Signicat

The State of Digital Identity in Europe 2024 – 2025

Contents

Introduction

The world is seemingly becoming smaller and more interconnected. Modern communication and trade are shrinking both the time and distance between buyers and sellers. In a digital network where everyone is included, the global becomes local and the local, global. In this report, we examine how digital identity is helping to power this.

We will discuss the state of digital identity in Europe, plus examine the possible outlook for the future or futures. (For a regional perspective, see The State of Digital Identity in the Nordics 2024 report). Europe is a single continent, and various initiatives are underway to harmonise regulation across the single market. Yet the route to the future all depends on where you start.

I wouldn't start from here

There's an old joke about a tourist who stops a local and asks, "How do I get to x from here?" The local replies, "Well, if I were you, I wouldn't start from here!" Yet when it comes to digital identity, each country in Europe starts from a different 'here', namely from a different place regarding identity verification: electronic identification (eID) and electronic identity document verification (eIDV).

Let's start by defining these mechanisms:

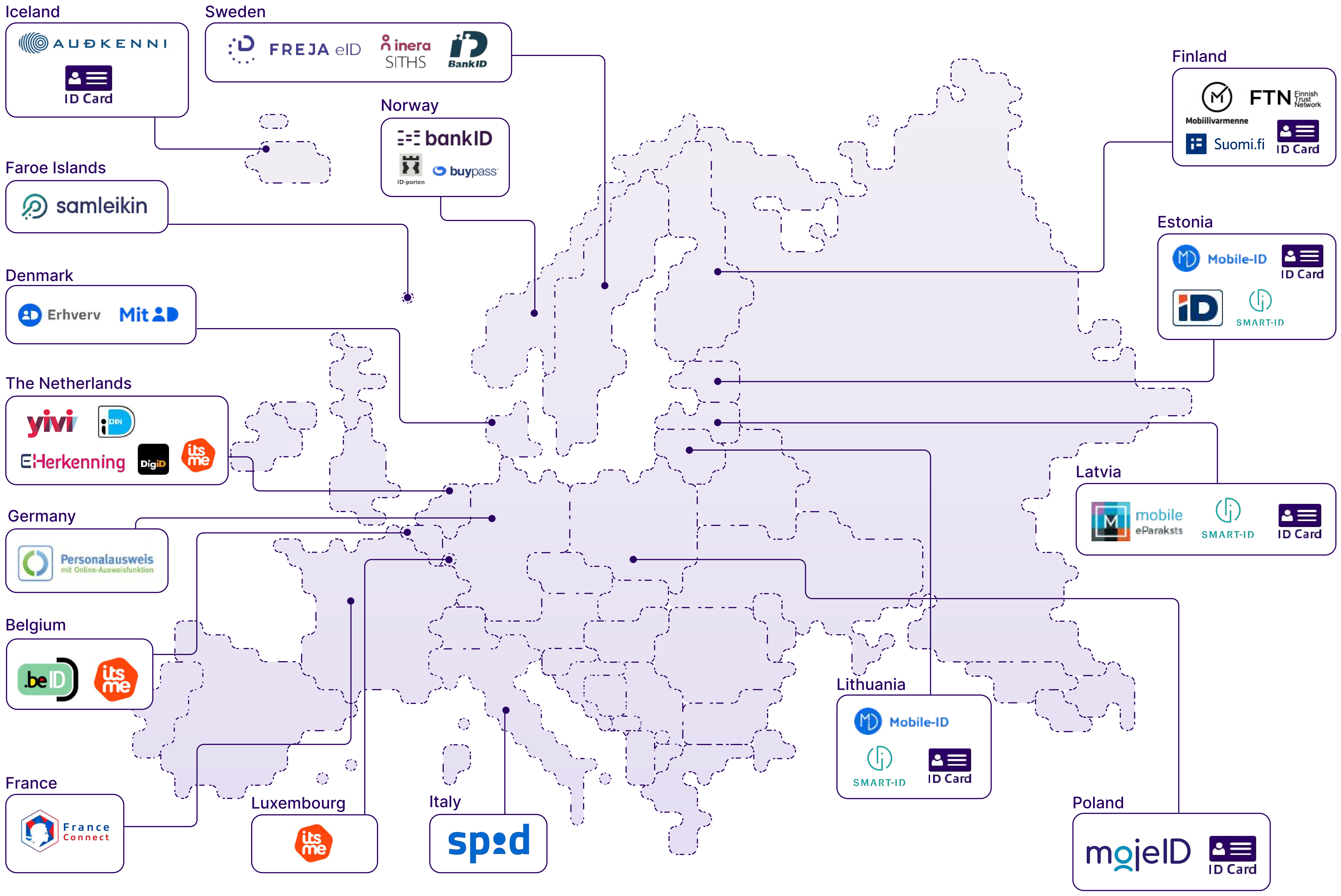
> **Electronic ID (eID)** is a digital representation of an individual's or entity's identity. eID serves the triple purpose of identification, authentication and signing in the digital sphere, akin to traditional, physical identification forms, such as passports or identity cards.
>
> This enables individuals to assert their identity online securely to access various services and execute transactions. eIDs can be issued by governments, private sector institutions or schemes and have been pioneered in the Nordics by Norwegian and Swedish BankID since the early 2000s. Today, there are 60+ eIDs across Europe with varying levels of assurance under eIDAS[1], but factoring in all identity providers, the number is likely 150+, with varying use cases and levels of take-up.

Signicat eID Hub

Signicat's **eID Hub** is the world's largest electronic identity hub, integrating over 35 identity methods across Europe. It offers a single point of integration, which drastically simplifies different protocols to market-standard APIs with additional customisation capabilities. This ensures seamless access to various eID methods, while guaranteeing compliance with local and European regulations such as eIDAS.

Signicat's eID Hub is a trusted partner with global reach, designed to evolve with your needs. It offers secure, seamless online onboarding, authentication, authorisation, and electronic signing, improving user experience and customer engagement while enabling expansion into new markets and sectors.

[1] eIDAS stands for electronic Identification, Authentication and Trust Services. The eIDAS Regulation creates a framework for safer, faster, and more efficient electronic interactions between businesses across Europe, unifying electronic identification (eID) and trust services. For eIDAS Levels of Assurance of eIDs see Page 7.



eIDs supported by Signicat

Electronic identity document verification services (eIDV) focus on remotely verifying a person's identity using an identity document. This process is crucial for various scenarios, including onboarding, issuing eIDs or certificates for signing, and serves as a fallback for individuals without a functional eID. eIDV operates effectively across borders, as official identity documents—particularly passports—are globally recognised.

The general use cases for eIDV can be grouped into three key areas:

- **Onboarding:** The most critical use case, where eIDV verifies a person's identity when they join a service or platform.
- **Step-up:** Enhancing an existing eID with additional security measures as needed.
- **Obtaining QES:** Providing a qualified electronic signature for users who do not have an eID or other usable means.

Typically, eIDV involves capturing an identity document, such as a passport, national identity card, or, in some cases, a driving licence. The capture can be done either by optical scanning of the identity document or by reading the chip of an identity document that has this feature. The process includes capturing an image of the applicant, often via a selfie-video, and comparing it with the photograph on the identity document using biometrics and/or manual verification. Security measures, such as liveness checks, ensure that the video is of a real person in front of the camera.

VideoID by Signicat

VideoID is an advanced eIDV method that utilises video streaming for identity document and biometric verification. This solution enables users to securely scan international ID documents, verify identity by comparing facial patterns, and perform liveness checks to prevent fraud. Known for its speed, superior user experience, security, and compliance, VideoID is widely adopted across regulated industries. It provides the same level of security and legal compliance as face-to-face identification.

Signicat's VideoID is a certified technology that leverages AI to identify individuals in real time from any device or channel. It is approved in Spain under the LINCE standards, facilitating identity proofing accepted across the EU while ensuring protection against document tampering and identity fraud.

This global solution supports a wide range of ID documents from over 150 countries. Driven by machine learning, it employs multiple models to detect document tampering and identity fraud, including black-and-white copy detection, document integrity checks, and hologram verification. Additionally, it incorporates various liveness detection challenges and mechanisms to identify presentation and injection attacks.

The entire process is fully automated and unattended. If VideoID High is required, for example, for a qualified electronic signature, a human agent must review the result, which takes a few minutes. Otherwise, the result is available immediately. This provides a quick and convenient user experience that significantly enhances conversion rates for our customers.

PictureID by Signicat combines an ID document with a selfie to verify likeness without full liveness checks. This AI-powered solution offers real-time processing and completes onboarding in seconds, resulting in high conversion rates and global compliance. It effectively addresses challenges such as high abandonment rates, fraud risk, and regulatory requirements while minimising onboarding delays and manual verification costs, ensuring a swift and efficient user experience. This product is ideal for use cases with a medium or low level of assurance.

How different European countries 'do' identity has been shaped by various cultural, political, economic and technological factors. Travelling the length and breadth of Europe, the digital identity tourist will encounter innovators and early adopters through to laggards and everything in between.

Let us be your knowledgeable guide in the digital identity landscape. Signicat is Europe's leading provider of digital identity solutions, covering the entire digital identity lifecycle—from identity proofing to authentication, signatures, and the orchestration of onboarding and signature workflows. We are the trusted partner of some of the largest enterprises in Europe and beyond, delivering the highest level of assurance for their transactions.

