector applications will work in practice.

At a national level, in many countries, the private sector and the mobile industry is already involved: Member States are electronically identifying and authenticating their citizens by leveraging mobile solutions offered in the market place. According to the eIDAS trust framework, such private sector solutions could also be recognised by national legislation and notified to the European Commission as per the eIDAS notification requirements.

However, in order to make mobile a truly scalable solution for digital identity-enabled use cases there is a need of greater collaboration between governments and private sector players. For example, some changes in the law may be required to enable full use of private sector-led solutions. Amongst the European Union, few countries such as Finland have a law covering eID (Act on Strong Electronic Identification and Electronic Signatures) as a legal basis for eID. In other countries, the practice is to use e-signature legislation.

More broadly, the eIDAS Regulation needs to be implemented with greater urgency to support the development of Europe’s Single Digital Market. Although all Member States have stated an intention to notify an eID scheme, more governments need to make a strategic decision to give their residents access to services in other countries and vice versa. To be successful, eIDAS needs to be consistently implemented throughout Europe.



Trust is the most basic, and yet most fundamental, of building blocks of business and the combination of trusted cross-border digital services and the convenience of end user authentication is key to a successful digital economy.

Simon Wood, Ubisecure CEO



² Source: PWC Study 2017

1.4 Impact of eIDAS on mobile operators: authentication and identification via Mobile Connect

By leveraging eIDAS, mobile operators have an opportunity to become the trusted providers of digital identity and authentication in Europe. As the Regulation will accelerate the implementation of national digital identity strategies, eIDAS helps to open up a wide range of opportunities for mobile operators. For example, mobile operators could potentially earn new revenues from the provision of trust services encompassing the creation, verification, and validation of mobile signatures and related services.

The mobile industry's contribution to identity is about reach and security. Mobile operators have the capabilities, the experience and the track record to provide fast and

secure authentication. For more than three decades, mobile operators have been authenticating consumers' devices on their networks, securely providing voice calls, messaging, internet access and other services, while safeguarding consumers' privacy and personal data.

Together, the GSMA and mobile operators are building on the security of their networks with Mobile Connect, a consistent service framework for identity provided by the operator community to service providers. For users, Mobile Connect provides simple, secure and convenient access to online services via a multi-factor baseline solution for authentication, authorisation and attribute sharing. More information on Mobile Connect is in Box 1.

Box 1

About Mobile Connect

Mobile Connect is a global open and common framework developed by the GSMA in cooperation with leading mobile operators. Through a single consistent interface, Mobile Connect supports authentication, authorisation, identity and attribute sharing or verification for service providers, whilst putting the user in control of their data. For end users, it combines the user's unique mobile number, and an optional PIN and/or other authentication factors for added security, to verify and authenticate the user. The combination of mobile device, mobile network and operator business process security features enables secure and user-friendly services for a wide range of online use cases, including e-government services, e-commerce, e-Health, electronic payments and many others.

Mobile Connect's key benefits:

- **Easy to use, as it employs the mobile phone for authentication (i.e. no passwords)**
- **Secure strong customer authentication (no passwords to steal, improved user experience, less friction)**
- **Adds security and trust into digital transactions (e.g. by confirming location, user identity, usage)**
- **Protects privacy (operator confirms credentials, user gives consent for sharing)**
- **Simple and cost effective to deploy**

To date, Mobile Connect is supported by 60 mobile operators and in over 30 countries worldwide and available to more than 3 billion people.

In summary, Mobile Connect enables governments and other service providers to provide citizens with an authentication experience on a par with best practice in the private sector, while using mobile technology to leap frog legacy infrastructure and economic barriers to delivering secure digital identity programmes. For governmental organisations worldwide, Mobile Connect can deliver flexibility, real-time access to information, assured interaction with citizens and multi-function digital identity, while reaching the required levels of security for robust mobile identity issuance and authentication.

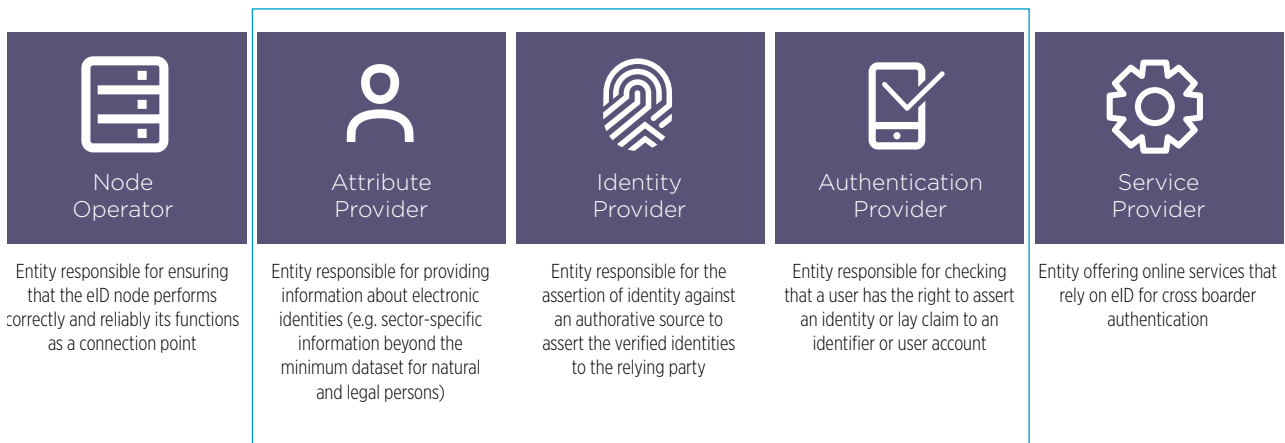
General information on Mobile Connect: <https://mobileconnect.io/operators/>



Mobile Connect operators can play three distinct roles in the eIDAS ecosystem (see figure 3):

Figure 3

Mobile Operators role in the eIDAS ecosystem

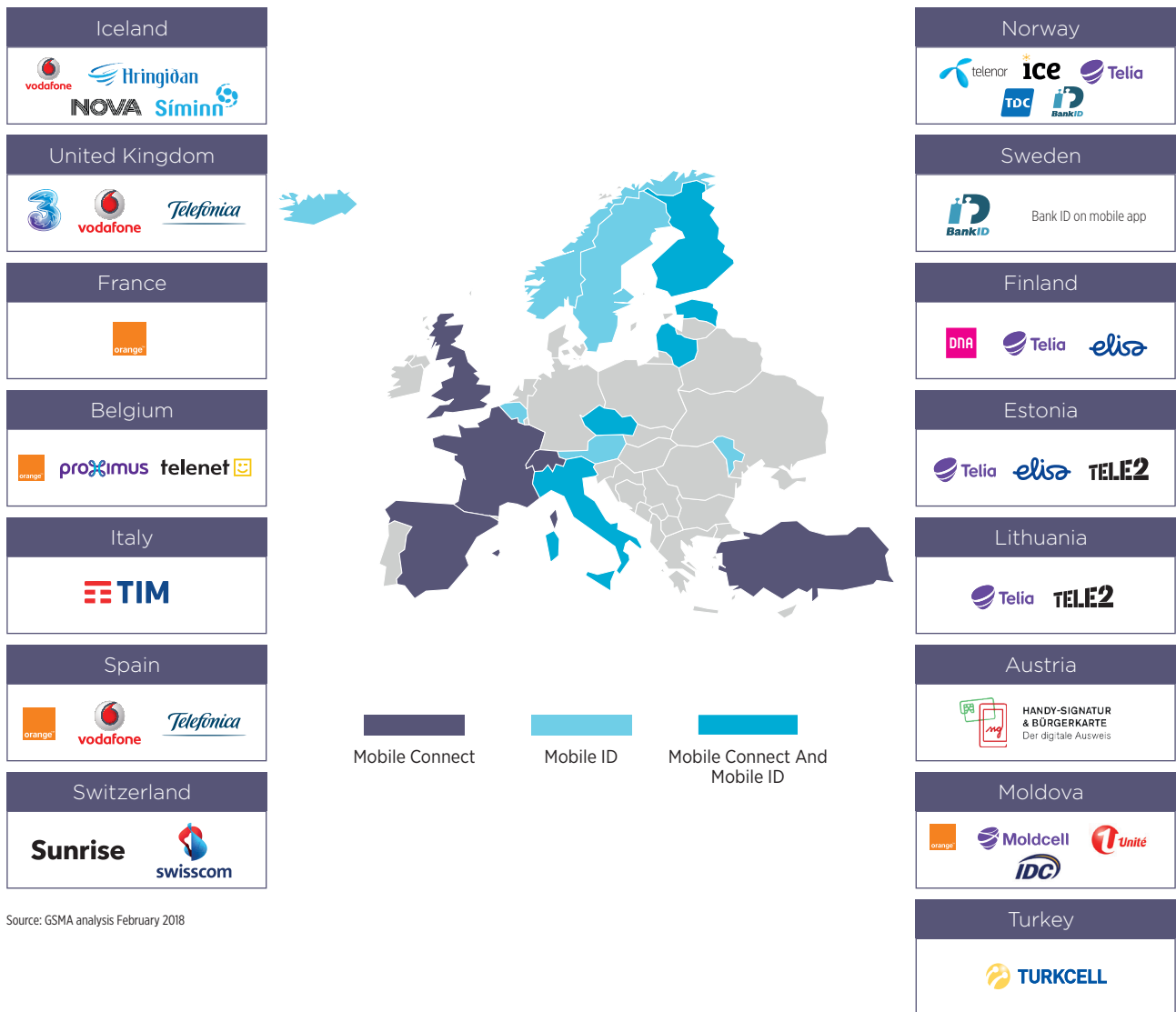


MOBILE OPERATORS ROLES IN THE eIDAS ECOSYSTEM

Figure 4 illustrates existing mobile identity and Mobile Connect deployments in Europe highlighting how mobile identity solutions are emerging rapidly throughout Europe.

Figure 4

Mobile Connect and Mobile Identity availability in Europe



Source: GSMA analysis February 2018

2

An Overview of the Pilot

2.1 Mobile Connect and the eIDAS pilot: Phase I

In November 2015, the GSMA, mobile operators and government agencies launched a pilot to demonstrate how Mobile Connect can be used to identify a citizen of one EU Member State in order to gain access to a public service of another. Spanning Catalonia in Spain and Finland, phase I of the pilot established a proof-of-concept for cross-border authentication to e-government services, in line with the technical requirements of the eIDAS Regulation. This first proof of concept established Mobile Connect as the first private-sector cross-border service authentication solution prepared to meet the technical and regulatory requirements of eIDAS.

The pilot enabled customers of participating Spanish operators to login to Finnish e-government services and vice versa. The login through an identity hub granted access to a complete public services portfolio. After the customer clicked on the Mobile Connect button and entered their mobile number on the discovery page, a PIN request appeared on their mobile phone. By

entering the correct PIN, the user was authenticated and then the identity attributes were shared to verify the individual logging into the online service.

The two-month pilot was a collaboration between organisations seeking to accelerate the uptake of trusted and secure digital authentication in response to the eIDAS Regulation. The GSMA and major operators, Orange Spain, Telefónica, Telia Company, and Vodafone Spain, supported the trial, together with technology company Gemalto, Mobile World Capital, the Catalonia Regional Government, the Finnish Ministry of Finance and Finnish Population Registration Centre.

Phase I provided a good understanding of the Mobile Connect architecture options (see Figure 5) that are compatible with government and eIDAS requirements. It also highlighted the key issues that should determine the choice of option, demonstrating the flexibility of Mobile Connect to meet government requirements across the EU.

Figure 5

Mobile Connect and eIDAS architecture Options



The first two models are based on the so-called middleware model, while the third model is based on a “pan-European proxy-service model”. The flexibility of Mobile Connect ensures that mobile operators can meet both the middleware and eIDAS reference architecture models implemented within eIDAS by Member States.

For the middleware approach, the middleware was tested in the pilot as a virtual machine in the receiving Member State. The middleware model is being used by Germany and Austria, which has a four-year old national eID system that supports several smart cards and mobile eID.³

3. The middleware virtual machine must expose the same SAML interface towards the “connector” of the Receiving Member State. The “southbound” interface to the middleware virtual machine is dependent on the implementation. For Mobile Connect – the middleware can be provided as a virtual machine which connects to the Mobile Connect infrastructure at the southbound.

2.2 Mobile Connect and the eIDAS pilot: Phase II

Phase II of the pilot built on the lessons learned from the proof of concept delivered in phase I to demonstrate the scalability of Mobile Connect as a Europe-wide solution for eIDAS. Employing the requirements for a commercially-viable, government-backed solution, it demonstrated how Mobile Connect can also support the deployment of private sector use cases and help deliver a sustainable eIDAS system throughout Europe.

In particular, phase II of the pilot was designed to:

- Improve knowledge and best practices about Mobile Connect as a compliant solution with eIDAS regulatory and technical requirements.
- Trigger a commercial launch for the proposed use case.
- Contribute to the EU Digital Single Market by advocating for the notifications under eIDAS of eID schemes based on mobile identity solutions.

The 12-month pilot was a public and private sector collaboration between several organisations seeking to accelerate the uptake of trusted and secure digital authentication in response to the eIDAS Regulation and its implementation acts.

The pilot employed the Mobile Connect authentication process and validation of the citizen's digital identity, across Member States, via the eIDAS framework. The pilot used the available connectivity in a test environment between eIDAS Node operators in France, Norway and Sweden to demonstrate how these Node operators could easily and securely integrate into Mobile Connect to delegate both authentication and identification services. Through the implementation of healthcare services and Internet of Things technologies provided by an innovator company in this field, the pilot showcased how service providers can use eIDAS and Mobile Connect as a trustworthy environment to unlock some of these new applications services in the Digital Single Market.

Pilot participants

The GSMA managed the delivery and execution of the project in a public and private sector multi-stakeholder collaboration with National eID Node authorities, mobile operators, private online services for observers and advisors (see Figure 6 on pilot participants).

Figure 6

Mobile Connect and eIDAS pilot participants



A National eID system authorities and eIDAS Node single point of contact

The pilot involved 3 national eID systems authorities and eIDAS Node single point of contact from France, Norway, and Sweden:

- France Connect providing access to their eIDAS Proxy Node in its test environment;
- the Norwegian Agency for Public Management and e-Government (Difi) providing access to their eIDAS Proxy in its test environment;
- the Swedish e-Identification Board, eIDAS Connector Node providing access to its eIDAS Connector in their test environment for both France and Norway.

B Mobile Connect operators

Two mobile operators participated in the pilot providing Mobile Connect authentication process and validation of the citizen's digital identity. The operators included were:

- Orange France, in partnership with AriadNEXT, a technology partner, providing remote identification built on top of Mobile Connect in France, and
- Telenor Norway.