In our Grand Tour of European eID and eIDV solutions, we offer pen portraits of 16 key countries. These profiles spotlight some of the most important nations in the landscape of electronic identification (eID) and electronic identity verification (eIDV) in Europe. Please note that this is not an exhaustive list; the report highlights countries with notable developments or influence in the eID/eIDV domain.

eID and electronic signatures are regulated in the EU by the eIDAS Regulation. This regulation was recently revised to introduce the European Digital Identity Wallet (EUDIW). By the end of 2026, all EU Member States must offer an EUDIW to their citizens. Over time, this may completely change the identity landscape in Europe—see Page 38 for information on the EUDIW.

Grow your business securely: the strength of combining verification methods

Integrating electronic identities (eIDs) with electronic identity verification (eIDV) significantly enhances digital identity verification across Europe. This combination:

1. Enables cross-border expansion with a unified approach

2. Creates significantly improved conversions through an enhanced and inclusive user experience

3. Enables onboarding to your own multi-factor authentication (MFA)

4. Steps up security in case of elevated risk of fraud

5. Creates qualified electronic signatures for high-value transactions

Cross-border expansion with a unified approach

As businesses expand across markets, combining eIDs and eIDVs unlocks extensive commercial potential by providing a flexible approach to digital identity verification of end users. Relying on just one method can limit reach—eIDs are local and at best region-specific, making them effective only where they are widely used. eIDVs offer broader coverage but may create friction for users accustomed to eID-based systems.

Signicat bridges this gap by offering both eIDs and eIDVs in the optimal combination. Through its world-leading eID Hub, which supports over 35 eID options and its pioneering eIDV product VideoID which has the same security and compliance as face-to-face identification according to eIDAS, Signicat allows organisations to seamlessly navigate regulatory complexities and onboard end-users from virtually any country.

Efficient scaling across multiple regions demands a unified approach to managing electronic identification and verification processes. Partnering with a single vendor for both eID and eIDV allows businesses to enter new markets in as little as 17 days while meeting local regulatory requirements.

By partnering with Signicat, **Bank Norwegian** has found a one-stop shop for all its identity needs, creating a seamless identity management solution that enhances customer experience without compromising security. This collaboration has also enabled the bank to expand its services internationally, streamlining identity verification and catering to a wider customer base while ensuring compliance with local regulations. Read the full customer story of Bank Norwegian.

Improved conversions through enhanced and inclusive user experience

Fast and efficient user onboarding is critical for business growth and competitiveness. Yet, over two-thirds of potential users abandon digital financial applications, leading to an estimated €5.7 billion in annual revenue loss for financial services, according to Signicat's Battle to Onboard research.

While eIDs alone provide a solid onboarding experience, integrating eIDVs enhances flexibility, allowing organisations to onboard users who don't have an eID. This empowers users with a choice in how they verify their identity, creating a more inclusive and personalised experience.

By combining eIDs with eIDV options, organisations can offer greater flexibility in user identification, significantly improving the onboarding experience and thus lifting the onboarding conversion significantly. Signicat's customers have seen conversion rates increase by 19 percentage points, turning a once burdensome process into a seamless one.

To optimise results, companies should tailor their approach to the specific needs of each market. For instance, in markets like Germany where eID usage is lower, combining eIDs and eIDVs ensures a balance between user convenience and security. By addressing diverse user preferences, organisations can boost satisfaction and drive higher conversion rates.

The University of Turku has revolutionised its identity verification for international students by implementing Signicat's automated solution. Previously taking 30 minutes per student via video calls, the process is now fully automated, significantly enhancing efficiency and saving resources.
To discover how the University of Turku streamlined its onboarding process, read the full customer story.

Onboarding to your own multi-factor authentication (MFA)

Relying solely on eIDs to authenticate returning users during login can be expensive. What's more, it's not always user-friendly in circumstances when quick, secure authorisation is needed, for example in payment scenarios.

Signicat's MobileID provides a secure alternative by offering a custom multi-factor authentication (MFA) solution compliant with Strong Customer Authentication (SCA) under PSD2. MFA combines at least two factors, such as something the user knows (password), something they have (mobile device), or something they are (biometrics). To ensure this authentication process is secure, eIDV plays a vital role during onboarding, as it can use identity documents from any country. This flexibility allows organisations to implement a single MFA solution globally, enhancing the onboarding process by incorporating information validated from trusted channels.

Entercard, a leading Scandinavian credit market company, enhanced its onboarding and authentication processes by partnering with Signicat. Using Signicat's MobileID, Entercard implemented a multi-factor authentication (MFA) solution compliant with Strong Customer Authentication (SCA) under PSD2. This shift reduced client acquisition costs and streamlined ID verification, enabling quick and secure authorisation while maintaining compliance across multiple countries. Read the full customer story.

ReuseID: Signicat's reusable identity solution
A reusable identity is an electronic identity that can be securely used across multiple user journeys, such as onboarding, authentication, and signing, including across different merchants. It's characterised by its portability, interoperability, consistency, and user control. Customers can also integrate their own eID within their ecosystem.

Why choose a reusable identity?
- Single verification: Create and verify an identity once, then reuse it across your entire ecosystem.
- Customisable attributes: Add specific attributes to the identity, whether industry-specific or geographic, such as affordability or user segmentation.
- Future-proof: Reuse the same identity for all future operations.
- Adaptive security: Apply the right level of assurance at the right time, with the ability to add step-ups as needed.
- Custom branding: Maintain your branding throughout the identity process.
- Comprehensive security: Benefit from transaction monitoring and fraud prevention across all operations.
- Global reach: One solution that works across all markets.

More information on ReuseID.

Security step-ups in case of elevated risk of fraud

eIDs are effective in preventing fraud, but they will not eradicate it fully. Signicat's Battle Against AI-driven Identity Fraud found that 60% of organisations stated that eID fraud is a bigger threat than three years ago. Over the last three years, deepfakes have become the most common threat used in eID fraud. Interestingly, the study showed that Norway experienced the highest level of deepfakes attacks among the countries we surveyed. eID (NBID) penetration is very high in Norway and NBID is a high-tech eID, which shows that fraudsters are also getting more sophisticated in their attempts to counter eIDs.

Businesses increasingly realise that while eIDs are a big part of the puzzle in fighting fraud, they are not a complete solution. Appropriate security step-ups in higher risk situations is an effective way to fight fraud as part of a multi-layered strategy.

Voima Gold has strengthened its ability to prevent fraud by integrating Signicat's eIDV as a step-up security measure. This allows for enhanced identity verification during high-risk situations, ensuring a secure yet seamless user onboarding experience. Read the full customer story here.

Obtaining qualified electronic signatures for high-value transactions

In the digital age, being able to sign electronically is crucial. eIDAS defines three levels of signatures. While all levels are useful, the top level, Qualified electronic signature (QES) provides a legal guarantee that is not there for lower levels and is required for many purposes in many countries. QES is the only signature level guaranteed to work cross border. Use cases can be mortgage agreements, real estate transactions, and sensitive contracts. QES always has the same legal effect as a handwritten signature, guarantees the signer's identity, and safeguards the integrity of the document. Electronic identity verification (eIDV) plays a crucial role in establishing the signer's identity for QES. While only a limited number of eIDs meet the stringent requirements for QES, eIDVs that meet specific criteria are currently approved at the national level, with EU-wide harmonisation expected by 2025.

Signicat's expertise streamlines this process, delivering secure and compliant QES solutions tailored to organisational needs.

Signicat combines its unparalleled eID Hub with high-assurance eIDV methods, enabling customers to seamlessly achieve qualified electronic signatures across Europe. As a Qualified Trust Service Provider, Signicat operates its own qualified certification authority, along with qualified time stamping and validation services, as well as sealing, storage and archiving services.

MyInvestor, a fully digital bank, has onboarded over 180,000 customers since 2017 with Signicat's identity verification and e-signature solutions. This partnership has streamlined its process, ensuring compliance with Spanish regulations while enhancing user experience. E-signatures enable quick and secure contract signing, making banking seamless. To learn how MyInvestor transformed its services, read the full customer story.

eIDAS Levels of Assurance of eIDs:

- Low: Offers a basic level of confidence, appropriate for transactions with low sensitivity.
- Substantial: Delivers medium to high confidence with thorough identity checks, suitable for transactions of moderate sensitivity.
- High: Provides the highest level of confidence through rigorous identity verification and strong authentication, ideal for highly sensitive transactions.

Digital maturity indicators

This overview provides a clear snapshot of key metrics reflecting the digital landscape across European countries, including **eID user rates** and scores from **the Digital Economy and Society Index (DESI)**. Created by the European Commission, the DESI measures digital performance and competitiveness among EU member states and Norway. It examines essential areas such as digital skills, connectivity, business tech integration, and digital public services, offering useful benchmarks for progress.

Additionally, metrics like e-government usage, access to e-health records, and the adoption of digital services by citizens and businesses help track digital maturity and pinpoint areas for improvement.

Country		eID user rate (as % of total population)	Digital Economy and Society Index (DESI) Score (2022)	E-government users, DESI (2024)	Access to e-health records, DESI score (2024) (0 to 100)	Digital public services for citizens, DESI score (2024) (0 to 100)	Digital public services businesses, DESI score (2024) (0 to 100)	Population, mio (2023)	Population 15+, mio (2023)
Austria		49% (2023)	54.7 (No.10)	79%	88.17	80.72	82.86	9.1	7.8
The Baltics	**Estonia**	84% (2024)	56.5 (no. 9)	95%	97.5	95.83	98.75	1.4	1.1
	Latvia	70% (2024)	49.7 (No. 17)	79%	84.82	88.22	87.22	1.9	1.6
	Lithuania	60% (2022)	52.7 (No. 14)	81%	95.42	86.7	95.94	2.9	2.4
Belgium		77% (2023)	50.3 (No. 16)	86%	100	82.33	91.59	11.7	9.8
Denmark		90% (2024)	69.3 (no.2)	99%	97.92	82.24	88.69	5.9	5.0
Finland		98% (2023)	69.6 (no.1)	98%	82.62	90.61	100	5.6	4.7
France		79% (2024)	53.3 (No. 12)	91%	79.27	72.09	79.31	66.5	55.2
Germany		22% (2024)	52.9 (No. 13)	62%	86.96	75.83	78.58	84.5	72.0
Italy		56% (2023)	49.3 (No. 18)	69%	82.69	68.28	76.26	59.4	52.2
The Netherlands		94% (2021)	67.4 (no. 3)	95%	72.47	85.87	86.65	18	15.3
Norway		97% (2024)	64.3 (No.5)	92%	-	-	-	5.5	4.6
Poland		67 % (2024)	40.6 (No. 24)	66%	90.03	63.73	72.88	38.7	32.9
Spain		54% (2023)	60.8 (No. 7)	83%	84.58	84.18	91	47.9	41.5
Sweden		90% (2023)	65.2 (no.4)	96%	77.94	93.28	95.97	10.6	8.7
UK		Not applicable	60.4 (2020 data)	-	-	-	-	68.6	56.7

Austria

49%

of the population used eIDs in 2023.

79%

of Austrians are active e-government users.

No. 10

in the EU on the 2022 Digital Economy and Society Index (DESI), Austria excels in e-government and broadband but faces challenges in digital skills and business tech, supported by significant investments in digital transformation.

For years, digital identity solutions in Austria were dominated by the Handy Signatur (mobile phone signature solution) and the Bürgerkarte (an eID card). But recently digital identification has undergone major changes due to the introduction of ID Austria, which incorporates a fully automated solution including biometrics for remote identity verification.

Types of eID solutions

- **ID Austria** has been available in Austria as a pilot project since January 2021 and fully operational since December 2023. ID Austria has around 3.05 million registered users (34% of the population) and provides access to over 400 connected services.
- **Handy Signatur,** a mobile phone signature solution, has been a longstanding method of electronic identification in Austria, enabling users to sign documents and authenticate their identity via mobile devices.
- **ich.app** was introduced in 2023 by PSA Payment Services Austria GmbH in collaboration with multiple banks. ich.app focuses on authentication and identification, though its adoption is still growing.
- **Bürgerkarte,** the citizen card, remains a popular eID solution, primarily used for secure online transactions and authentication in e-government services.

In the private sector, the Austrian Financial Market Authority (FMA) amended the Austrian Anti-Money Laundering Act (Austrian AMLA) in 2022 to allow fully automated biometrics for remote identity verification. Additionally, a 'liveness-check' must be conducted to determine whether a biometric sample, such as a fingerprint or face, is genuine (from a live person present at the capture point) or fake (from a spoof artefact or lifeless body part). From January 1, 2023, fully automated biometrics for remote identity verification must be combined with NFC (Near Field Communication) technology. The regulations require the use of NFC to read the electronic security chip in identity documents, combined with biometric verification such as facial recognition.

A qualified electronic signature can also be used for remote identification. The natural person needs to sign a legal declaration with the QES.

While ID Austria has a considerable user base, it is currently utilised predominantly in the public sector. There are no restrictions preventing the private sector from adopting ID Austria, apart from the necessary registration and accreditation as a service provider.

To ensure a comprehensive solution accessible to all Austrians, biometric-based electronic identity verification should be included in the mix. Fully automated processes combined with NFC technology for reading identity document security chips will empower users to conduct identity verification independently at their convenience.

Signicat in Austria

Signicat facilitates all electronic identity document verification methods: from our proprietary VideoID for automated identity verification, the issuance and use of a qualified electronic signature, to the identification via a live video interview with an agent, including the reading of the NFC-chip from identity documents.

Signicat can also facilitate ID Austria, among other electronic identities and perform data verifications in several registers. Together these services provide the best possible mix for onboarding and authenticating customers in Austria.

The Baltics

Estonia:

84%

of the population uses eIDs.

95%

of the population uses e-government services, making Estonia a global leader with its advanced e-residency programme and digital ID solutions.

No. 9

in the EU on the 2022 Digital Economy and Society Index (DESI).

Latvia:

70%

of the population uses eIDs.

79%

of the population actively uses e-government services.

No. 17

in the EU on the 2022 Digital Economy and Society Index (DESI).

Lithuania:

60%

of the population uses eIDs.

81%

are active e-government users. Lithuania is enhancing its health services information system and electronic personal ID solution.

No. 14

in the EU on the 2022 DESI, demonstrating its commitment to digital innovation and public service efficiency.

In the Baltic States (Estonia, Latvia, and Lithuania), eIDs are well-integrated into digital services. Estonia's e-residency programme and digital ID solutions are highly advanced, offering comprehensive onboarding and authentication capabilities, which have become the de facto benchmark of what has been possible for other EU member states for many years. Latvia and Lithuania also utilise eIDs effectively for secure access and transactions. The Baltic countries rely heavily on Qualified Electronic Signatures (QES), which are required for various purposes. All Baltic eIDs can be used for QES.

Estonia

In Estonia there are three commonly used identity solutions, which are deployed in a variety of use cases from voting to getting married.

- **The Estonian eID Card** is used regularly by 64% of the population and has been around since 2002. It requires a card reader and works with two separate PIN codes, one for identification and one for digital signatures. It is mandatory for all citizens.
- **Mobile-ID**, used by around 19% of the population, is a SIM card-based solution that works with most telcos that perform the initial identification of users.
- **Smart-ID** is an app-based solution that is used by more than half of all Estonian citizens; it can be used almost anywhere.

Latvia

Latvia also shows a high level of digitalisation, with over 70% of citizens using some means of electronic identification.

- **eParaksts** mobile is a mobile application issued in Latvia by SJSC "Latvian State Radio and Television Centre". As with all Baltic eIDs it can be used for authentication and document signing.
- **The Latvian eID Card** is also a certificate-based solution that works with a card reader. It is mandatory for over 15s.
- **Smart-ID** is the app-based solution that can be used anywhere in the Baltics. It is also certificate-based and used by around 75% of Latvian citizens over the age of 15.

Lithuania

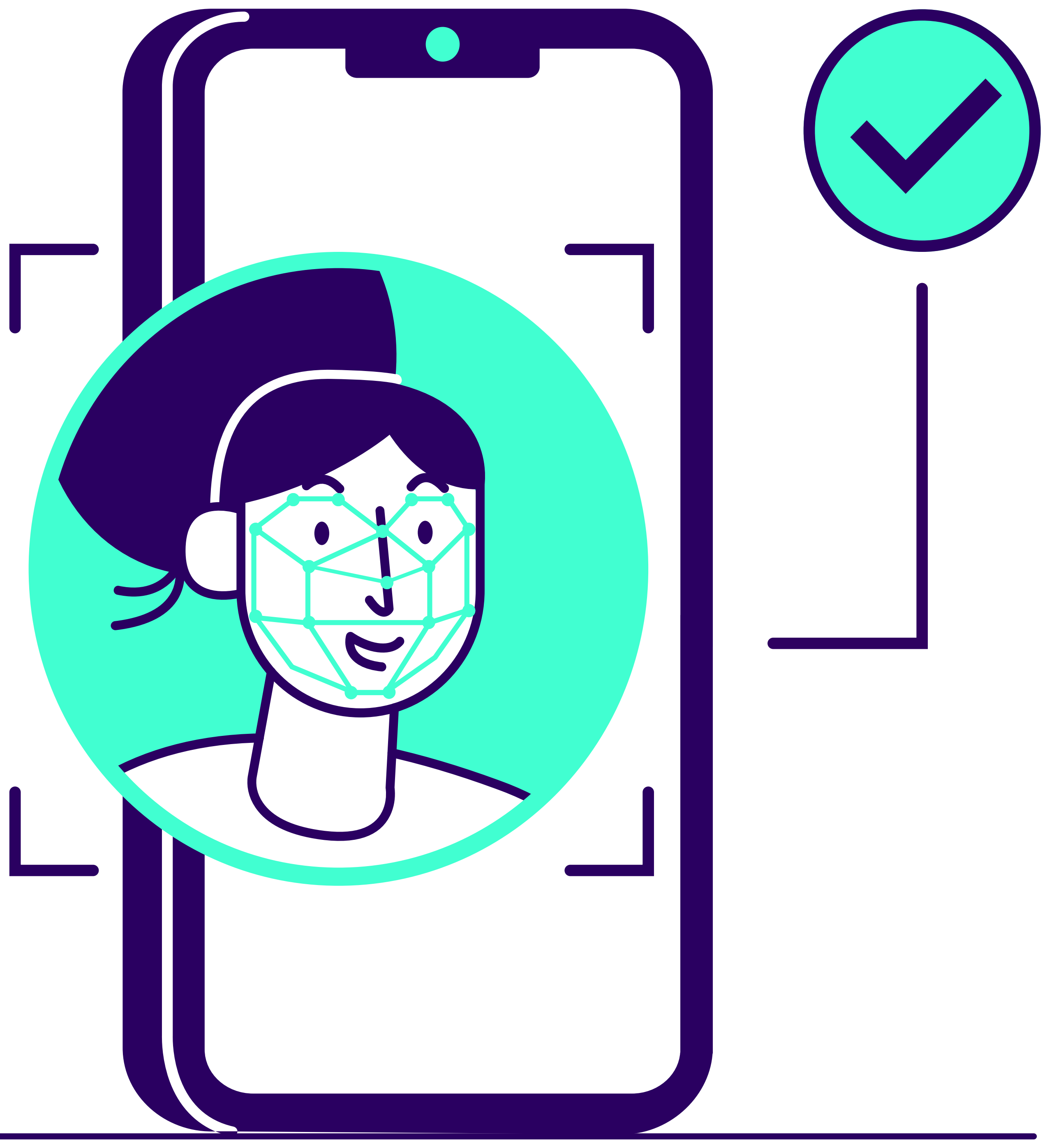
Lithuanian eID methods overlap with those in the other two Baltic countries, mainly the Mobile-ID and Smart-ID solution, both provided by the same vendor.