The mobile operators have worked with the French and Norwegian eIDAS Node authorities to integrate Mobile Connect as an eID authentication solution to the national ID portals in France and in Norway. The operators also provided SIM cards to test the use case, and user-flow.

C. Online private services

The pilot partnered with a private online service based in Sweden to demonstrate a cross-border use case. This private online service, called Clayster⁴, is a digital entitlement management platform for the Internet of Things.

D. Observers and advisors

Telia Company and the Finnish Population Register Centre (PRC) were also key contributors to workshops and meetings hosted throughout the pilot, but could not complete its technical implementation as the necessary eIDAS Nodes won't be available until later this year and will only support requests for public sector use cases. The Estonian Information System Authority has also made key contributions and provided strong leadership in discussions on the issues considered throughout the pilot.

The European Commission services of DG CONNECT and DG DIGIT also supported the pilot by providing advice and guidance on the architecture interoperability requirements and other regulatory issues.

4. More information about Clayster and its technology can be found here: <http://www.clayster.com/index.html>

Methodology: the pilot roll-out

Phase II of the pilot rolled out in two stages. Stage 1 defined minimum viable products, including a process of consultation and surveys with key stakeholders on the selected architectural option and business models considerations and finding a use case. During Stage 2, the pilot participants focused on technical integration including:



- country-level operational integration with the Mobile Connect ecosystem (e.g. whether identity and authentication provider);
- service providers' on-boarding and technical integration into the eIDAS Node;
- cross-border eIDAS Nodes operators' connectivity.

The pilot also explored the use of the eIDAS minimum identity attributes, privacy considerations for the use case and high-level considerations on the sustainability of commercial business models for eIDAS and Mobile Connect. The pilot tested eIDAS with “low” and “substantial” levels of assurance in a user-controlled environment.

Figures 7 and 8 summarise the analysis carried out during the pilot in consultation with the multi-stakeholder group and the pilot timeline.

Figure 7

Phase II Methodology of the pilot

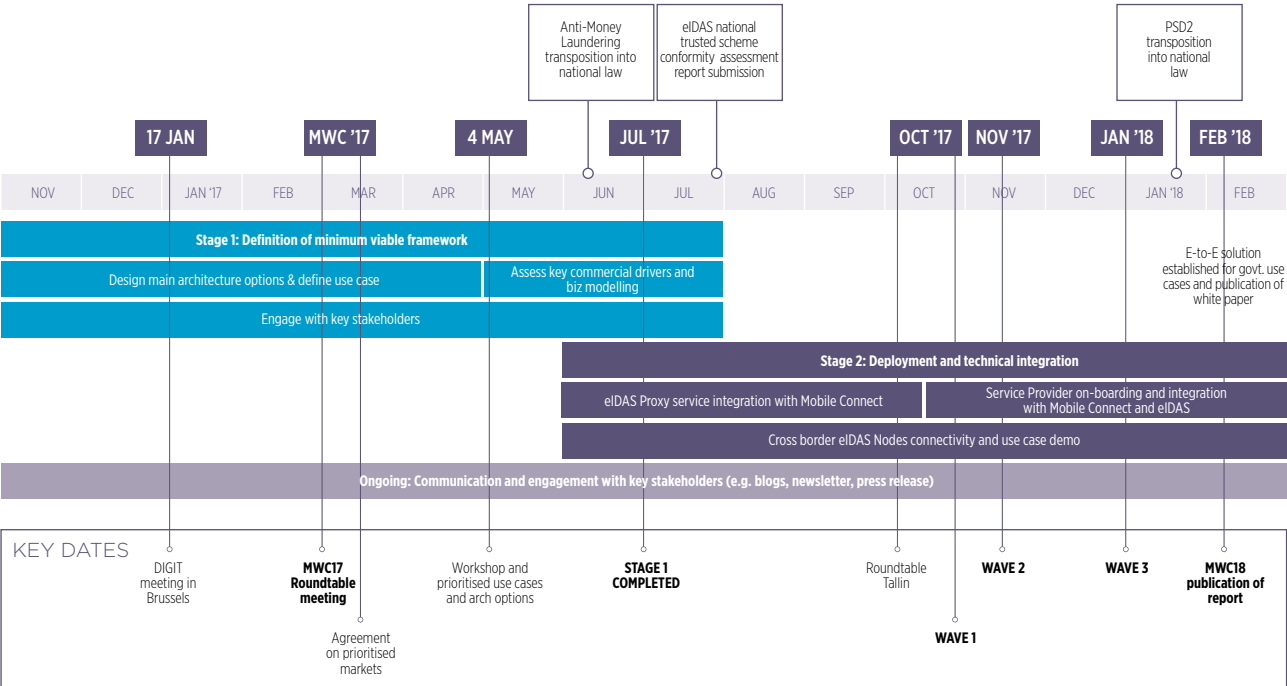
 REGULATORY	 TECHNICAL	 COMMERCIAL
A mapping of Mobile Connect level of assurance against eIDAS guidelines. An analysis of the use of attributes and privacy considerations for the use case. An analysis of the key issues of the eIDAS notification process.	An assessment of the eIDAS key requirements and delivery of a consistent terminology and requirements across stakeholders to ensure the interoperability of private sector solutions. A test of eIDAS reference architecture to achieve technical integration against eIDAS interoperability technical requirements for eIDAS nodes country level. A test and assessment of the eIDAS nodes technical policy requirements for public and private sector use cases.	Identification of high level considerations and key issues with Mobile Connect and eIDAS business models. Public sector and private sector services.

CONSULTATION WITH KEY STAKEHOLDERS



Figure 8

Pilot Timeline



3

Analysis and Key Findings from the Pilot

This pilot demonstrates that the Mobile Connect framework can leverage mobile operators' key assets to deliver a scalable solution that is also easy and secure, while giving citizens control of their data. Mobile Connect operators, in partnership with the broader ecosystem, can provide an interoperable and decentralised federation layer that can be built on top of existing national eID solutions. The pilot also demonstrates that Mobile Connect can effectively support multiple factors of authentication and meet the levels of assurance requirements of the eIDAS Regulation.

The pilot tested a use case where a French citizen that wants to access a Swedish brainwave data service can use Mobile Connect and eIDAS to share her brain

data with a Norwegian doctor. The two-leg use case employed the Mobile Connect authentication process and validation of the citizen's digital identity in France and Norway, via the eIDAS framework. Leveraging the eIDAS federation, and the one-connector to many-proxies technical infrastructure, Clayster, integrated into the Swedish eIDAS Connector Node.

The following sections explain the use case and its findings in more detail, together with a number of technical integration and interoperability issues for consideration for Member States' eIDAS implementations. The pilot also highlights a need for eIDAS implementations to go beyond the mandatory set of attributes for applications in healthcare and some other sectors.

3.1 Terminology and architecture design for technical integration

This section describes how the integration of Mobile Connect with the eIDAS Nodes architecture works and the methodology and critical steps that were deployed during the pilot. The terminology and architecture design were subject to an extensive process of consultation and stakeholders engagement with the European Commission and the eIDAS Nodes single point of contact.

Article 5 of the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework requires:

1. A Node in one Member State to be able to connect with Nodes of other Member States.
2. The Nodes to be able to distinguish between public sector bodies and other relying parties through technical means.
3. A Member State implementation of the technical requirements set out in this Regulation should not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State.

Within these specifications, Member States Nodes include the:

- eIDAS Connector: an eIDAS-Node requesting a cross-border authentication (mandatory for mutual recognition of eID);
- eIDAS Proxy Service: an eIDAS-Node providing cross-border authentication (optional component operated when the Member State notifies one or more eID schemes).

Phase II of the pilot employed the Mobile Connect and eIDAS Reference Architecture (labelled Architecture 3 in figure 5) as the architecture of reference where the Receiving Member State eIDAS Connector Node interacts with the eIDAS Proxy Node of the Sending Member State. The Sending Member State Proxy Node then uses the Mobile Connect system to request the discovery and authentication. The data exchange is managed by the eIDAS Nodes without involving Mobile Connect.⁵

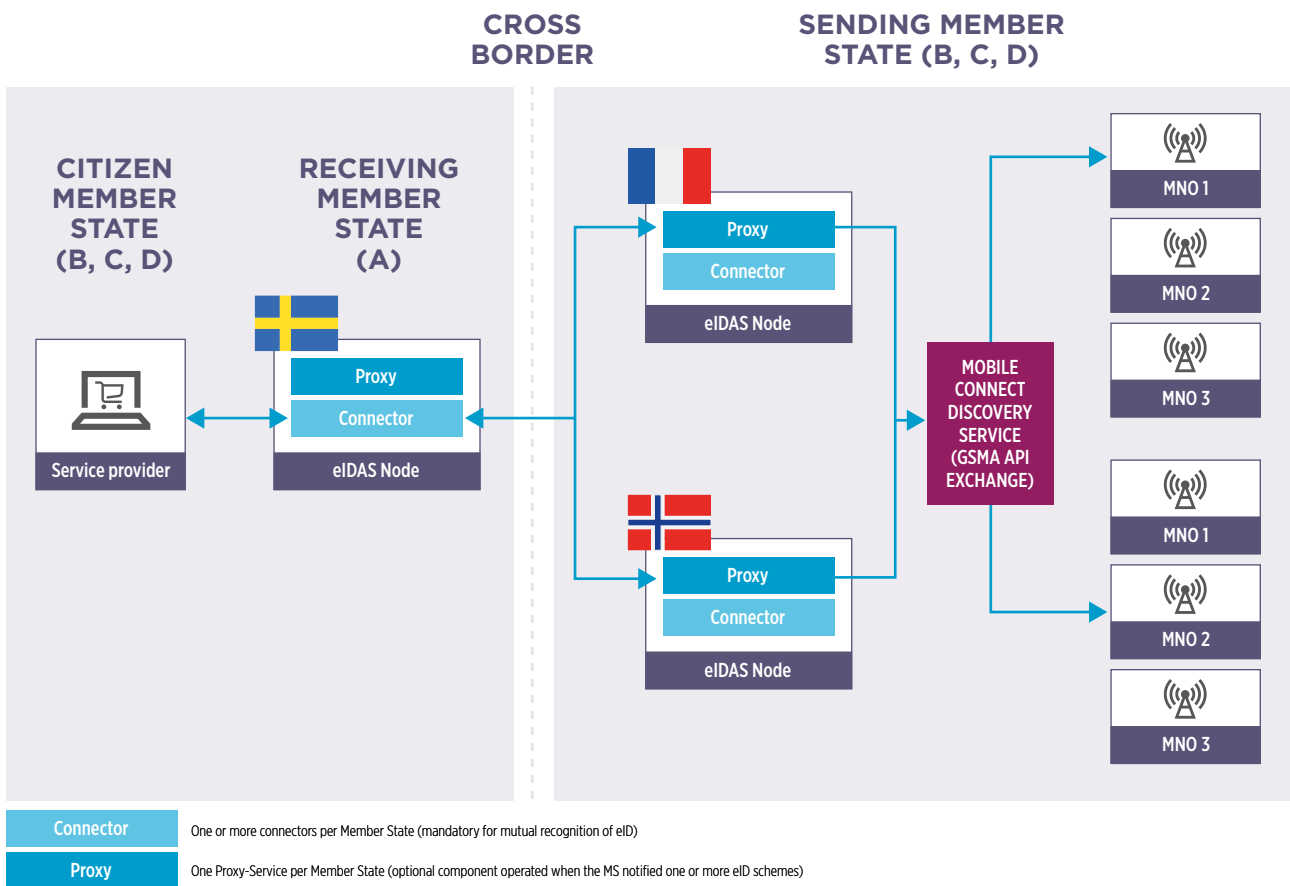
4. With the other models, which are based on a eIDAS Middleware Service, an eIDAS-Service running Middleware is provided by the Sending Member State and operated by the Receiving Member States and providing personal

5. With the other models, which are based on a eIDAS Middleware Service, an eIDAS-Service running Middleware is provided by the Sending Member State and operated by the Receiving Member States and providing personal identification data. In the middleware the proxy service is not in the sending MS but in the receiving MS.

The architecture used in the pilot has been designed to meet the eIDAS Nodes technical specifications developed by the European Commission and Member States technical sub-group of the eIDAS Expert Group including the eIDAS Interoperability Framework (eIDAS IF), in accordance with the eIDAS Technical Specifications of the eIDAS Technical Subgroup (eIDAS Arch), (eIDAS SAML), (eIDAS Attributes), (eIDAS Crypto).⁶

Figure 9

Architecture 3: Mobile Connect and eIDAS reference architecture



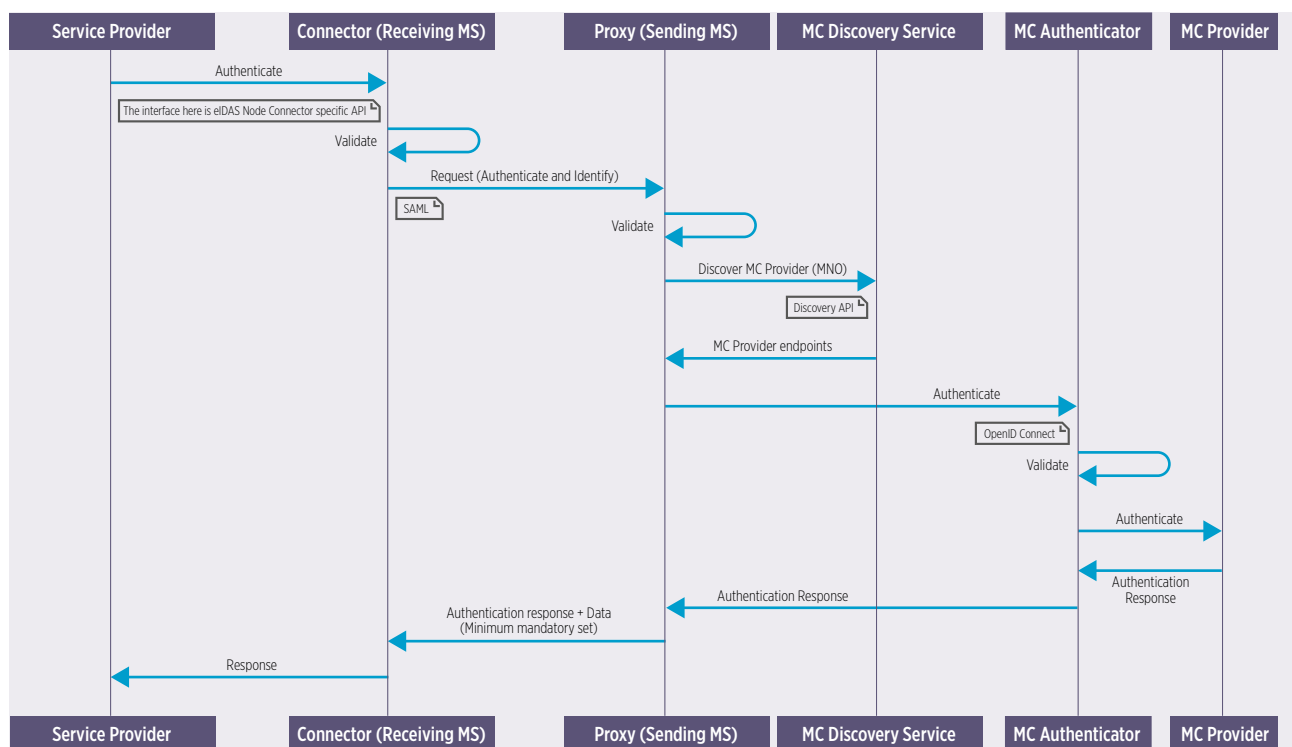
6. <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile>

Here are some key characteristics of the eIDAS Reference Architecture:

- The eIDAS Connector and Proxy Nodes interact with each other as per the eIDAS Interoperability Architecture.
- The eIDAS Proxy Node at the Sending Member States uses Mobile Connect for local federation and authentication.
- The minimum identity attributes are shared between the eIDAS Nodes; in the pilot these are asserted by the Mobile Connect operators as trusted national identity providers.