- **The Lithuanian eID** can be issued either as a physical card or as a USB token used in online authentication or document signing.
- **Mobile-ID** is the same solution as in Estonia, based on the secure digital identity in the SIM card. It provides strong authentication and is a method trusted by the government and financial institutions.
- **Smart-ID** is the app-based solution that also works across borders and is used by most Lithuanians.

Signicat in Baltics

Signicat has a strong presence in the Baltics, with offices in Vilnius and Tallinn since the acquisition of Dokobit in 2021. Dokobit has been an established household brand for document signing and authentication, active since 2008. The Dokobit by Signicat sign portal is used by companies, large and small, as well as individuals for securely signing documents, with the resulting Qualified Electronic Signatures being recognised throughout Europe. Dokobit by Signicat sign portal is powered by the Signicat eID Hub and VideoID.

All eID methods are supported by Signicat, both as a signing method, but also for authentication and identification through the eID Hub.



Belgium

77%

of the population in Belgium uses eIDs.

86%

of Belgians actively use e-government services.

No. 16

in the EU on the 2022 DESI, marking a drop from previous years. The country excels in digital training and internet access but needs further progress in digital public services and nationwide connectivity.

Belgium's digital identity landscape is a collaboration between the government, banks, and telecom providers, offering secure access to digital services. The country's main eID solutions are itsme app and the government-issued .beID card, both compliant with EU standards such as eIDAS. These tools enable citizens to securely authenticate, sign documents, and access public and private sector services, playing a key role in Belgium's digital transformation.

Types of eID solutions

- **itsme** is a Belgian digital identity solution, co-created by banks and telecom providers. It is widely used for secure digital identity verification and electronic signatures, with an eIDAS assurance level of 'high'. It allows users to log in to both business and government services, as well as electronically sign documents. Onboarding is simple, requiring either a bank account or the Belgian National Identity Card (eID). The mobile app provides a secure and user-friendly way for millions of Belgians to access a wide range of digital services.
- **.beID** is Belgium's electronic identity card, used for both authentication and Qualified Electronic Signatures (QES). Issued by the government, it is available to all citizens aged 12 and over, mandatory for those over 15, with a 'Kids-ID' version for younger children and a separate card for foreign residents. Users need a smart card reader and special software to utilise the card for online services. It can be used by public and private organisations; however, legal regulations prevent private entities from accessing the national social security number.

In Belgium, itsme is the most widely used identity method, including for KYC processes, and offers a user-friendly experience during onboarding and daily use. itsme has a wide range of attributes, including user's address, and offers higher conversion rates compared to BeID. Although both itsme and beID can be used for identification and electronic signatures, they are often presented together to ensure broader user coverage.

Recent developments include the entry of **SmartID**, from the Baltics, into the Belgian market. Additionally, from 2026, a new government mobile solution, **MyGov.be**, will replace beID. This alternative can be activated via itsme or the identity card, providing more flexibility for users.

As for electronic identity verification (eIDV), there are fewer use cases in Belgium due to the comprehensive attributes and high assurance levels of the existing eID solutions. However, in situations where organisations require proof of life, solutions like VideoID are a viable option.

Signicat in Belgium

Signicat offers service providers flexibility in connecting to identity services, accommodating various customer IT landscapes and allowing for the combination of services. For instance, authentication can be paired with data from the national business register.

Through Signicat's eID Hub, both itsme and beID can be integrated, alongside identity providers from many other countries. In Belgium, this enables authentication and signing at the highest assurance level. Signicat supports various protocols to connect to these services and provides access to many other solutions. Notably, Signicat's own VideoID onboarding service and MobileID technology are used by several banks and payment service providers (PSPs) in their mobile apps, offering an excellent user experience with high-security authentication and PSD2-compliant Strong Customer Authentication (SCA) for payment authorisation. Regulated industries also benefit from the company's risk management technology for AML KYC processes and fraud detection.

The proprietary automated identity verification process VideoID solution, ensures full coverage for all users, including those unfamiliar with eID solutions or don't have an eID. VideoID can also be extended with asynchronous verification by a human agent and enhanced with a QES signature.

Denmark

90%

of the population in Denmark uses eIDs.

99%

of Danes actively use e-government services.

No. 2

in the EU on the 2022 DESI. Over the years, Denmark has taken various policy measures to encourage a strong uptake of digital public services at all levels of government.

Digitisation has been a cornerstone of Denmark's agenda since the late 1990s, culminating in the launch of the country's first official digital strategy in 2001. Regular updates to national digitisation strategies have been implemented since, with the most recent one covering the period 2024-2027 introduced in November 2023.

Denmark's eID system has a single eID. The old **NemID** has now been completely replaced by its successor, **MitID**. As with NemID, MitID is the result of a public procurement process in collaboration with Danish banks. This means that the Agency for Digital Government, Digst, controls MitID contractually.

MitID was launched in May 2021. Nets won the competitive tender, continuing their core role as provider of the previous NemID. Despite Nexi's acquisition of Nets in 2020 and the subsequent divestment of the eID business to IN Groupe, MitID continues to evolve, prioritising authentication. Signing must be offered as a separate value-added service to MitID by parties, such as Signicat, who build on top of MitID.

MitID and the accompanying regulation represent a shift in Denmark's eID governance, mirroring Finland's model with a formalised and regulated broker role overseen by Digst. Private service providers are mandated to integrate with MitID through licensed brokers. Digst runs a dedicated broker for government services, NemLog-in3.

While use of a broker for Denmark's single eID solution may seem overkill, especially when compared to Finland's diverse landscape, the broker scheme offers adaptability for varying MitID use cases and minimises complexity for service providers. Despite MitID's capability to support all assurance levels, its focus is primarily on the 'substantial' level of eIDAS.

MitID's extensive functionality extends beyond basic eID to encompass a comprehensive ecosystem including extensions for professional use, MitID Erhverv, allowing individuals identify themselves as an employee of their organisation. There is also the option provided under the header of Local IdP, where company employees can use the same login and password to log into internal systems as well as external websites of service providers on behalf of their company. For an organisation to be able to issue and use Local IdP, they need to adhere to the strict NSIS standards specified by Digitaliseringstyrelsen. This caters to diverse user needs while enhancing digital accessibility and security.

Signicat in Denmark

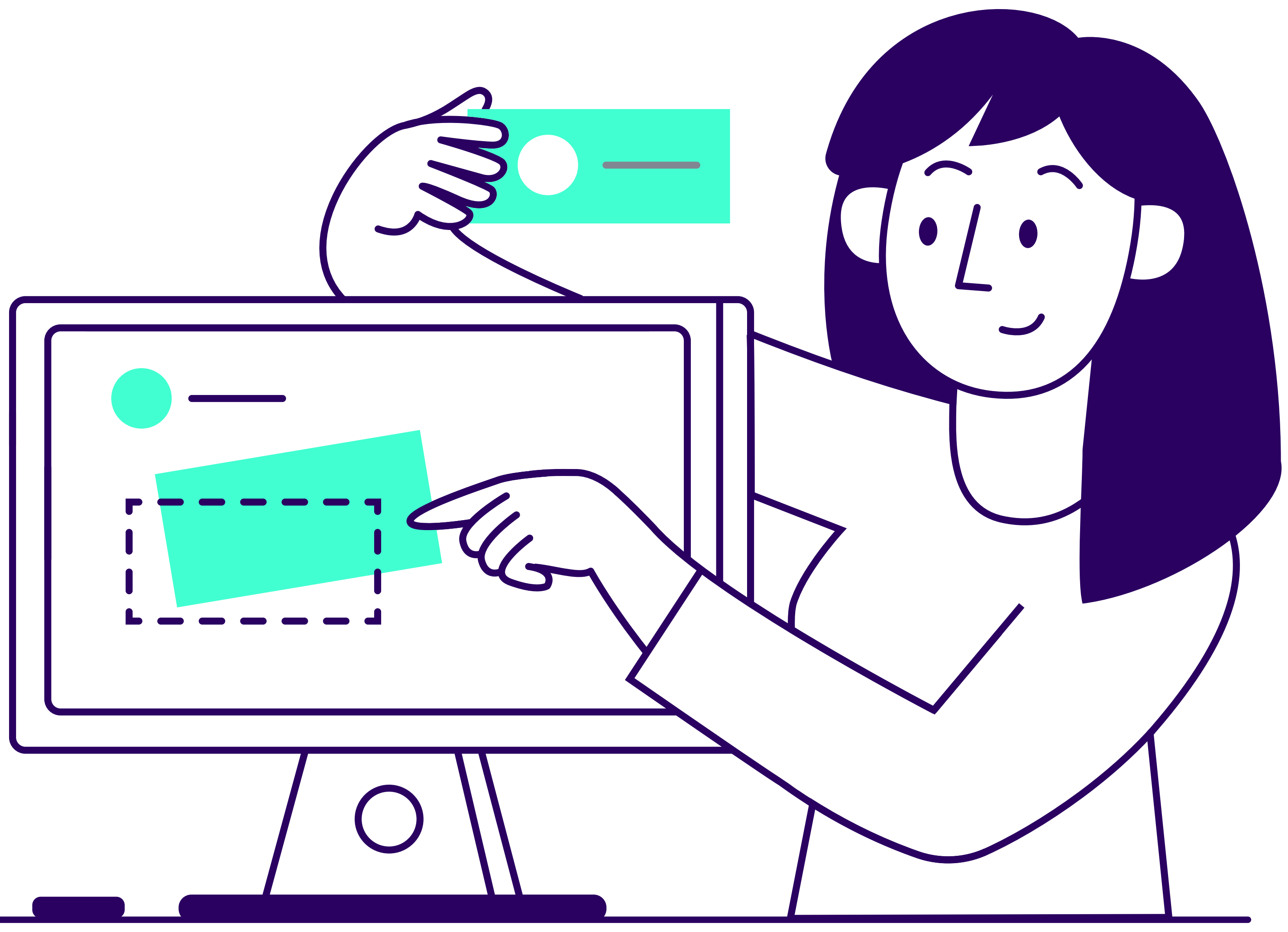
Signicat opened an office in Denmark in 2011 and has acted as a provider of NemID and now MitID ever since, particularly around the provision of signing services, authentication and data verification.