Figure 10

Mobile Connect and eIDAS technical flow chart



As shown in Figure 10, the service providers interact with the eIDAS Node Connector of the Receiving Member State and the connector sends a request to identify or authenticate the user to the proxy of the Sending Member State. The proxy Member State tasks the Mobile Connect discovery service to authenticate

the customer through the Mobile Connect operator, which then authenticates the user and sends an authentication response to the proxy of the Sending Member State, together with the minimum identity attributes to the service provider.

Box 2

Open ID Connect Framework and Mobile Connect

The Mobile Connect product portfolio is delivered through participating operators exposing their Mobile Connect application programming interfaces (APIs) using the OpenID Connect Mobile Connect technical standard. OpenID Connect is one of the most widely adopted identity standards, from the OpenID Foundation. It is based on the OAuth 2.0 protocol and adds a secure identity layer on OAuth. It is used by many digital identity providers, including Google and Microsoft.

OpenID Connect uses cryptographically-signed identity tokens, which provide the authentication context (e.g. time when the authentication happened, the type of authenticator used, how long is the authentication valid for, who is the recipient of the authentication response, who is the authentication provider etc.).

There are several working groups within the OpenID Foundation across a broad variety of sectors, including governments, which are working to create ad-hoc OpenID Connect profiles. See, for example, the work of iGov (International Government Assurance Profile) and FAPI (Financial API) etc.



3.2 Findings and recommendations regarding technical integration

Efficient and effective integration to eIDAS Nodes is critical to ensure that the full economic and societal value of cross-border eID can be realised in Europe. This section summarises the key benefits for Mobile Connect and eIDAS and then analyses the successes and challenges encountered during the pilot.

How to combine cross-border eIDAS recognition with the convenience and security of Mobile Connect for users and online transactions

The eIDAS Regulation and its interoperability framework aim to provide a seamless and trustworthy environment for service providers throughout Europe. The identification mechanisms can be electronic/mobile IDs, national identity cards, bank cards and others, whether based on single, second or multi-factor authentication as the baseline.

This pilot demonstrates how Member States can work in collaboration with mobile operators through the Mobile Connect framework and leverage mobile operator's key assets to deliver a scalable solution that is also easy and secure, while giving citizens control of their data.

In particular, the pilot focused on how, for both public and private sector use cases, there are benefits in leveraging:

- **eID asserted by a notified identity scheme via the eIDAS Nodes operators**, as assured by the eIDAS interoperability architecture and Member States' Nodes issuing electronic credentials trusted by the government;
- **an interoperable and decentralised federation layer offered via Mobile Connect that can be provided by individual mobile operators and be built on top of existing national eID solutions;**

- **the Mobile Connect API Exchange for the discovery service** helping direct identification providers (or relying parties) to the correct operator that can serve a particular mobile user wherever they are in Europe;
- **the Mobile Connect authentication mechanism to interact with end-users and support different level of assurance** ranging from single factor ("click OK"), two factors ("enter PIN on mobile phone") or multi-factor ("enter PIN plus use of biometrics"); the choice of authentication mechanism depends on the requirements of service providers and eIDAS level of assurance needed during the transaction, trade-offs of cost, coverage and security (e.g. SIM applet, SMS, smartphone app, etc.).⁷

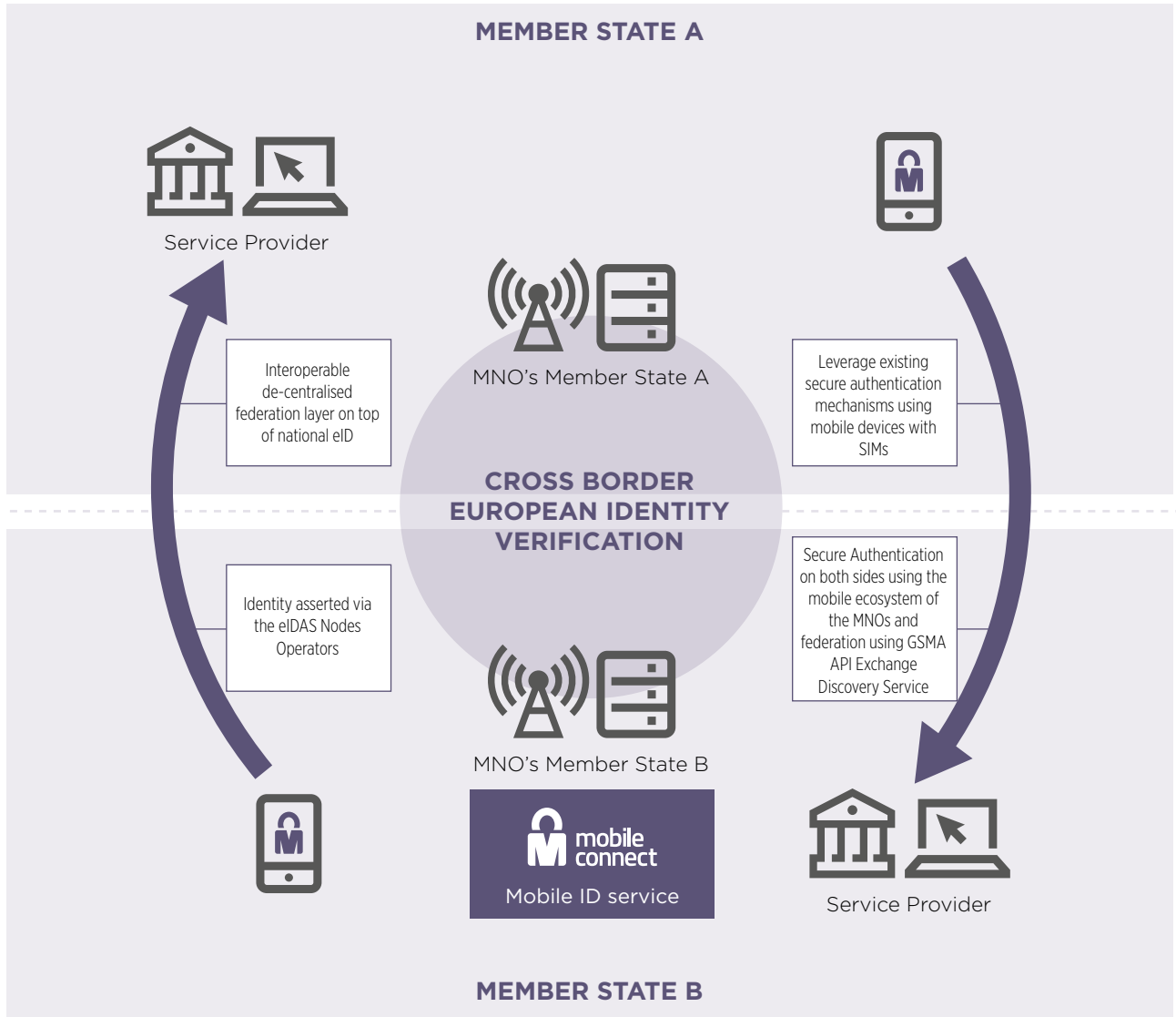
This combination provides a unique opportunity to scale and accelerate the deployment of electronic identification and authentication services both in the EU Digital Single Market and internationally (see Figure 11).

⁷ More details on the role of authenticators and the way piloted mobile operators have met eIDAS level of assurance requirements are provided later in this report.

Figure 11

Mobile Connect and eIDAS

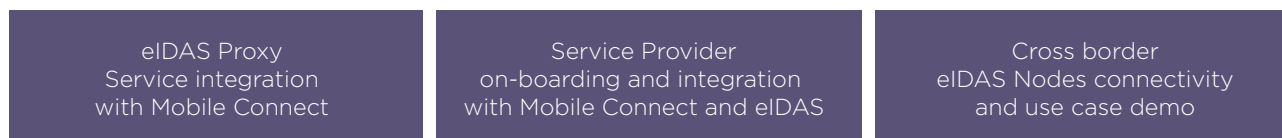
CITIZENS CONNECT TO NATIONAL PUBLIC & PRIVATE SERVICE, CROSS BORDER



Deployment and technical integration between eIDAS Node, Mobile Connect and service providers

Figure 12

Key steps for technical integration and deployment



eIDAS Proxy Service integration with Mobile Connect

The first step during the technical deployment and integration of the pilot was to ensure that the Mobile Connect architecture that was designed during consultation with the eIDAS Node single point of contact was agreed and implemented. This was followed by the

integration and deployment with the eIDAS Node of the “Sending Member State” Proxy service to establish the Mobile Connect connectivity, including for API Exchange and Mobile Connect Identity Gateway and provisioning of eIDAS Node as a client in Mobile Connect. The final step was the routing to the identity provider from the eIDAS Node operator.

Figure 13

eIDAS Proxy service integration with Mobile Connect successes and challenges

SUCCESSSES

- The process of consultation, approval and design with the eIDAS Node Single Point of Contact allowed time to the mobile operators and governments to understand technical requirements and related business opportunities with eIDAS and Mobile Connect.
- The current implementation of Mobile Connect as a national identity and authentication provider for usage through France Connect towards French service providers substantially facilitated the completion of the pilot on the French leg.
- In Norway Difi's flexibility to swiftly include Mobile Connect in their current architecture for the purpose of this pilot, and their current configuration for eIDAS Node directly connected to the national ID-porten, through the use of an “eIDAS adaptor”, facilitated the integration of additional IDPs to the eIDAS Proxy Service.

CHALLENGES

- There are benefits to add optional libraries for Authentication Providers including guidance for integration with the eIDAS Node software reference implementation.
- When routing to the identity provider from eIDAS Node operator current protocols do not flag sectoral and service level specifications. These are needed for business model flexibility and commercial integration, particularly for the private sector.
 - The eIDAS Node Proxy may be connected to multiple IDPs/Authentication and they will need information to route/select the appropriate IDP/Authentication to Service Provider.
 - Currently this is achieved on the basis of level of assurance which is insufficient with live use cases or for example in cases of disputes.

eIDAS Proxy Service integration with Mobile Connect: recommendations

- Consult with industry on the chosen eIDAS architecture, as its selection has important implications for the technical infrastructure deployed by private sector identity and authentication providers. While Mobile Connect can meet both the middleware and eIDAS reference architecture models, a consultation and process of approval and design will also allow time for mobile operators to understand better government's requirements and related business opportunities.
- Publish guidance to help companies to comply with each eIDAS Node's specifications including provision of more granular information about identity and authentication provider's service level specifications (see Box 3).

Box 3

Suggested practical steps for eIDAS Nodes to facilitating the integration with identity and authentication providers

- Publish optional libraries for authentication profiles, including integration with the eIDAS Nodes software reference implementation.
- When routing to the identity provider from eIDAS Node operator, current protocols do not flag sectoral and identity and authentication providers' service level specifications. Additional granularity - such as their level of service provided, costs points, additional attributes available, etc. - will improve the policy implementation for eIDAS Node Proxy when selecting IDPs. This will be particularly relevant in commercial scenarios with live use cases or for example in cases of disputes.



Service providers on-boarding and technical integration into the eIDAS Node

During this step, pilot participants focused on the

integration with the eIDAS Node of the “Receiving Member State” Connector service and testing the service provider integration in a cross border scenario.

Figure 14

Service providers on-boarding and technical integration into the eIDAS Node: successes and challenges

SUCCESSSES

- Leveraging the eIDAS federation and enabling access through one single technical integration to many identity and authentication providers throughout Europe yield significant benefits to companies interested to access the eIDAS infrastructure. By on-boarding into one single connector of the eIDAS federation, service providers can have access to all IDPs/notified and available in EU.

CHALLENGES

- The eIDAS technical specifications adopt a framework that uses SAML extensions to encode and transports. SAML profile is used for the exchange of metadata by the sending Member State. However this only happens for cross-border services, and country implementations standards could vary, which may create inconsistencies for both private sector companies, which largely use more universal frameworks such as the Open ID Connect Framework (OIDC), as well as national eID implementations.
- During the pilot the service provider experienced some difficulties such as ambiguous error codes that delayed the on-boarding at the eIDAS Node level. Pilot participants believed that additional support could include more documentation published for on-boarding portals, and standard documentations

Service providers’ on-boarding and technical integration into the eIDAS Node: recommendations

- Leveraging the eIDAS federation and the one-connector to many-proxies technical infrastructure enables service provider to reach scale and maximise investments made with a single technical integration. Stakeholders should be consulted on the potential for a single contractual and commercial structure, similarly to the technical federation. More considerations on the business model are discussed in Section 4.
- Standardisation of the interface exposed by the eIDAS Connector Nodes to the service providers via the OpenID Connect Framework. OIDC uses cryptographically-signed identity tokens, which are widely used in the industry and also recommended by several governments in Europe including in the piloted countries national eID implementations, such as France and Norway.
- Additional support for service providers and standardised recommendations for service provider onboarding at the eIDAS Node level – especially for the private sector. Support could include more documentation published for on-boarding portals and standard documentations (see Box 4).

Box 4

Suggested practical steps to facilitate the on-boarding of private sector service providers

- **Make available a test suite to test integration before going live including a standardisation of the interface exposed by the eIDAS Connector Nodes.**
- **In addition to the single point of contact, a service desk could be made available by email, live chat and phone to resolve technical issues and questions.**
- **The guidance and required materials to comply with the integration should also be available in English, as well as the language of the eIDAS country.**

Cross-border eIDAS Nodes operators' connectivity

In the last phase of the pilot, participants primarily focused on:

- test the eIDAS Nodes connectivity across countries (see Figure 15); and
- testing the service provider integration in a cross border scenario;
- demonstrating the use case.

Figure 15

Cross-border eIDAS Nodes operators' connectivity: successes and challenges

SUCCESSSES

- The availability of CEF eIDAS nodes connectivity in a test environment significantly helped to an effective implementation of the pilot.
- eIDAS in Sweden, Norway and France in particular having completed the CEF test for many countries across Europe have created a fertile ground for cooperation with interested eIDAS ecosystem players.

CHALLENGES

- Member States eIDAS Node deployments are often based on the CEF releases, which are not necessarily intended to be used as a front-API for services. This means that on-boarding and integration work today must be national. As a result services that are developed to be used cross-border by design will still have to do manual integration for each country.

Cross-border eIDAS Nodes operators' connectivity: recommendations

- eIDAS Nodes services should be designed and tested by default for cross border use cases with a consistent front API based service.



3.3 Data flow and minimum identity attributes

According to the eIDAS Regulation, Member States are responsible for providing assurance of the unique identity of the natural or legal person that is requiring electronic identification and authentication to access digital public services in another Member State.

The eIDAS Regulation has, therefore, defined a minimum set of unique identity attributes to represent an individual, which is usually available from a national identity system. This minimum set of attributes is essential for establishing digital identity across actors within a country's ecosystem and also across borders. As well as mandatory attributes, it may also contain one or more additional optional attributes.

The eIDAS Implementing Regulation (2015/1501) established that the minimum data set of unique identity attributes for a natural (i.e. a physical) person includes both:

- mandatory attributes (current family name(s), current first name(s), date of birth, and a unique identifier which is as persistent as possible in time); and
- additional attributes (first and family name(s) at birth, place of birth, current address, gender).

In many Member States, public sector authorities are responsible for collecting and storing these identity attributes. In others, these may be collected by the private sector or a combination of both.

Typically, a population register office is responsible for the collection of natural and legal person's data and is considered an authoritative source⁸ for identifying and verifying the existence of a natural person. Practices, however, may vary, with some Member States relying on one single authority and others augmenting their security measures through multiple authorities or organisations. Additionally, Member States may have different requirements of the minimum identity attribute that defines a natural or legal person. For example, the approach to unique identifiers varies across countries.

In the pilot, on the basis of the eIDAS Reference Architecture the eIDAS-Service, the assertion of the identity was operated between the IDAS Nodes and the Mobile Connect operators as trusted national identity providers.

Table 1

Considerations on the use of minimum identity attributes for eIDAS

eIDAS Node used	Unique identifiers	Source	Notes
Norway (Proxy)	National ID: Fødselsnummer("birth number"); or a "D-nummer" for persons that are not citizens or permanent residents	Telenor	In Norway, the national ID is required for all government services and many services in the private sector. For cross border services it can be used only if there is a documented need. For the pilot, Telenor has provided full name, date of birth and national ID asserted to a "low" level of assurance, based on its subscriber database and existing on-boarding procedures. Before the information is passed to the foreign service provider, the user must consent in a dialogue implemented in the Norwegian eIDAS Node.
France (Proxy)	Does not include a unique identifier from the user	Mobile Connect et Moi	For this pilot, Mobile Connect is a trusted identity provider. Personal data are scanned and retrieved through KYC secure mobile application. The current solution delivers a substantial level of assurance for eIDAS Before the information is passed to the foreign service provider, the user must consent in a dialogue implemented in the French eIDAS Node.

8. The definition in Implementing Act 1502/2105 is: 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.

From previous research and pilots⁹, other observations that were relevant to this pilot and that can accelerate eIDAS and Mobile Connect implementations include:

- attributes retrieval varies between national register and private sector services. Some countries, for example, do not use dynamic retrieval e.g. when the attribute is in the chip of the national ID card. In addition, in some countries, the use of personal identifiers is forbidden and the policies for consent procedures are not clear. Dynamic retrieval from an authoritative source should be the recommended method for supplying the eIDAS identifying attributes. Countries should also seek to amend national regulation prohibiting the use of national identifier cross-border.

- eIDAS only defines four mandatory attributes. In some domains, such as the healthcare sector, this is not sufficient for operational reasons. As patients and doctors are moving across borders, their data history will require a standardised protocol for exchange, i.e. common concepts that are related to the specific sector domain will need to be agreed across borders to ensure consistency and security in use cases applications. There is a need for standardisation of domain specific attributes to be shared across borders, including mapping of domain specific identifiers.

Overall, clearer rules and standardisation on the use of personal identifiers for eIDAS implementations at Member States level, will yield benefits for scalable cross-border deployments.

Box 5

Mobile Connect Privacy Principles

In alignment with governments' priorities, Mobile Connect solutions focus on privacy and preserving citizens' trust. For example, in keeping with the eIDAS Regulation, and the General Data Protection Regulation, Mobile Connect adopts the principle of privacy by design, seeking to ensure the services and an individual's identity attributes are used in a secure way that respects and protects their privacy.

The Mobile Connect Privacy Principles are intended to guide the use of personal information in Mobile Connect-branded services. Mobile Connect enables verified authentication, authorisation, identity and attribute solutions from pseudonymous log-in, to consent-based attribute verification or validation supporting 'know your customer' purposes, through to helping prevent fraud, and identity theft and account takeover.

The principles apply to mobile operators and third-party online service providers ('participating organisations') that use personal information in Mobile Connect-branded services.

Mobile Connect Privacy Principles contains useful guidelines for the use of identification and authentication services via Mobile Connect. Such principles are published here

<https://developer.mobileconnect.io/privacy-principles>

9. e-SENS 5.2 eHealth eIDAS eID Pilot: Technical Feasibility Report and Norden, Nordic digital identification (eID) Survey and recommendations for cross border cooperation.

3.4 The use case and user journey

Throughout the pilot, a key focus for participant organisations was to offer a service where individuals could claim ownership of their data. This is particularly important for healthcare applications enabled by the Internet of Things.

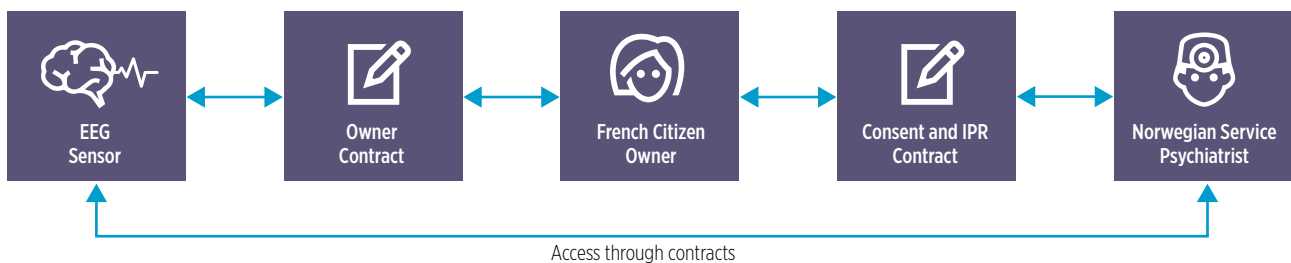
A key differentiator for Mobile Connect implementations is to give users control of their data for both national and cross border transactions. In a connected digital society, the potentially significant benefits of eIDAS for society may remain untapped without enabling an owner-centric approach that puts privacy at the core of the service. Therefore, the pilot designed and tested a user flow that gave a central role to the user as the owner of the device, enabling them to take full ownership of their data.

In the pilot, Mobile Connect authentication mechanisms in combination with eIDAS were used to verify individuals' identities and their digital entitlements for cross-border healthcare digital services, through the Clayster digital entitlement management platform (see Figure 16). The digital entitlement process enables individuals to claim or remove their rights associated to the identities, identities can be revoked and the use of data can be monitored for real time use. In commercial settings, these capabilities present opportunities for mobile operators to create new business models using data and connectivity in a more meaningful and responsible way.

The pilot implemented a use case where a French citizen that wants to access a psychiatrist healthcare service in Sweden can use Mobile Connect and eIDAS to share her EEG brain data with a Norwegian doctor.

Figure 16

Clayster digital entitlement platform



Clayster's technology is supported in existing and emerging standards, such as IETF, W3C, XMPP Foundation, ISO, IEC, IEEE, SIS, IPSO, OCF. Clayster is also on the Swedish committee for ISO/IEC JCT1/WG10 to design a reference architecture for the Internet of Things (IoT)

In the use case, both the doctor and the patient have a contract which links the data and the ownership of the devices to enable a permission framework that has legal value and can be presented in legal proceedings through Clayster's platform. The data is linked to the real identities of the individuals, but in a way that respects privacy and is not stored in mobile operators' databases.



Figure 17

As step-by-step description of the use case

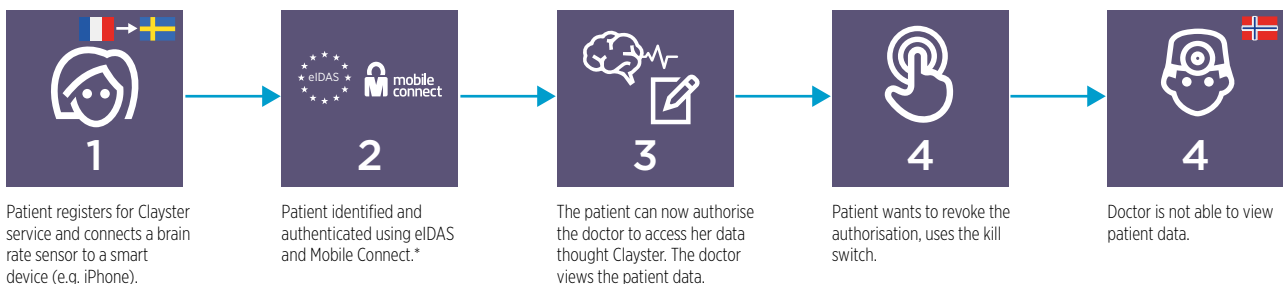
The use case is about how a patient gives consent to a doctor to read out the EEG data, so they can offer their eHealth service to the patient through Clayster’s digital entitlement platform/technology.

USERS:

HELENE: FRENCH patient moves to Sweden to visit family (she has a FRENCH eID)

JORGEN: NORWEGIAN doctor move to Sweden to spend his summertime there (he has a NORWEGIAN eID)

USER FLOW: Helene wants to access to Swedish online service (Clayster) to share her brain data with a doctor.



SUMMARY:

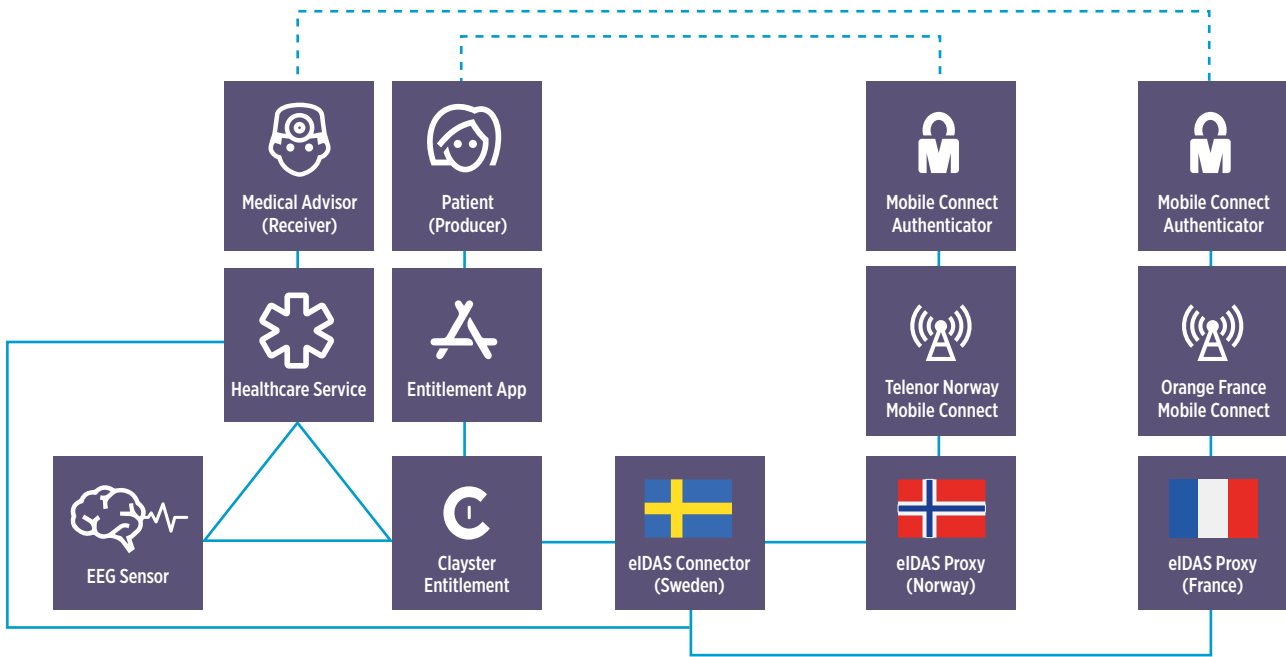
- In summary the use case include a scenario where the user:
- Connects a brain rate sensor to a smart device as a the device to communicate data (e.g. iPhone)
 - Takes digital ownership of the sensor and real time data it produces
 - Invites a medical advisor to read out data
 - Grants access to the sensor for the medical advisor to provide their service

* For the demo the doctor is assumed to be already logged in

Figure 18 shows more details about the two legs of the pilot and how they were technically compliant with the eIDAS requirements.

Figure 18

Pilot use cases: Patient is a citizen of France and doctor is a citizen of Norway



We are honoured to participate in a project that we believe is of the greatest importance for the future of digitalisation and our Internet. Without trusted digital identities, the transition into the digital world will be halted. With a robust eID infrastructure in place, we enable people to claim digital ownership of what they previously could only own physically. In order to control who and when someone has the right to access our IoT device's data, a hard-digital identity is essential. By securing our integrity while connected, trusted digital identities can be attained – allowing for an exponential growth of new services and applications. But this is only possible if we direct the consent decisions towards the rightful owner, rather than third-party delegated owners acting on our behalf. This is what we call the Human-Centric Internet.

Rikard Strid Clayster CEO



3.5 Authenticators and level of assurance

The level of assurance (either low, substantial or high) is a guide to the degree of confidence in an authentication process. As a critical element within the Mobile Connect ecosystem, it is used in the Mobile Connect API (OpenID Connect), in the cryptographically-signed identity token sent as an authentication response to the service provider, in the authenticator-selection policy and also in the Mobile Connect product-enablement policy.