Signicat was the first organisation to obtain a broker certification for MitID and provides advanced and value-added Hub services covering all functions offered by MitID. As MitID itself does not have a built-in signing function, one of the most important value-added offerings Signicat provides is signing.

In addition to the Hub functionality, Signicat allows various ways to connect to the services. It also allows the MitID Business (Ehrverv) that can include a verification in virk.dk to find a private person with sole signing rights for a company or the business identity that is not tied to a private identity. And Local IdP, where company-issued identities can also be used for authentication and signing.

ReuseID, a white labelled solution that allows for onboarding at different levels, step-ups and supports authentication and signing, can be used by customers in need of a more flexible solution.

Signicat also offers identity proofing and data verification services in Denmark, which draws on data from population and business registers.



Finland

98%

of the population in Finland uses eIDs.

98%

of Finns actively use e-government services, positioning the country strongly to meet the 2030 Digital Decade target for online public services.

No. 1

in the EU on the 2022 DESI. It scores highly in digital skills, connectivity, and technology integration, with 82% of SMEs achieving at least a basic level of digital deployment—well above the EU average of 55%.

Finland has various eID solutions, including **Bank eIDs, Mobile ID, FINeID** and **Suomi.fi** e-Identification service for the public sector.

Finland's eID landscape is highly regulated and governed by the Finnish Trust Network (FTN), established through national eID legislation. The legislation, which was enacted in 2019 and subsequently amended in 2022, requires eID issuers and brokers in FTN to be audited and approved by the national supervisory authority, Traficom. FTN aims to ensure interoperability between different eID solutions so that Finland has a number of eIDs that work together seamlessly to benefit users and service providers, uniting a previously divided landscape.

eID issuers integrate with brokers to provide a seamless interface for service providers. The Finnish eID assurance levels align with eIDAS standards. What the FTN terms 'strong electronic identification' corresponds with the 'substantial' level of eIDAS.

Types of eID solutions

- **Bank eIDs** form a significant component of Finland's eID ecosystem, originating from collaborative efforts among Finnish banks dating from the mid-1990s. Ten Finnish banks issue eIDs approved for FTN, each offering authentication services at the 'substantial' level.
- **Mobile ID** or Mobiilivarmenne, is jointly offered by the mobile operators DNA, Elisa and Telia, and has emerged as a popular eID option alongside bank eIDs. Mobile ID has experienced rapid growth, becoming the third most-used eID in Finland. Mobile ID is also part of FTN.
- **FINeID (Finnish eID Card)** is issued by the Digital and Population Data Services Agency (DVV). It's the sole Finnish eID at the 'high' level. Employing smart card technology, FINeID includes Qualified Electronic Signatures (QES) in accordance with eIDAS standards, primarily utilised in the healthcare sector.
- **Suomi.fi** is not part of FTN and functions similarly to an FTN broker, integrating eIDs from banks, mobile operators and FINeID. It serves as a centralised buyer of eID authentication methods for the public sector, offering a wide array of identity attributes.

The Finnish government's initiative to introduce a wallet-type eID, as an alternative to FINeID, reflects ongoing developments in the eID landscape. Despite initial setbacks, Finland is piloting an experimental wallet implementation, paving the way for a Finnish European Digital Identity Wallet (EUDIW), with potential implications for government-provided eID alternatives.

Signicat in Finland

Signicat opened an office in Finland in 2013 and has provided identity services in the Finnish market ever since. Today, Signicat is the leading licensed FTN broker covering all bank eIDs and Mobile ID. Signicat has an integration to Suomi.fi that can be used by public sector customers and supports the use of the Finnish eID card.

As signing is not a functionality provided by the FTN eIDs, one of the important offerings from Signicat is providing signing as a value-added service to FTN eIDs and the Finnish eID card. In addition, Signicat offers identity proofing and a data verification service in Finland, which draws on data from population and business registers.

Signicat's own MobileID technology is used by several banks and payment service providers (PSPs) in their mobile apps. This offers an excellent user experience alongside high-security authentication and PSD2-compliant Strong Customer Authentication (SCA) for payment authorisation. A notable example is S-Pankki, which utilises Signicat's MobileID product, Encap SCA, for their FTN-approved eID. Read the S-Pankki customer story.

ReuseID, a white labelled solution that allows for onboarding at different levels, step-ups and supports authentication and signing, can be used by customers in need of a more flexible solution.

Signicat offers service providers flexibility for connection to these services, allowing for varying customer IT landscapes, and ways to combine services so that for example an authentication is accompanied by the results from the population register for that person.

France

79%

of the population uses eIDs in 2024.

91%

of the French actively use e-government services.

No. 12

in the EU on the 2022 DESI. France aims to boost digital literacy to 80% of individuals and 90% of SMEs by 2030, up from 62% and 47% in 2022. It is also advancing digital services with electronic health records and expanded digital ID cards.

In France, online digital solutions have been split between various document verification options. But in the last couple of years, the eID solution **FranceConnect** has become the unified identification service. This was launched by the French government in 2016. This framework run by the French public administration supports seven identity issuers: impots.gouv.fr account, Ameli.fr, La Poste Digital Identity, MSA, YRIS, France Identité, and TrustMe.

FranceConnect is utilised by more than 43 millions users, 1,800 online services are connected and more than 19 million French people use FranceConnect four times or more per year, primarily for accessing public services. However, the use of biometric and document-oriented solutions still accounts for the majority of identifications in France, especially in the private sector.

All seven issuers of FranceConnect provide assurance level 'low', however, only France Identité and the leading identity provider in France, La Poste, are able to offer assurance level 'substantial' through a reinforced mobile version named FranceConnect+, which is required for health services, financial flows (banks, gaming), and the processing of sensitive personal data.

eIDV can be used to enhance user verification and/or level of assurance during onboarding (e.g in the financial services sector), or for users not using an eID. For example, a basic digital identity, comprising a username, password, and deviceID, can be enhanced with additional attribute verification through eIDV, upgrading from a 'low' level of assurance, and can add value in AML/KYC processes.

Signicat in France

Signicat offers both FranceConnect and eIDV solutions in the French market to power the best possible mix for onboarding, authentication and signing. With our easy to connect platform, Signicat's eIDV services provide the right level of assurance for onboarding processes of highly regulated sectors in France. VideoID as eIDV in combination with Signicat's MobileID is an ideal solution for onboarding, step-up identification and re-authentication for many markets and use-cases.

Signicat offers value-added services such as digital signing in addition to information lookup services using external population and business registers. The company's risk management technology is valuable to regulated industries and businesses and used for example AML/KYC processes or detection of fraud.

Germany

22%

of the German population uses an electronic ID card, reflecting a significant increase from 14% in 2023, marking an 8% rise in adoption.

62%

of Germans actively use e-government services.

No. 13

in the EU on the 2022 DESI. Germany's digital metrics are around the EU average, with SMEs at 59% digital intensity versus a 90% target for 2030, and mixed adoption of digital public services.

Identity proofing in Germany has long been conducted via a video call or at a point of sale. Residents are used to being interviewed by a live agent via a video call, using their national identity card or passport to prove their identity. Post offices and even petrol stations are points of sale where an identity can be verified in person.

Legislation may act as both a catalyst and a barrier to the wider rollout of digital identification in Germany. The German government is promoting the use of the electronic identity function in the national identity card (Neue Personalausweis or nPA), particularly for public sector use cases. It is backing this with legislation to improve online access to governmental services. At the same time, though, German anti-money laundering regulations limit digital identification procedures that can be used.

The most common ways of online identification

- **Video-Ident** enables users to prove their identity via an online video interview with a live agent. However, there are drawbacks including the availability of agents and hours of operation. The method is accepted under German law for AML-compliant onboarding, but not uncontroversial as the opportunities for fraud have increased with the advent of AI.
- **Auto-Ident** is an automated identity verification process in which the identity document is captured, the holder and their liveness is verified, but not checked by a live agent.
- **Post-Ident** is the service provided by the German Post to verify someone's identity in-person at a post office. The customer receives a coupon from the company requesting their identification. With this coupon and an identity document, an employee from the post office verifies the customer's identity. The company requesting the identification will be notified and the result from the transaction will be shared via secure data transmission.