Mobile Connect supports the same security assurance levels as with those stipulated in the eIDAS Regulation (low, substantial and high) as described in Figure 19. In broad terms, the security of the mobile device is ensured via the mobile network in a two-way process, which can, for example, be used to disable a device's connection to the mobile network and the services if the phone is lost/stolen, or in case of SIM swaps or other unusual transactions that are flagged as potential fraud. The mobile phone is used as a mechanism through which the user can authenticate and claim a right to whatever service or transaction they are accessing or approving.

Multiple factors of authentication

Two-factor and multi-factor authentication are increasingly recognised as compliance tools for current and forthcoming regulations in a number of sectors, ranging from electronic payment services to e-government services. Such regulations in Europe include the EU General Data Protection Regulation, the eIDAS Regulation and the Payment Service Directive 2 PSD2.

The user's unique mobile number can be employed as the user identifier in a privacy-preserving way¹⁰ - the "possession" of the mobile phone associated with the mobile number represents the "user has something" factor for authentication, combined with second factor, such as a unique Mobile Connect PIN/Personal Code ("user knows something") or biometrics ("something

the user is"). Mobile Connect can also utilise the secure network of the mobile operators, as necessary, employing mobile operator data and business processes to enhance user security and combat identity theft.

In other words, mobile operators through Mobile Connect have the flexibility to use and combine different authentication factors and meet different eIDAS requirements at different level of assurance. Mobile Connect can employ three assets to provide the different factors of the authentication:

- The mobile device;
- The SIM, providing the security, connectivity to the mobile network and representing the mobile network in the mobile device;
- Contextual data as known by the mobile network.

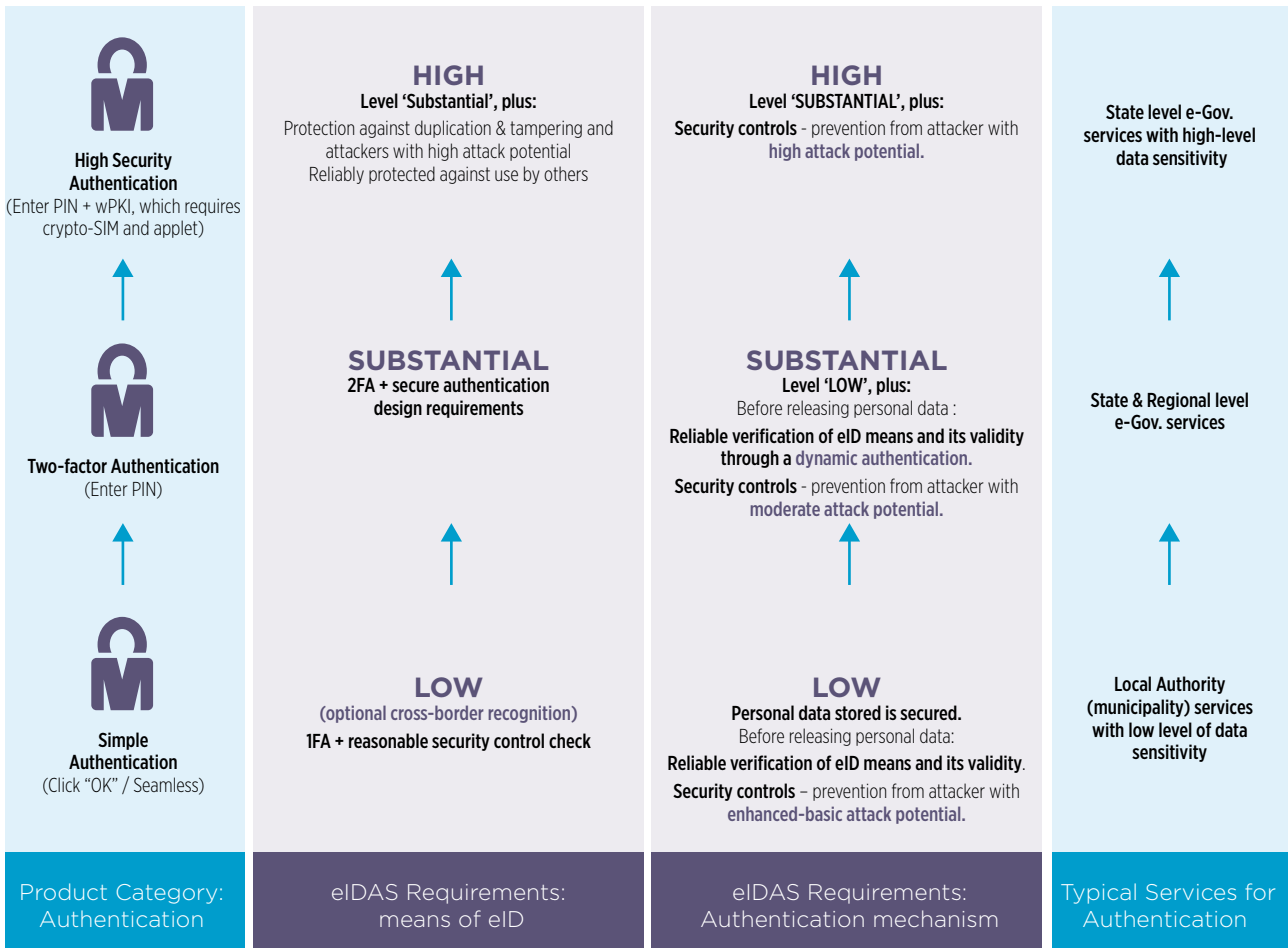
Mobile Connect authentication factors include:

- Possession-based (Something I Have); the possession of the mobile device by the user. This is the first factor used in Mobile Connect Authentication.
- Knowledge/secretcy-based (Something I Know); e.g., PIN/Personal Code.
- Active Inherence (Something I Am); e.g. biometrics: fingerprints, iris scan, facial biometrics etc.
- Passive Inherence (Something the Network Knows); Mobile network-based inherence elements, such as usual cell sites (can also be used as "something the user does") available to the mobile operator. This separation between device and network is vital to fighting fraud and establishing ownership of the device.
- Contextual (Something I Do); e.g., supplement the device-based authentication with network-based insights to create a more robust multi-factor authentication mechanism.

¹⁰ Mobile Connect profile provide a Pseudo Anonymous Customer Reference (PCR) instead of the real identifier to the third party service providers - the mobile phone number. The concept is to share a token (i.e. the PCR) when the user is authenticated - rather than actually sharing any data.

Figure 19

eIDAS level of assurance mapping with Mobile Connect



4

Business Models: High Level Considerations

The goal of the eIDAS Regulation is to advance the European Digital Single Market by serving both public and private sector use cases through eIDAS federation. Regarding public sector use cases, the Regulation is clear – transactions across borders between EU Member States are free. In a domestic context, each Member State can independently decide how they authenticate citizens and the underlying business model and cost-structure.

Private sector use cases are integral to eIDAS federation for two reasons. Firstly, public-sector use cases are not high frequency and high interest for users. Therefore, private sector use cases can help create user acceptance and familiarity in digital authentication. Moreover, it is easier for the individual if they can use the same authentication method for both public and private sector use cases. Secondly,

only a small fraction of public sector use cases involve authentication of EU citizens across Member States. To justify the investment and operational costs of eIDAS federation, the costs need to be spread over a large volume of both public and private use cases. This would also help to create a Single Digital Market within the EU.

Introducing private sector use cases into eIDAS federation brings with it several challenges that will need to be solved before they are commercially viable. Although this topic was at the fringes of the pilot discussions, it is a pressing issue that is gaining increasing attention and interest from participants. Member States have different authentication solutions for citizens with different underlying business models and cost structures. Often multiple solutions are available in a country, e.g. national IDs issued by

government, bank IDs and mobile IDs issued by mobile operators. The market shares of public and private authentication solutions differ across countries. Some Member States, such as Estonia, Austria and Denmark, offer citizen authentication as an “almost free” public service either by the government or through a public-private partnership. .

Several other Member States, such as Norway, Finland, UK and France, are using or planning to use private sector authentication solutions for both private and public use cases. In these models, the government pays for the authentication transactions that it consumes for public use cases. Naturally, private sector companies (as service providers) pay for their own authentications.

Aligning these differences between Member States into a single eIDAS commercial business model is a considerable task that should be urgently tackled. eIDAS Regulation Art. 5 states that “national Nodes shall be able to distinguish between public sector bodies and other (=private) relying parties through technical means.” The protocol has a parameter defined for this, but clear rules and implementation guidelines are still lacking.

This challenge is particularly acute in Member States where the government incurs a cost per transaction for citizen authentications. These countries are not able to serve private sector authentication requests coming through eIDAS from other Member States for free, as they need revenue to offset the cost they pay to the authentication services. Instead, they are likely to refrain from serving private use cases at all, until the business model and commercial structure is in place. The following issues urgently need further work and definition for eIDAS to be a viable solution for commercial use cases in the foreseeable future:

1. **Aligned definition of access conditions for the private sector:** Currently there may be inconsistencies within national authentication schemes regarding the access conditions for private use cases and probably large variances across Member States. In a cross-border context, this might give rise to companies attempting to cherry-pick the cheapest connectors through which their authentication requests are routed - and thus create market distortions.
2. **Commercial contracting structure and pricing:** If private sector authentication transactions through eIDAS federation are chargeable (as they can be in the Sending Member State’s domestic market), a contract with a price needs to be in place between the requesting private company – the Sending Node – the Receiving Connector – and the authentication provider. How are these contracts negotiated, signed and executed? Who gets which part of the revenue that the requesting company pays?
3. **Liability and support structure:** What kind of liability framework covers eIDAS private use cases? How does it relate to the above contracting structure? Who offers customer support to the requesting company if needed? Are any service level agreements applicable?
4. **Billing and payments, credit risk:** Where is the billing data coming from? Who takes care of the data consolidation? Who is doing the billing and payment collection? Is the billing consolidated in some way or is every party billed separately? How is credit-risk managed?
5. **Dispute resolution:** In the case of disputes, some effective dispute resolution mechanism is needed to avoid escalation of minor disputes through a court-of-law. How would this work?

One possible commercial solution could emerge from the ongoing work at the GSMA and several EU mobile operators in forming a commercial federation service called MC Link. MC Link aims to become the commercial contracting, support and billing “one-stop-shop” for cross-border private use cases. In future, it could also possibly contract with national eIDAS Nodes to solve the commercial federation challenges.



eIDAS is a big leap forward in EU Digital Single Market – and a global benchmark outside of EU. But to really drive volume, private sector use cases require further work on business models and public / private cooperation.

Janne Jutila, MD, Internos Partners



5

Piloted Countries

A woman with long hair is sitting at a table, looking down at her smartphone. She is wearing a dark top and a smartwatch on her left wrist. The background is blurred, showing what appears to be a cafe or office setting with a cup of coffee on the table.

This section provides an overview of the eID services being employed in the Member States and relevant organisations involved in phase II of the pilot.

5.1 France

Launched in June 2016 by the French Government, France Connect is an identification and authentication system, which allows citizens, businesses and civil servants to access all online public services in France. The system is intended to provide a unique mechanism of trust and identity federation for all of France's administrative services.

In France, identity attributes need to be verified by France Connect, which acts as a trusted intermediary, validating the user's identity before any data is exchanged with service providers. France Connect provides a unique key to each service provider, which then has the approval to ask other administrations for any data they need. The system can be used by foreign citizens who live and work in France, if an administration has given the foreign citizen access to its services.

The France Connect portal will enable citizens to check their pension plans, their license points and get access to other public services. Interestingly, France Connect is also planning, in partnership with the mobile operators and service providers, to enable access to many other private sector services. More than 30 services have already committed to using France Connect mainly related to PSD2, online gambling, registered mails and identity management corporate services.

France Connect federates separate online identities, such as the ones from the tax authorities or Ameli, the national health insurance organisation, as well as online identities provided by the private sector such as La Poste or Mobile Connect et moi (see Figure 20). France Connect currently has 3 million users and expects to serve 10 million users by the end of 2018.

Figure 20

France Connect portal



12. <https://joinup.ec.europa.eu/document/france-connect-id-federation-system-simplify-administrative-processes>

Mobile Connect in France

Mobile operator Orange and AriadNEXT have been working over the past two years alongside the French government to launch Mobile Connect as both an identity provider and authentication provider in France.

Since November 2017, “Mobile Connect et moi”¹³ has been launched and available to every citizen on France Connect portal along with other identity providers. The service is operated by Orange and AriadNext. After a successful launch, the objective is now to enable other operators to join the initiative and launch the solution in other European countries

The government finds Mobile Connect et moi attractive because:

- it removes the need for new username and password;
- it’s quick, mobile-based registration and access which attract younger generations;

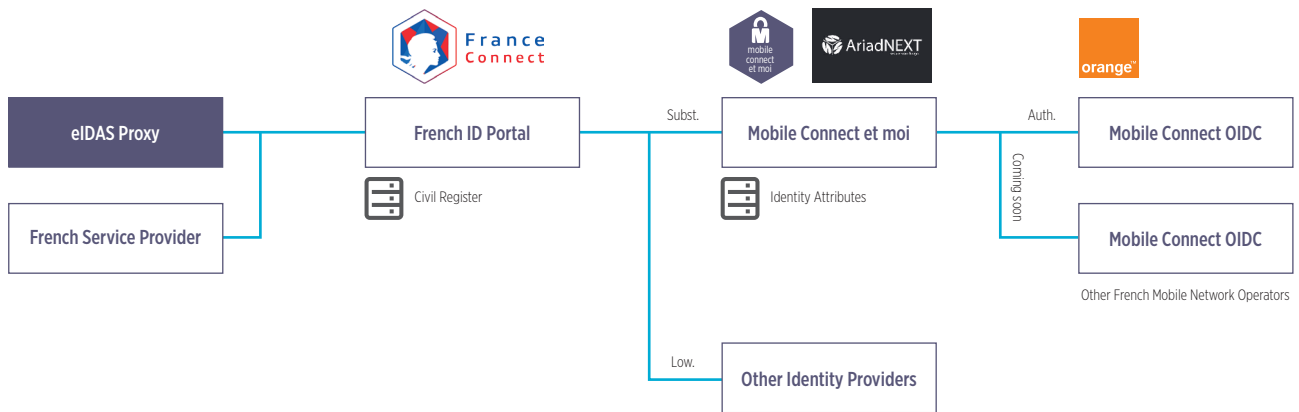
- mobile authentication offers high standards of security in line with upcoming eIDAS Regulation;
- respects privacy – customer information is not shared without permission;
- Mobile operators can increase user trust through government endorsement.

Mobile Connect et moi relies on a symmetric key generated on the SIM for two-factor authentication and a secure KYC mobile application enrolling the user for identity verification. The current solution delivers a substantial level of assurance for eIDAS, but there are plans to upgrade it to deliver a high level of assurance. More information on how to register for Mobile Connect at moi is detailed in Box 6.