- **The eID Neue Personalausweis (nPA)** is the electronic identity function of the German national identity card. To use the eID function, the user enters their PIN to authorise the reading of the NFC-chip on the card. A growing number of use cases are being supported, particularly as federal, state and local authorities must offer their services digitally via administrative portals, in accordance with German law. However, take-up rates for the nPA are low, partly because users do not know their PIN. And to obtain a new PIN, users must visit a public administration office in person. The German government is working on improving the retrieval of the PIN code to boost the use of nPA.

- **Konto-Ident** is a method growing in popularity because of its 24/7 availability and the fact that it does not require a live interview with an agent. It goes by various names, including Account-Ident or Bank-Ident, which conform to the third AML-compliant identification option specified under German AML law (GWG Section 12 art 1, sub 3). This comprises a qualified electronic signature (QES) in accordance with eIDAS requirements in combination with a bank transfer. A video identification can be used to obtain the QES, though not necessarily with a live agent.

Signicat in Germany

Signicat offers all digital identification methods in Germany. This includes:

- VideoID is a proprietary, automated identity verification process, which can be extended with an asynchronous verification by a human agent. Signicat VideoID and QES capabilities can also be combined with a bank transfer for identity verifications that conform to German AML requirements.

- Signicat KontoID is the automated process in which a user can verify their identity, 24/7, via a guided VideoID process and execute a bank transfer in accordance with German AML requirements.

- The commonly used Video-Ident (live interview with an agent) is also available for users who prefer guidance by a human agent. Video-Ident, as described in the Bafin circular, is an identity verification method permitted for AML purposes.

- Signicat is a certified identity service provider for the Neue Personalausweis. That means we are allowed to read and share the information from the chip with respect to identity. Since the digitalisation of government services and advent of the EUDI Wallet, interest in the use of the electronic identity function within the German identity card is growing.

In addition to the various digital identification methods, the Signicat platform also offers orchestration capabilities for the best possible combination of methods. Pre-defined InstantKYC and InstantKYB for Germany, drag-and-drop flows via the Signicat Mint journey builder, or tailor-made flows are available via the RiskFlow Orchestration platform.

This enables organisations to offer more choice to their end-users, depending on customer segment and use case etc., and contributes towards conversion rates of up to 98%.

Italy

56%

of the population uses eIDs.

69%

of Italians actively use e-government services.

No. 18

in the EU on the 2022 DESI. Italy has improved its score over five years but still faces significant gaps in digital transformation. Efforts are underway to boost workforce digital skills and capabilities.

Italy has made significant strides in adopting electronic identity (eID) solutions, reflecting the country's commitment to digital transformation. By October 2021, 43% of Italian citizens had a digital identity, up from 22% in October 2020. By July 2024, 38 million Italians were registered users of **'Sistema Pubblico di Identità Digitale' (SPID)**, the officially recognised private eID.

Although an Italian citizen can have a SPID from multiple identity providers, the rapid growth in eIDs places Italy's eID adoption rates on par with France and Belgium, but still lagging behind leading countries like Sweden and Norway. The increasing reliance on digital identities underscores their importance in facilitating secure access to a broad range of services, making digital interactions more efficient and secure for Italian citizens.

Types of eID solutions

- **Sistema Pubblico di Identità Digitale (SPID)** was notified as an electronic identity within eIDAS in 2018. This eID scheme enables Italian citizens, holders of permanent residence permits and Italian businesses to access online services. Over 12,000 public administrations and 186 private service providers are active in the SPID scheme. SPID simplifies access to services such as healthcare, education, taxation, and banking by providing different levels of authentication tailored to the sensitivity of the service accessed. SPID enables different levels of assurance and attribute sets about the user to be shared, to allow the best possible solution for a specific use case.
- **CIE (Carta d'Identità Elettronica)** is a physical card with a microchip that contains the holder's personal information and can be used for both identification and authentication purposes in digital services.
- **CNS (Carta Nazionale dei Servizi)** is used for accessing public administration services. It is typically issued by regional authorities and is commonly used in healthcare and social services.

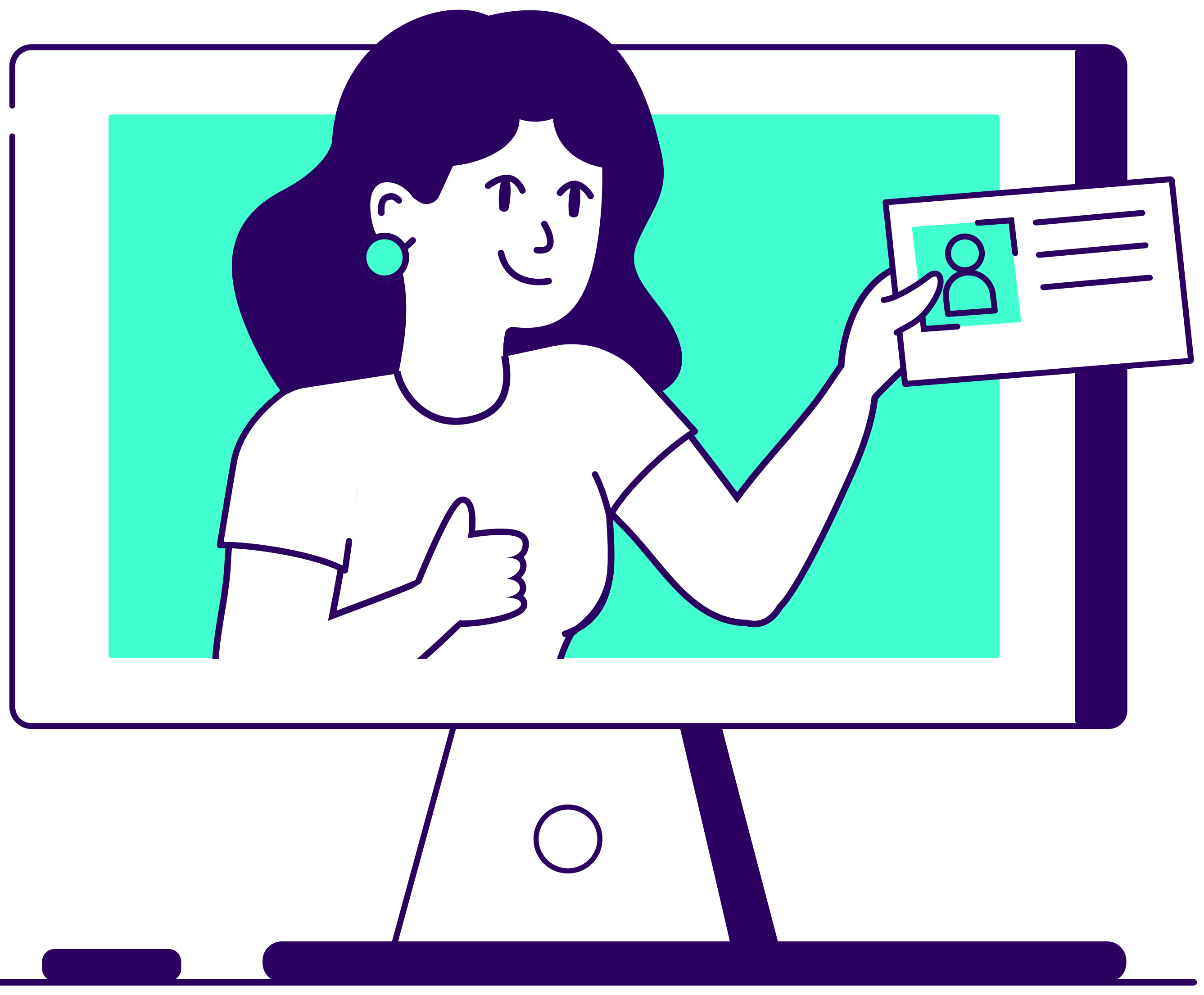
SPID, CIE, and CNS will soon be replaced by the IT Wallet. The government aims for over 34 million Italians using SPID to transition to the IT Wallet almost seamlessly by 2025, ensuring the continuity of public administration. The IT Wallet will integrate existing solutions like CIE and SPID, which will no longer exist independently by 2025-2026. While the timeline is ambitious, the IT Wallet builds on Italy's existing IO app, launched in 2020, which already supports various digital documents.

Signicat in Italy

The Agency for Digital Italy (AgID) has appointed Signicat as the aggregator for SPID, enabling end-users to verify their identity using SPID once organisations are connected to the Signicat eID Hub. No additional integration, contact, or contract with AgID is required. Signicat became the first international provider to offer SPID in September 2023.

In addition to SPID, Signicat offers robust digital identity solutions in Italy including eIDV (VideoID), providing businesses with seamless identification, authentication and signature processes catering for all levels of assurance with enhanced security, compliance with regulatory requirements, and improved customer trust.

Signicat's integration capabilities ensure a smooth implementation across various platforms, setting it apart from other providers. Its user-friendly interface and scalable solutions cater to diverse industries, from finance to e-commerce, making it a versatile choice for organisations looking to enhance their digital identity management while optimising operational efficiency.



The Netherlands

94%

of the Dutch population uses eIDs, reflecting the country's strong digital maturity.

95%

of those in the Netherlands actively use e-government services.

No. 3

in the EU on the 2022 DESI. The country excels in digital skills and has a high share of ICT specialists within the workforce. Digital connectivity is robust, with high-quality coverage from multiple fixed and mobile network providers.