Mobile Connect et moi is under evaluation of the Agence nationale de la sécurité des systèmes d’information (ANSSI) and it is expected to be certified during 2018. Its architecture is described in Figure 21.

Figure 21

Mobile Connect et moi architecture



13. More information (in French) can be found here <https://mobileconnectetmoi.fr>

Box 6

The KYC process with Mobile Connect et Moi

Registering for Mobile Connect et moi requires using a KYC mobile application. Registration is based on a biometric process of automated remote verification. This is based on AriadNEXT's technology, which processes identity document verification and facial recognition information in seconds. In about 2 minutes, the user can benefit from a usable electronic identity assured by the government that work on all services offering France Connect authentication.

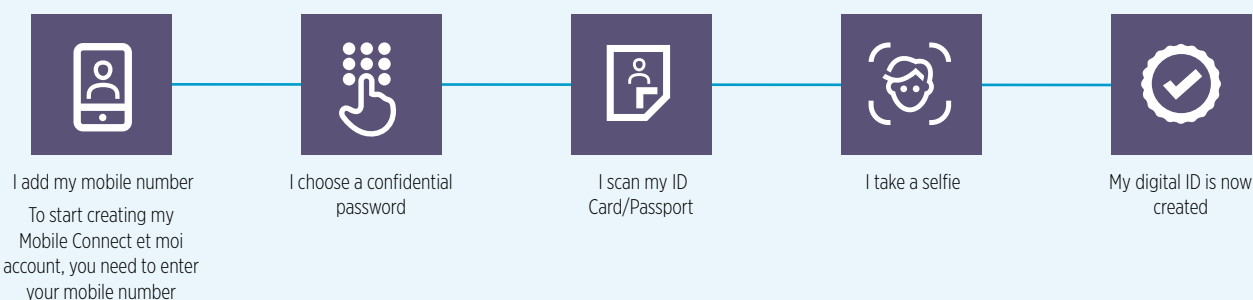
After installing the mobile application on the smartphone, a Mobile Connect et moi account is created. This requires:

- a PIN code for activation;
- a valid Identification document;
- a selfie.

AriadNEXT acts as identity provider and retains the user's personal data combining its remote recording technology with Orange's Mobile Connect SIM based two-factor authentication.

AriadNEXT retains the user's personal data and once initialisation is complete, the user can use Mobile Connect for authentication and identification. If the subject consents, his or her personal data will be made available to the service provider. Once a person has been identified, Orange may share additional information (besides that on the identity card) with service providers. This allows the operator to monetise some attributes of his customers (address, bank details, etc.).

Mobile Connect at moi take can resolve the issues of SIM change, number change, PIN code loss and portability between all French operators.



Mobile Connect and eIDAS pilot in France

For the pilot in France, Mobile Connect was integrated into the eIDAS Proxy service (i.e. as an identity provider).

Since Mobile Connect is a national identity and authentication provider for usage through France Connect towards French service providers, the completion of the pilot leveraged this existing implementation.

However, the eIDAS nodes deployment in France is only available in a test environment, with connectivity currently available with Sweden and Denmark. Other test environments, with no connectivity, are currently available with Belgium and Spain. With Norway, some additional reconfigurations are needed.



Digital identification is essential for the development of our economies and modern democracies. The eIDAS Regulation states nothing else.

In just a few years, mobile phones have become indispensable to our existence. They are already being used to pay, it is natural that they are being used to identify us. Mobile Connect brings authentication, a key element of digital identity. By combining an innovative recruitment method, we have given France Connect, the French digital identity hub, the trusted identity it needs for everyone.

We were thrilled to participate in this pilot. Seeing a French citizen connect to a Swedish service using Mobile Connect et moi has been an experience that we want to become a habit for all European citizens.

Marc NORLAIN, CEO and cofounder AriadNext



5.2 Norway

In Norway, the Difi (Agency for Public Management and e-Government) is responsible for coordination of use of eID in the public sector through the services of ID-porten. Under the Ministry of Local Government and Modernisation, Difi is responsible for regulation and implementation of eID usage for eGovernment services.

Under the Ministry of Transport and Communications, the Norwegian Communications Authority (Nkom) is responsible for the supervision of eID systems under eIDAS. To ensure the security of information, Difi, in 2006 implemented a central authentication and single sign-on service for the different government agencies in Norway. This solution enables citizens to use the same login portal regardless of which public service they intend to access. This central service is called IDPorten and has been implemented as a hub and bespoke architecture.

The “ID-porten” is mandatory and is used for authentication by most public services. As of today, various authentications solutions are available for service providers (see Figure 22): one public IDP on assurance level substantial (MinID) and three market solutions on assurance level high, BankID, BuyPass, Commfides. Private sector service providers are not

Facts about the ID-porten

- **The ID-porten provides access to more than 1,100 networking from more than 600 public works and is a public joint venture run by the Directorate for Administration and ICT (Difi).**
- **The ID-porten allows residents to choose between five electronics IDs: The public owned, their own MinID and the private lanes: BankID, BankID on mobile, Buypass and Commfides.**
- **MinID is at an intermediate level of security. MinID accounts for 28.4% of login paths in the ID-porten.**
- **BankID, BankID on mobile, Buypass and Commfides provide access to the highest-level security services. BankID issues 48.5%, BankID on mobile 20.4%, Buypass 2.7% and Commfides 0.02% of login paths in the ID port.**

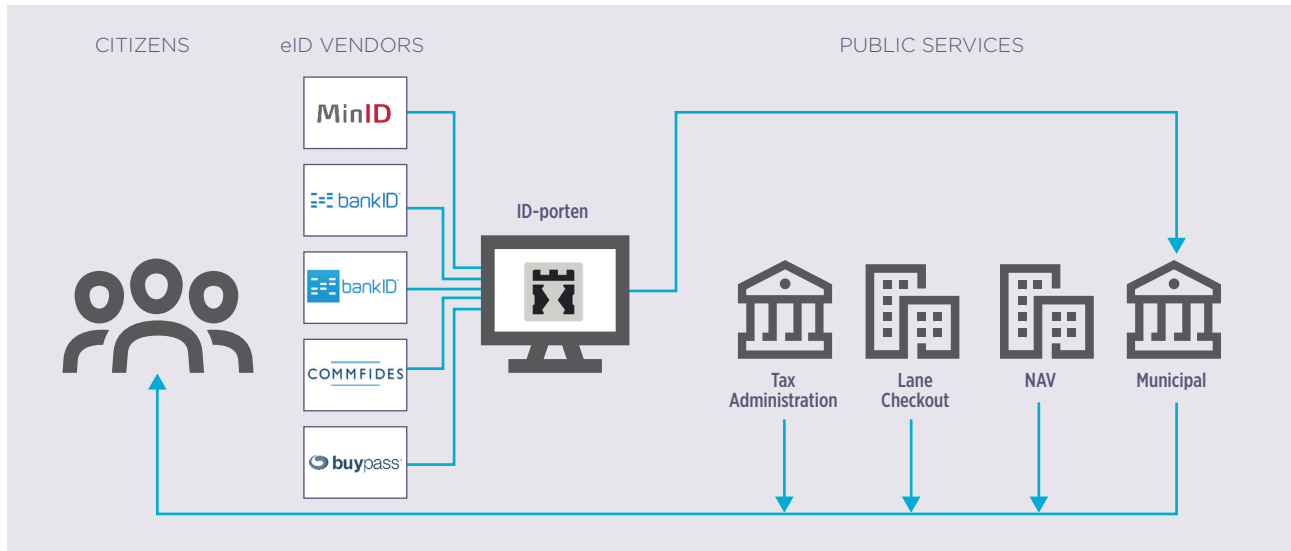
Source: Difi report on the public Norwegian eID market, 2016

allowed to connect through the ID-porten, as this would distort the free market. Private sector service providers must thus make agreements with the market IDPs directly. Due to competition law «statsstøtte», private service providers are only allowed to connect to ID-porten, if they operate “on behalf of a public body.”



Figure 22

eID vendors currently operating in Norway



Source: www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/id-porten

Current regulatory requirements in Norway are summarised in the «Rammeverk» document¹⁴ and for Person-Høyt (aka LoA-4).¹⁵ However, these documents will be revised this autumn, and the eIDAS-levels and requirements will be included in Norwegian Law.

Mobile ID in Norway

In 2009, a partnership between DNB Bank, a leading Norwegian bank, and Telenor, the country's largest mobile operator, brought about the launch of Mobile BankID, a personal electronic identification credential which supports secure transaction authentication and legally binding signatures across a wide range of online services through the user's mobile phone. Using secure PKI technology and storing bank-generated certificates

on the SIM card, Mobile BankID enables users to login and conduct transactions without the need for a traditional code calculator, using only their mobile phone and a secure PIN code of their choice.

Strong customer demand for Mobile BankID now means all five of Norway's mobile operators have signed on to offer Mobile BankID to their customers, leading to full market coverage.

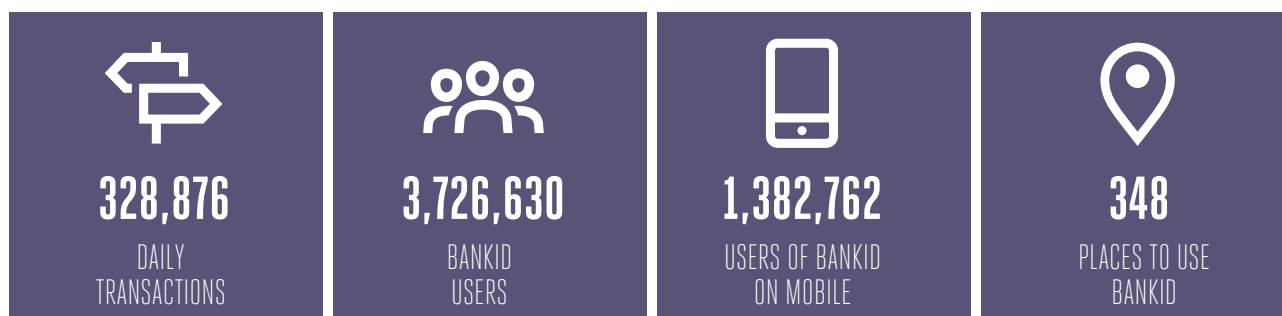
Users can have their BankID stored on their mobile phone's SIM card. BankID on mobile has more than 1.38 million users at present (see Figure 23). In order to sign something or verify your identity using BankID on mobile, you use your mobile phone number, date of birth and a self-selected PIN code.

14. <https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/>

15. <https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/>

Figure 23

Mobile Bank ID number of transactions per day (last update January 2018)



Source: www.bankid.no/en/company/

The role of Difi (Agency for Public Management and e-Government) for eIDAS

Difi plays a central role in establishing the connectivity with the building blocks from the EU's Connecting Europe Facility (CEF). Difi has deployed an eIDAS Node and has tested it with several EU Member States, including Denmark, Estonia, France, Iceland, Sweden and the UK.

OpenID Connect is available for Norwegian public service providers. A study is under way to improve record matching of eIDAS users towards the Norwegian Population Registry.

Mobile Connect and eIDAS pilot in Norway

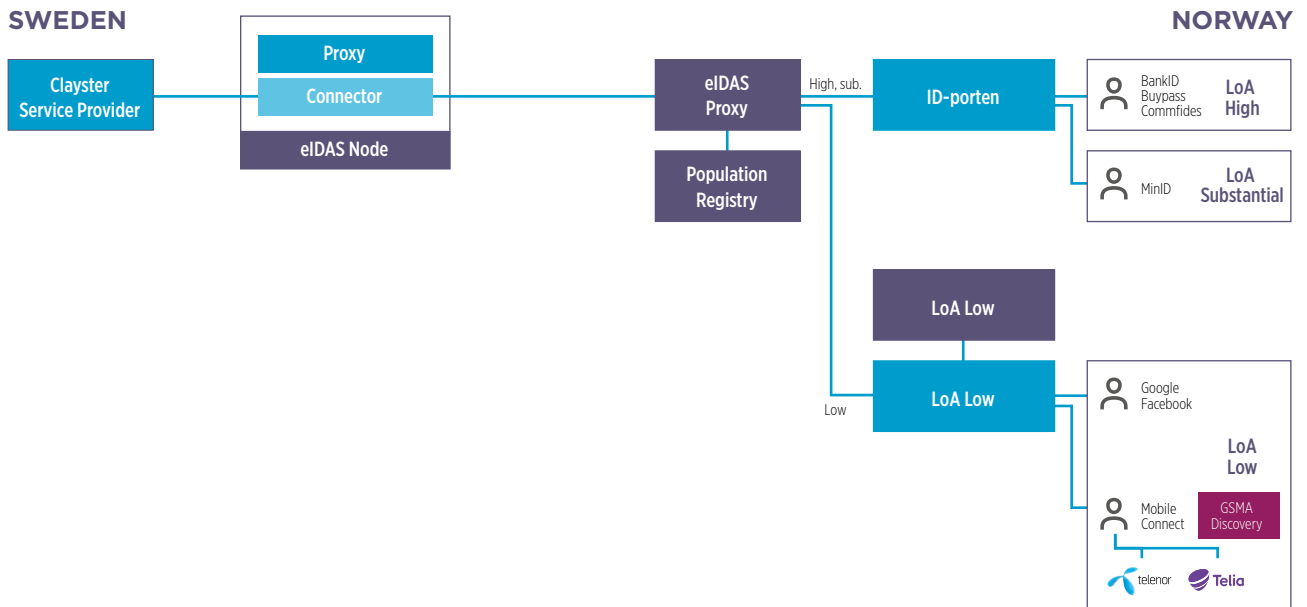
For the pilot, Norway acted as an eIDAS Proxy service (i.e. an identity provider). To enable easy introduction of eIDAS services towards the Norwegian eID infrastructure, the eIDAS Node is connected to ID-porten, through the use of an "eIDAS adaptor". The adaptor is handling both the eIDAS Service and the eIDAS Connector flows.

Since Mobile Connect is not among the procured national eID schemes approved for usage through ID-porten towards Norwegian services, it was not possible to add Mobile Connect as a regular eID scheme in ID-porten for this pilot. But as Difi was running a separate pilot on authentication using low level of assurance, it decided to add Mobile Connect to this component. Support for the GSMA API Exchange discovery service, as well as pilot-specific scopes from Telenor (eIDAS minimum attribute set), was added to the level low as per eIDAS requirements.

In the eIDAS Proxy flow, the adaptor then chooses between regular Norwegian eID schemes and Mobile Connect based on the requested level of assurance, where "low" triggers a Mobile Connect authentication towards Telenor. See figure 24.

Figure 24

eIDAS and Mobile Connect architecture for the pilot



Source: Difi analysis



5.3 Sweden

In Sweden, the Swedish E-Identification Board, an agency under the Ministry of Enterprise, Energy and Communications, is responsible for the eID system and eIDAS Nodes.

Since 1999, the Swedish eID system has relied on eIDs issued by the private sector, mainly banks and a large telecoms operator. A bank ID and mobile bank ID is the main solution people use to login to public administration websites and private sector websites.

The BankID network includes 11 banks and is available on smart card and a soft certificate, as well as mobile phones and tablet computers.

In 2017, the transaction volumes of Bank ID on mobile application were 91.4% compared to 30.6% for the use of Bank ID on a smart card and only 9.7% when used on the file. In the Swedish Mobile BankID the eID is stored and used in a mobile application.

Figure 25

Transaction volumes for Bank ID (Mobile, smart card, on file)



This approach has driven the uptake of eID for online services for both the private and public sector. For all eID vendors, however, users must be registered in Sweden and have a Swedish social security number.

The Swedish government has identified the requirement to make an ID check in-person as a barrier to broader availability and competition between eID mechanisms. BankID remains the only widely used e-credentials for both the private and public sectors, creating in effect a market monopoly.

To deal with some of these issues, the government launched a project called the “National Infrastructure Authentication Control” in 2016. The aim of the project is to ensure universal access to Swedish e-credentials by developing a national distributed service to perform the in-person identity checks of individuals. The service would be shared by every provider, regardless of their technical solutions.

The project has delivered a technical platform that enables credential control through a distributed, shared Infrastructure that meets the requirements of the E-credentials’ Trust framework for Swedish e-ID. By separating the legitimacy check from the other issuing process, it has facilitated the approval of a number of independent e-credentials by the E-Identification Board for the Quality Mark “Swedish e-ID”. This should catalyse the development of mobile solutions, facilitate the integration of more online services, and facilitate cooperation with other Member States.

The public sector buys the validation control services of eIDs on a commercial basis. eID providers which join the federation will thus generate an income based on a flat rate, as opposed to the previous pay-per-use model. Payments from the service providers to the eID providers are made centrally via the eID Board. A flat rate was preferred, over a ‘pay-per-use’ solution, to facilitate the development of public services with high volume of transactions. However, reaching an agreement on the value of this rate proved to be difficult, as the government wants to stimulate the entry of new providers, but has a limited budget.

eIDAS in Sweden

For Swedish actors who will link up via the eID, the SAML 2.0 method is used according to the E-ID Board’s technical framework.

The Swedish test infrastructure site provides information about test services provided as a means to investigate and test national infrastructure components in accordance with the eIDAS technical specifications. Any entity, both private and public, is welcome to test free of charge. More information is available online.¹⁶

16. <http://eidasweb.se/home/connectioninfo.jsp>

5.4 Finland

Finland has had an electronic identification infrastructure for more than 10 years. The Ministry of Finance is responsible for the overall strategy, coordination and budget.

The Population Register Centre (PRC) is responsible for issuing e-identities and for hosting the Finnish eIDAS Node. It creates an electronic identity (eID) for Finnish citizens when providing them with a personal identity code. This electronic client identifier is used for electronic user identification in secure online transactions. It is a dataset consisting of a series of numbers and a check character that helps identify Finnish citizens and foreign citizens permanently residing in Finland who are entered in the Population Information System.

FICORA (Finnish Communications Regulatory Authority) is the regulator and supervisor authority.

eID solutions in Finland

Finnish banks launched their eID solution Tupas more than 10 years ago and it has full coverage across almost the whole population. Tupas is used for online banking authentication, payment authorisation and third party service identification across private and public use cases. Tupas is based on username-password complemented with a one-time-passcode from a paper list. It is still the dominant authentication solution today in the Finnish market despite the obvious drawbacks on usability and security.

Mobile Identity services

In Finland, mobile operators understood the importance of identity comparatively early, and have worked collaboratively to offer a mobile identity service that allows the user to strongly authenticate themselves across a broad variety of services.

The three leading mobile operators – Telia, DNA and Elisa, have launched Mobile ID (“Mobiilivarmenne” in Finnish), an identity service that employs a shared, common platform for the authentication of users to third party service providers, irrespective of the network operator to which they subscribe. Uniquely, the three operators have formed a “circle of trust” – an agreement under which the operators accept digital identities created by each other, and allow those identities to effectively “roam” on their network and make use of agreements that each individual operator has with third party service providers.

Mobile ID has been widely adopted by both private and public services providers and there are well over 1,000 services active. The user-side has scaled slower because of the dominant position of Bank ID. Although the banks have been slow to adopt the operator-driven Mobile ID solution, Finland offers a compelling glimpse of the future: mobile identity services are not only mature in their own right, but also offer consumers access to a compelling and growing range of services.



Box 7

Mobile Connect in Finland, Estonia and Lithuania

Mobile Connect is connected to Finnish Mobile ID through the Telia Identity Gateway. Mobile Connect service providers from anywhere can reach all Finnish Mobile ID users through standard Mobile Connect APIs. The authentication request flows through the API Discovery service to Telia, which then either authenticates the Telia subscribers or passes the request to the other mobile operators through Finnish Mobile ID Circle of Trust.

As per the Finnish Mobile ID solution, users have a wPKI client on their SIM-card and they enter their PIN-code to confirm authentication at level of assurance substantial. Likewise, the Finnish service providers using Mobile ID are looking to expand their reach and to authenticate Mobile Connect users in other countries where possible.

Telia is currently using Mobile Connect for authentication of employees in Finland, Lithuania and Estonia on internal human resources services.

eIDAS Node in Finland

The Finnish eIDAS Node is being developed and will be hosted by the Population Registration Centre. The Connector and Proxy will be available during 2018 and will support eIDAS authentication requests for public sector use cases. The private sector use cases will not be supported for the time being, as in Finland, the Government needs to pay the authentication service providers (Bank ID and Mobile ID) for each authentication.

Finland has a long history of cooperation with other Nordic and Baltic countries (especially Estonia) in the area of eID and authentication. There are large numbers of tourists and workers crossing the borders, as well as companies operating across the region. There is a strong need for regional cross-border eID solutions, which can be relatively easily agreed and implemented due to the advanced infrastructures, trust and close cooperation ties. Thus, the Nordics and Baltics are likely to be at the forefront of cross-border authentication in the years to come.

5.5 Estonia

The state issues electronic identity, in the form of a smartcard (e.g. ID-card, digiID, etc.) and SIM card-based Mobile-ID, to citizens. The government also uses bank-ID, a private solution provided by banks, for authentication. The RIA (Estonian Information Systems Authority) is the entity responsible for the eID technical architecture, development of client / end-user software, chip technical specification and application for eID. It also coordinates the state information system development projects and the preparation and participation in EU and international projects.¹⁷

e-ID card

The main e-ID card is ID-card (the physical identity document with eID chip¹⁸) mandatory by law owned by 99% of population. This is issued from the service offices of the Police and Border Guard Board.

e-ID card can be used to authenticate the holder in an electronic environment, enable a user to create qualified electronic signatures and decrypt encrypted data (addressed to the user). In order to fully use eID functionalities, an ID-software is required, which can be downloaded from the website <http://installer.id.ee>, as well as a card reader. Almost all private sector e-services accept government-issued eIDs. Some public services accept other credentials, such as the bank ID, but only for services where the security requirements are not as high as those offered by government-issued eIDs.

Mobile-ID

Mobile-ID is a government-issued eID solution, operated by the certificate authority called SK ID Solutions. Mobile operators primarily provide the data exchange and maintenance of the SIM card. Unlike e-ID, Mobile-ID is not mandatory in Estonia and can be applied for from the age of 15. Today it is used by about 25% of the active eID users.

In this solution, the secure element is embedded into the SIM card allowing people to use their mobile phone as a form of secure digital ID. Like the e-ID card, it can be used to access secure e-services and electronically sign documents (qualified e-signature), but without the disadvantage of requiring a smart card reader or software installation to the computer). Moreover, it works on any handset so the user does not need to have a smart phone. Mobile-ID, however, doesn't support decryption functionality (decryption of the data with a private key on the SIM card).

To authenticate oneself securely with Mobile-ID, the user clicks on a dedicated button in the web environment (see Figure 26). Upon completion of this action (giving his/her personal identity code and mobile-ID phone number), the login web page will show the control number. The user receives an operator message with the e-service name and the control number, which is calculated locally in the phone. If the control number matches and the user accepts the transaction - he/she will be requested to enter their authentication PIN number. Once this operation has been completed, authentication is performed.

17. https://www.gsma.com/identity/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf

18. <https://www.politsei.ee/en/nouanded/dokumentide-naidised/identity-card/>

Mobile-ID's major advantages include user-friendliness and convenience. The rapid uptake of Mobile-ID in Estonia has been driven by the private sector with the support of the government. Consumers in Estonia are increasingly demanding services that are accessible via mobile.

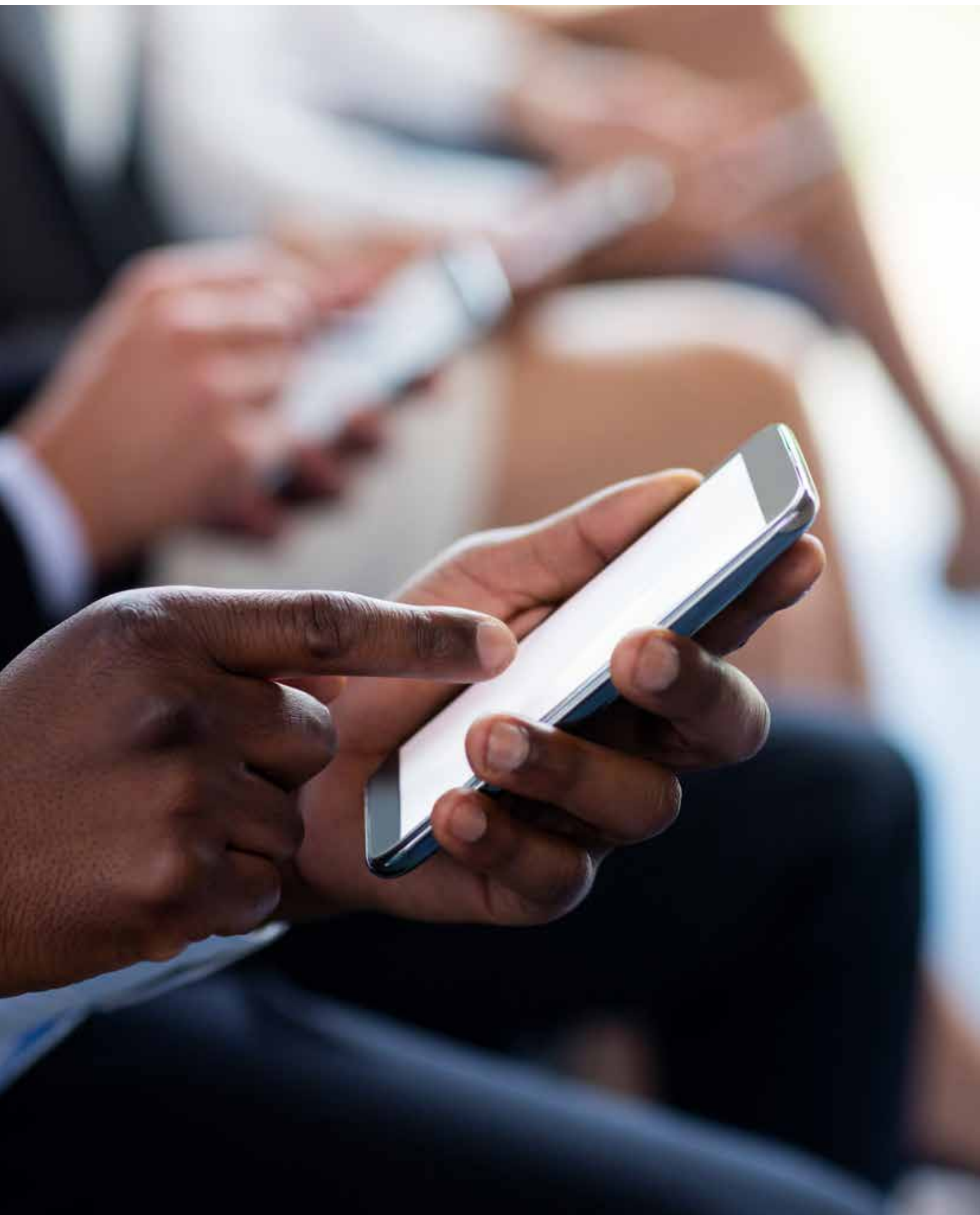
Figure 25

EESTi Single portal and Mobile ID

The screenshot displays the EESTi Single portal website. The header features the EESTi logo with the tagline "Gateway to eEstonia", a search bar, and navigation links for "Site map" and "Advanced search". The main navigation bar includes "My Data", "Services", "Topics", and "Contacts", along with an "Enter" button. The main content area is titled "EUGO Point of Single Contact" and provides information about the EUGO network, which offers single contact points for entrepreneurs across the EU. A map of Europe highlights Estonia. Below this, there are sections for "Study in Estonia", "Starting a company", and "Official government services". A "Login" modal window is open, offering options to "Login with ID-card" (using KAART) or "Login with mobile-ID". The mobile-ID login form includes fields for "Personal code" and "Phone number", and an "Enter" button. Below the login options, there is a "Login via bank" section with logos for SEB, Swedbank, Danske Bank, Nordea, and Krediidipank. A disclaimer at the bottom of the modal states: "By entering this site you accept the Terms of use terms and conditions of the state portal Eesti.ee."