The Netherlands has a long history in the digital identity space with different electronic identification solutions (eIDs) currently in market: **iDIN**, **DigiD**, **eHerkenning**, **Yivi** and most recently **itsme**. eIDs in the Netherlands are strictly divided between public and private sector use cases, principally due to restrictions around organisations permitted to process the national identity number, Burgerservicenummer (BSN).

Types of eID solutions

- **iDIN** was launched by a consortium of Dutch banks and includes identification, login and age confirmation functionality at a 'substantial' assurance level. Subsequently, digital signing functionality was added. Although iDIN provides a range of attributes, including name and address and date of birth, it is not allowed to provide the Dutch national identity number (Burgerservicenummer, BSN) and therefore only used in the private sector.

- **DigiD** is managed by Logius, a public organisation responsible for many digital solutions on behalf of the Dutch government. It is used by nearly all Dutch residents to authenticate themselves for public services, and conforms to eIDAS assurance levels 'low', 'substantial' and 'high' although 'high' is rarely used. DigiD is highly regulated due to its use of the BSN and contains no other data, so is mainly used for authentication. Lookups of other personal data are possible for public organisations via separate integrations. Recently there have been additions to include representation, where one person can act on behalf of another.

- **eHerkenning** allows users to identify themselves and act on behalf of their organisation, or even as an intermediary on behalf of other organisations. For example, an accountant or HR bureau providing specific tax or HR services to companies. eHerkenning is widely used in both the public and private sectors and provides 'substantial' and 'high' assurance levels. The eID is primarily intended for business identification, with service-specific authorisations. Although more data is available, the processing of personal user data under eHerkenning is less common but possible, dependent on purpose.

- **itsme** is a digital identification app/wallet, allowing Belgian, Dutch and citizens from several other countries to log into public and private sector organisations. Originating from Belgium, but increasingly becoming available in other countries, itsme is at assurance level 'high' and offers use cases for AES- and QES-level digital signing, login and identification. So far itsme is still primarily used in Belgium, but there have been pilots in the Netherlands as well. As the service was originally introduced in Belgium, the data provided by itsme will be different for non-Belgian users. Onboarding to itsme uses eIDV, so it is not expected to be used in combination with eIDV.

- **Yivi** started in 2012 under the name IRMA (I Reveal My Attributes). It was one of the first identity wallets in Europe. Users can prove various personal attributes in a privacy-friendly and secure manner. Attributes that can be shared include name, email or home address, plus company identification for business use cases. The take-up of Yivi remains limited.

- Several other use case- or business-specific identity methods exist including: Vidua, Datakeeper (both wallet type identities, focussing on complex use cases), Uzi-pas for healthcare professionals, Qiy, MyQii, Schluss and others. They have the potential to become more relevant under the revised eIDAS regulation with the introduction of the digital identity wallet.

Signicat in the Netherlands

Signicat entered the Dutch market around 13 years ago when it began acting as one of the six certified issuers for eHerkenning and offering a broker for various eIDs used by public and private sector clients. Signicat has integrations with DigiD, eHerkenning, iDIN, Yivi, Uzi-pas, itsme, and a bring your own IdP (Identity Provider), an access management service for user accounts registered with an organisation.

Signicat offers additional services such as verifying someone's legal representation of an organisation or of another person, and is involved in the pilot with the Dutch Digital Identity Wallet.

Signicat eID Hub offers value-added services over and above a pure broker, such as authentication-based signing and information lookup services using external population and business registers. Our risk management technology with our RiskFlow and InstantFlow products are valuable to regulated industries to orchestrate user-friendly flows for various AML/KYC-related steps or for continuously monitoring fraud. Signicat also offers a mobile identity solution MobileID that ensures a seamless user experience, including strong customer authentication.

Signicat works closely with governments and regulated private sectors, earning the trust of hundreds of organisations in the Netherlands. We provide a single, highly configurable platform, primarily managed through self-service.

Norway

97%

of the Norwegian population uses eIDs, reflecting the country's advanced digital maturity.

92%

of internet users in Norway access e-government services, showcasing strong adoption of digital public services.

No. 5

in Europe on the 2022 Digital Economy and Society Index, scoring highly on digital public services.

Norway has been using eIDs as the main digital identification method for many years now. It is used in many use cases, and by the vast majority of the citizens on a daily basis. The main eID in Norway is **BankID**[2]. **Buypass** and **Commfides** are used for certain professional and niche applications.

Regulation of eIDs in Norway is limited to self-declaration to a 'high' or 'substantial' assurance level. Supervision is provided by the national communications authority. Self-declaration is not mandatory to operate in the market, but a requirement to have an eID accepted for government services. The government has agreements with all three actors mentioned above, but only for eIDs at 'high' level.

Types of eID solutions

- **BankID** was launched in 2004. It is owned and regulated through a collaboration between the Norwegian banks. It has become almost the de facto standard for personal use cases. After the recent decommissioning of the BankID Mobile alternative, BankID is mainly based on an app, which supports two variants of BankID: BankID Biometrics at level 'substantial' and the old eID at level 'high'. BankID is one of the most successful eIDs in Europe today with a high usage, reach and support for different use cases.

- **Commfides** is a small actor providing eID level 'high', mainly in professional sectors such as healthcare. Commfides is also a qualified trust service provider for various types of certificates.

- **ID-porten** is the government's 'eID broker' integrating the eIDs of BankID, Buypass, and Commfides as well as the government's own **MinID**. MinID is the only level 'substantial' eID accepted by the government. Its main use case is youngsters applying for secondary school, who are too young to obtain a BankID.

- **Buypass** was established in 2001 and provides eID level 'high' with its main market in professional sectors, such as healthcare, accounting and auditing. It also supplies eIDs for specific sectors such as Norsk Tipping, the national gambling provider. Buypass is a leading qualified trust service provider for all types of certificates, with qualified signatures coming soon.

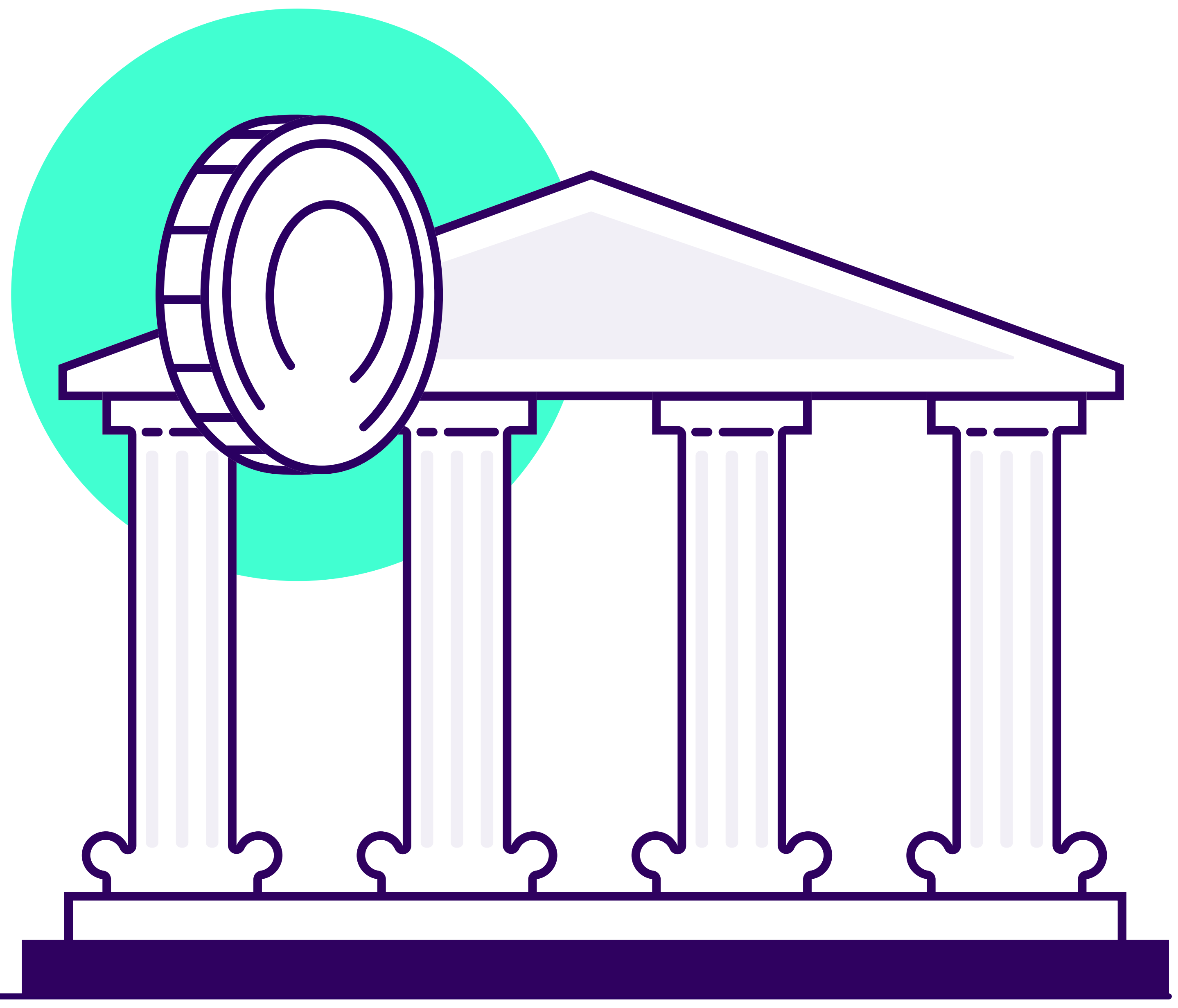
[2] Norwegian and Swedish BankID are completely different solutions although they have the same brand name.