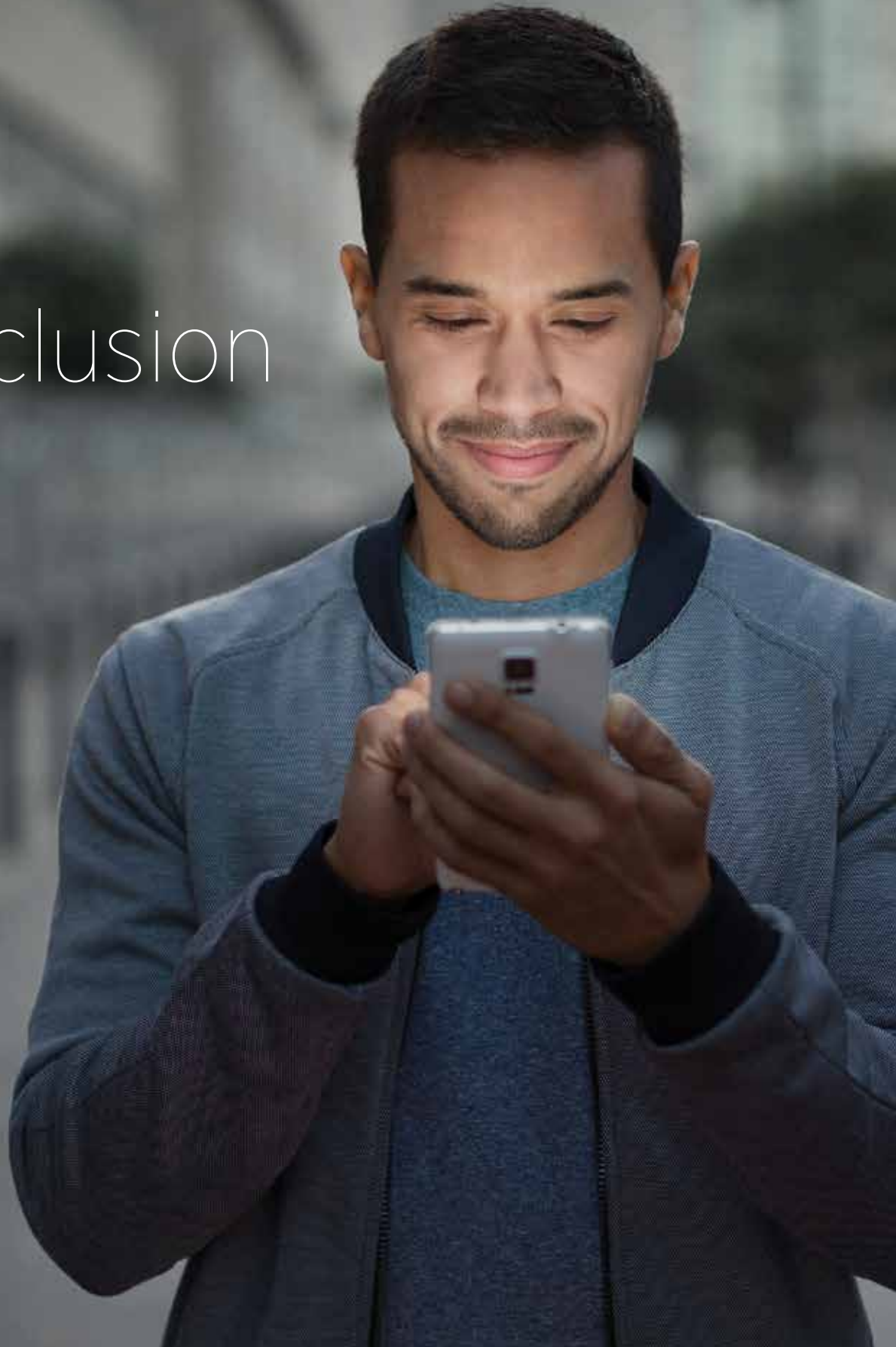
Mobile-ID is a chargeable service in Estonia costing users €1 per month. To use the Mobile-ID service individuals need to make a contract with their mobile operator to receive a mobile-ID ready SIM card. In the next step, they

need to apply for the Mobile-ID certificates at the Police and Border Guard Board website by authenticating themselves and electronically signing the application with their ID-card (eID).



6

Conclusion



Secure, convenient and trustworthy mobile identity solutions, such as those supported by Mobile Connect, can be delivered by mobile operators. The benefits of such solutions are widespread and well recognised by many stakeholders.

Mobile operators can help governments to deliver a digital transformation, while empowering citizens and building a more connected digital society. Mobile Connect is based on well-recognised international standards and, as demonstrated by this pilot, is compliant with the eIDAS regulatory and technical requirements.

The completion of the pilot (both phase I and phase II) is an important step towards developing a strategic action plan to accelerate the cross-border recognition of mobile identity solutions for both public and private sector use cases, driving scale and ensure interoperability across Europe and beyond

While the pilot demonstrated that the technical integration of Mobile Connect and the eIDAS framework is possible, and desired by an increasing number of stakeholders, the integration with eIDAS-Node infrastructure and eID schemes for private sector use cases is managed at national level, requiring a close co-operation between the eID system authorities and eIDAS Node single point of contact in each country. The introduction of a more formal, consistent process by Member States for integrating with the eIDAS nodes could yield benefits.

Last, but not least, it is crucial that a commercial model exists before any private sector use cases can move to commercial deployment within the eIDAS federation. As these issues are important for governments, mobile operators and private sector online services, they need to be fixed rapidly.

The GSMA will continue to convene the industry, develop material, such as this report, and work with governments and EU institutions to contribute to the European Digital Single Market.

Annex:

High Level Guidance For eIDAS Notification

Notification system for identification providers

Member States supervisors will typically issue guidelines or regulations to ensure compliance with eIDAS and national legislation.

Prior to commencement of services, a notification procedure will be typically required for all relevant stakeholders. Any changes to information provided will also have to be notified.

For each stakeholder different rules may apply as explained below:

From Member States to the European Commission

An eID scheme needs to achieve notification prior to commencement of services for eIDAS purposes. Notification of an eID scheme comprises several steps:

- 1. Pre-notification:** A Member State intending to notify an eID scheme submits the material necessary for notification to the Cooperation Network at least six months before it is seeking notification. This material should comprise:
 - A description of the eID scheme and how the scheme fits into the interoperability framework;
 - Documents providing information and evidence that the eID scheme complies to a chosen Level of Assurance;
 - Information on responsible bodies for supervision of the scheme, as well as enrolment and issuance.

- 2. Peer Review:** Based on the material submitted, the other Member States may initiate a peer review of the to-be-notified eID scheme. As part of the peer review, the reviewing states may ask for additional information from the notifying Member State. The peer review concludes with a formal opinion on the scheme by the eIDAS Cooperation Network. However, the results of the peer review process are not legally binding and, regardless of the outcome, the applicant Member State can still notify the scheme. But the political pressure of a negative or critical outcome of the review will hopefully suffice to stop notifying Member States from notifying a “broken” or “too weak” scheme.

- 3. Notification:** The European Commission publishes the notified scheme, which triggers the mandatory recognition of that scheme after twelve months. The Commission does not have the right to reject a notification, and must not judge the correctness of the notification. Only obviously wrong or incomplete notifications can be rejected.

This procedure is the result of long discussions during the deliberation on the regulation, as well as in the Expert Group. The main point of contention was the question who is responsible for evaluating the to-be-notified schemes: the notifying Member State, the receiving Member States, or the Commission. Each variant comes with its own (obvious) risks.

The situation is further complicated by the quite different situations in the Member States, ranging from eID schemes completely operated by the private sector at one end of the spectrum, to schemes based on governmental identity documents at the other end of the spectrum. The latter documents are comparable to passports, which are issued under sole authority of the Member State, but fully recognised by all (Schengen)

Member States. After weighing the risks and the needs of Member States to keep control of their national eID schemes, it was finally decided that the schemes should be evaluated by the notifying Member State. The peer review was introduced to address the receiving Member States' desire to have some insight in (and assurance on) the notified scheme.

Notification of eID to other Member States

- Pre-notification: submission of material necessary to the Cooperation Network at least six months before it is seeking notification.
- Peer review: under the monitoring of other countries (the reviewing states may ask for additional information from the notifying Member State) and a formal opinion issued on the scheme by the eIDAS Cooperation Network.
- Notification: Publication in the Official Journal.

Case study: National requirements for notification in Finland

An identification provider that want to be notified under eIDAS will need to provide specific information as part of the notification procedure in a specific Member State. In Finland, for example, the FICORA guidelines state that the information to be included in the notification process typically include:

- Company name, country of origin, contact details etc.
- Level of assurance provided (substantial or high).
- Financial resources.
- Organisational chart, functions and staff general description.

FICORA also calls for the service provider to describe the identification devices provided and their levels of assurance, together with the identification principles, including a description of the initial identification procedure (identification device providers only) or a description of the identification brokering principles (brokering principles, identification broker service providers only).

eIDAS Trust service providers: how to initiate services

The eIDAS Regulation creates an internal market for trust services, namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication. As of 1 July 2016, the provisions applicable to trust services apply directly in the 28 Member States. This means that trust services under eIDAS are no longer regulated by national laws. With this change there are opportunities for mobile operators and other companies to earn new revenues for the creation, verification, and validation of interoperable mobile signatures and other qualified trust services.

To become a qualified trusted service provider, the service provider needs to go through a pre-authorisation process, known as an initiation process. A service provider may only begin to provide the qualified trust service once qualified status has been granted by the competent supervisory body and it has been added to the national trusted list. The supervisory regime then oversee the full life cycle of each qualified trust service, and the associated service, from its genesis until its termination.

In practice, an unqualified service provider needs to successfully pass an external assessment (audit) to confirm it fulfils the eIDAS requirements, before notifying the competent supervisory body of its intention to start providing qualified trust services. The audit, which will evaluate the authentication method or brokering service and the associated information security, must be conducted by a conformity assessment body specifically accredited to carry out assessments of qualified trust services and providers. Once it has passed that audit, the service provider submits to the supervisory body a notification of its intention to provide qualified trust services, together with a conformity assessment report issued by an eIDAS-accredited conformity assessment body.

Based on the notified information, including the report of such an audit, the competent supervisory body will formally verify that the candidate service and service provider meets the applicable eIDAS requirements. It will then publish the qualified status of that service and service provider in the national trusted list. Only then is the service provider authorised to provide the corresponding qualified trust service. Qualified trust service providers may use the EU trust mark to brand and promote the quality and trustworthiness of the qualified trust service provided.

Notification of trusted service providers to national supervisory body

In summary, the initiation process consists of the following phases:

- The preparation.
- The notification.
- Initial compliance verification, including:
 - The analysis of the notification (procedure and format).
 - The analysis of the submitted conformity assessment report.
 - Granting, in case of positive verification, a qualified status to the trusted service provider and to the trust service(s) they provide.
- Publication of the qualified status in the national trusted list.

Once qualified status is granted, the competent supervisory body will ensure that the qualified trusted service provider and the corresponding service meet the requirements laid down in the Regulation. To that end, it will:

- conduct regular (every two years) audits (see below);
- monitor events, such as the termination of one, more or all of the qualified trust services, changes in the provision of a qualified trusted service; a security breach, a personal data breach and the results of surveillance audits, when applicable;
- respond to complaints;
- respond to requests for cooperation from other supervisory bodies.

In each case, the supervisory body can, where appropriate, withdraw the qualified status.

Note, the supervisory body may, at any time, audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body will inform the data protection authorities of the results of its audits.

Information included in the conformity assessment report

The conformity assessment report is to provide sufficient details to demonstrate that the assessed service provider and the associated service meet all the applicable requirements of the eIDAS Regulation. The structure and the information provided in the conformity assessment report should be aligned with the specifications provided in the notification form. It should include:

- Memorandum and Articles of Association of the notifying service provider.
- Evidence that the notifying service provider maintains sufficient financial resources and/or has obtained appropriate liability insurance with regards to the provision of the trust services for which a qualified status is requested, e.g. including:
 - Copy of the profit and loss account and balance sheets for the last three years for which accounts have been closed; failing that, appropriate statements from banks.
 - Liability insurance statements.
- Trust service policy(ies) that applies(apply) to the trust services for which a qualified status is requested.
- Trust service practices statement that applies(apply) to the trust services for which a qualified status is requested.
- Trust service detailed architecture (e.g. PKI hierarchy along with the indication of the supported trust service policies) of the trust services for which a qualified status is requested.
- Test samples of all relevant and applicable types of outputs from the qualified trust services the notifying TSP intends to start providing.

- List of standards with which operations are claimed to be compliant; and with which operations are audited, evaluated, certified or assessed to be compliant and details about the underlying audit, evaluation, certification or assessment scheme.
- Copy of standard end-user agreement the notifying TSP intends to use with regards to the provision of the trust services for which a qualified status is requested.
- The risk assessment related documentation aimed to support demonstration of the requirement of eIDAS Regulation Art.19.1.
- A security & personal data breach notification plan aimed to support demonstration of the requirement of eIDAS Regulation Art.19.2.
- The termination plan (eIDAS Regulation Art.17.4.(i), Art.24.2.(i)).

In addition to any applicable national language, all relevant documents regarding format and procedure for notification under Art.21.1 of the eIDAS Regulation should be made available in UK English. The confidentiality of the information notified by the service provider to the supervisory body should be ensured (since it may contain sensitive information).

Contributors to the Pilot

The GSMA would like to acknowledge the many valuable contributions received to the pilot and the report from all the following participants:

The Single Point of Contact (SPOC) of the eIDAS-Node implementer

Tor Alvik, Technical Director, Difi, Agency for Public Management and e-Government in Norway

Jørgen Binningsbø, Project Manager, Difi, Agency for Public Management and e-Government in Norway

Mark Erlich, eIDAS Coordinator, EISA, Estonian Information System Authority

Roger Fagerud, IT-Strategist and Project Manager for eIDAS in Sweden

Lionel Fouillen, Business Developer, Secrétariat général pour la modernisation de l'action publique, France Connect

Eric Heijligers, Product Owner, Secrétariat général pour la modernisation de l'action publique, France Connect

Gunilla Nordlöf, Director-General Swedish Agency for Economic and Regional Growth, Sweden e-Identification Board

Helen Raamat, e-ID Project Manager, EISA, Estonian Information System Authority

Mobile operators and online private service providers

Thierry Barba, Director Ecosystem Development, Orange

Brage Bjontegaard, Product and Business Manager, Telenor

Tobias Gockel, Product Manager for GSMA Mobile Connect, Telenor

Stefan Karlsson, CTO, Clayster

Ilkka Keisala, Development Manager, Telia

Serge Llorente, Mobile Connect Director, Orange

Jürgen Niinre, Development Manager, Telia Estonia

Marc Norlain, CEO, Ariadnext

Joni Rapanen, Global Product Manager, Telia

Rikard Strid, CEO, Clayster

Observers and advisors

Carlos Gomez-Munoz, Policy Officer - Seconded National Expert DG Communications Networks, Content and Technology (CONNECT)

Janne Jutila, Managing Director, Internos Partners

Andrea Servida, Head of eGovernment and Trust at DG Communications Networks, Content and Technology (CONNECT)

Kimmo Mäkinen, Development Manager, Ministry of Finance of Finland

Riita Partala, Development Manager, Population Register Centre of Finland

Olli-Pekka Rissanen, Special Adviser, Ministry of Finance of Finland

Keith Uber, VP Sales Engineering, Ubisecure

Alice Vasilescu, IT Project Officer, Directorate-General for Informatics (DIGIT)

The GSMA pilot team

Marta Ienco, Head of Government and Regulatory Affairs for the Identity Programme, GSMA

Gautam Hazari, Mobile Connect Chief Architect, GSMA

Claire-Marie Healy, Ecosystem Engagement Manager, GSMA



About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 300 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 industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

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

Follow the GSMA on Twitter: **@GSMA**

GSMA HEAD OFFICE

Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601