Signicat in Norway

Signicat was founded in 2006 in Trondheim, Norway, to commercialise solutions based on BankID. Today, Signicat is by far the largest and most important BankID partner in the Norwegian market. Signicat maintains a close cooperation with Buypass in relevant areas, e.g Buypass is Signicat's partner for certificate issuing.

Signicat provides a complete service portfolio to customers in Norway, not only supporting all the eIDs and their different flavours for different use cases, but also additional services such as data verification in business or population registers. A particular strength is providing signing with eIDs that do not have this as a built-in function. This also applies to BankID Biometrics. There are different ways in which customers can connect to the services, allowing for the best possible fit to the customers' IT landscape.

ReuseID, Signicat's solution that allows onboarding at different levels, step-ups and supports authentication and signing, can be used by customers in need of a more flexible solution and can be white labelled.



Poland

67%

of the Polish population uses eIDs.

66%

of Poles actively use e-government services.

No. 24

in the EU on the 2022 DESI. Gaps in digital skills, connectivity, and tech integration remain, with only 43% of Poles having key skills (EU average: 54%). Efforts continue to bring public services online by 2030.

There are several electronic identification (eID) services in Poland, from the widely used bank-issued **mojeID**, to the official **eDO App** that is approved for use for government services and the national physical **SmartCard**.

Types of eID solutions

- **mojeID** is Poland's bank-issued eID scheme, developed by KIR (Krajowa Izba Rozliczeniowa), Poland's national clearinghouse, in cooperation with 16 major Polish banks, which act as identity providers. mojeID is eIDAS compliant (levels 'substantial' and 'high') and complies with AML requirements through the onboarding process of participating banks.

  With 98% of electronic banking users in Poland already using mojeID, organisations across Europe can have trusted interactions with almost 22 million Polish users, namely citizens and residents with a valid national identity number. They can remotely verify a user's identity via their bank details, which opens up a wide array of use cases. These include remote customer onboarding, secure logins, verification of bank details and age verification.

- **eDO App** is recognised as the official electronic identification (eID) in Poland due to its endorsement by Public Administration and Government Agencies. It is officially approved for use in accessing government services and performing secure online transactions. eDO App is closely connected to the eID Card, widely used by Polish citizens. Although the physical eID Card is still used by many citizens, the eDO App is growing in popularity as a useful eID. It offers both authentication and signing functionality, which was extended with the addition of a biometric component in 2023. The expectation is that most Polish citizens will switch to the eDO app by 2026 instead of using the Smart Card.

- **Smart Card** is a physical eID with an encrypted chip, providing secure authentication and access to various services. It ensures high security for both online and offline transactions. Most Smart Cards are now NFC enabled.

Signicat in Poland

Since April 2024, Signicat has been the first non-Polish provider to offer mojeID. We also support the Smart Card solution.

Depending on customer use case, VideoID as eIDV could be a good solution for users who don't have an eID or when face recognition or liveness checks are desired in addition to the identity data from the ID document, e.g. to verify the identity as part of the KYC process of beneficial owners, who may be resident in other countries. This can be used in combination with Signicat's MobileID solution for onboarding, step-up identification and re-authentication, either stand-alone or part of Signicat's ReuseID proposition.

In addition, Signicat offers its RiskFlow Orchestration platform, giving clients access to a large number of leading fraud, identity and AML data sources, plus helping them automate workflows that meet relevant local and global regulations. This is particularly important for anti-money laundering, KYB and KYC.

Spain

54%

of the Spanish population uses eIDs.

83%

of the population actively use e-government services.

No. 7

in the EU on the 2022 DESI, Spain improved its digital technology integration ranking, moving up 5 places from 2021. It remains a leader in digital public services, advancing in health, digital ID, and cybersecurity.

The state of digital identity is far from homogeneous in Spain, rather it reflects a variety of different approaches and systems used by government entities and private sector organisations.

No harmonised eID exists in Spain at present. If public or private organisations need a strong verification of a user's identity, several service providers could facilitate the process. The service providers capable of offering qualified services are included on the Trust Service List, for example Spanish government departments and private RegTech providers, including Signicat.

Types of eID solutions

- **Spanish National Identity Document (DNI)** and its electronic counterpart, the DNIe, are the only identity documents formally recognised across all institutions. However, take-up for DNIe has been hampered by the need for specific hardware to read the chip. Years later when NFC emerged, using an NFC reader app was not convenient and managing digital certificates for PIN unblock to access certificates was complex. This has continued to slow down the expansion of the service, giving rise to other simpler initiatives such as Cl@ve.

- **Cl@ve** is an identification and signature system (mobile app) that allows citizens to securely access public digital services. The citizen registers on the system and authenticates or signs using the app and a temporary password sent to their phone. Many public institutions have integrated with Cl@ve as a way to remotely identify citizens. Municipalities, regional governments, the Public Employment Service (SEPE), the Tax Agency, and Social Security are examples of institutions using Cl@ve.

- **IDentifica ComMadrid** is an example of a private sector initiative to create a safer and more digitised relationship between Madrid's Public Administration and its citizens. It was delivered in 2023 by Signicat in collaboration with Comunidad de Madrid and Procesia. Thanks to biometrics and artificial intelligence, citizens can identify themselves through Signicat's VideoID process by simply showing a valid ID card, to execute digital transactions.

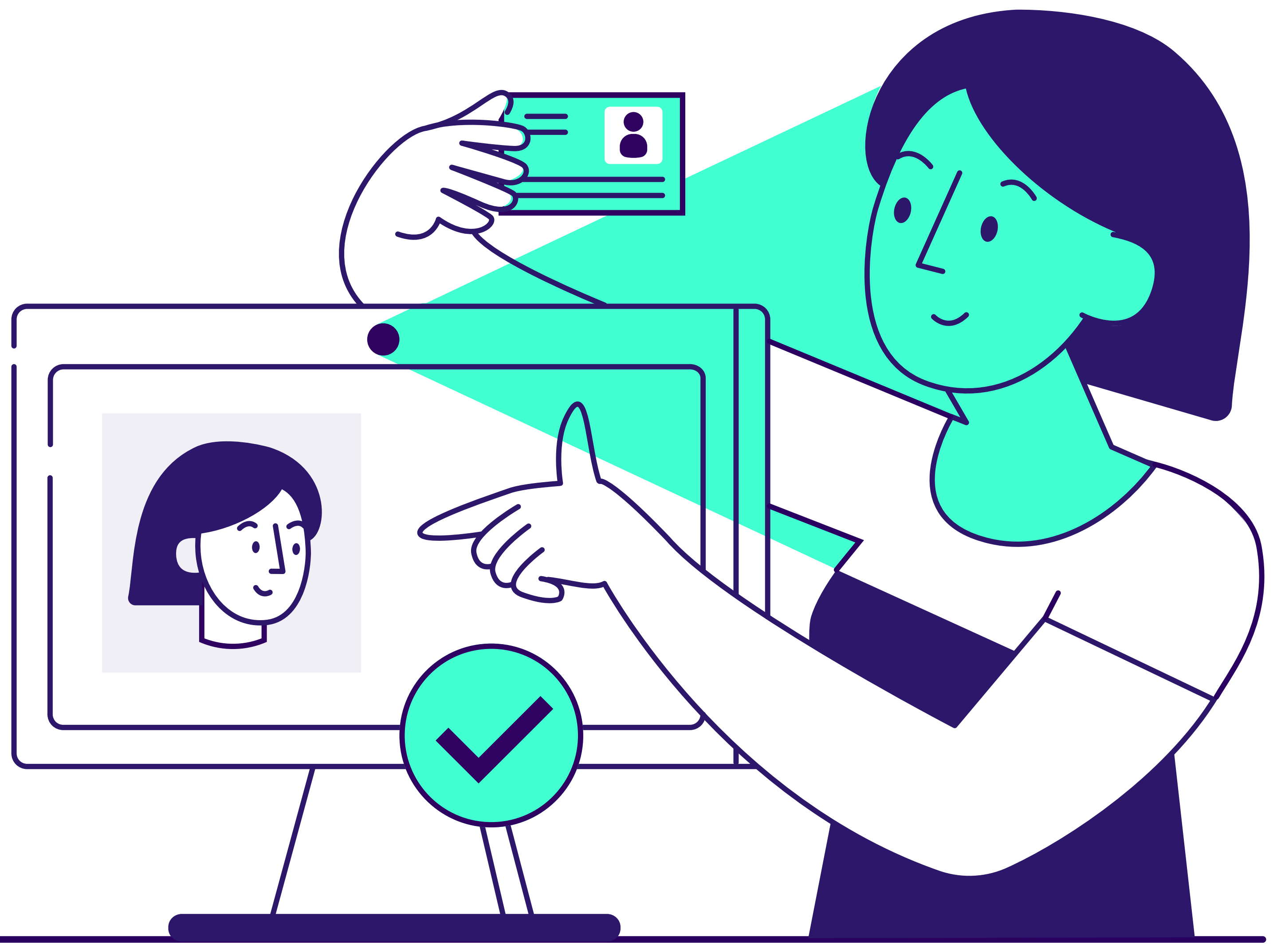
- **eIDV** is used by the Spanish private sector to enhance user verification during onboarding, mostly in the financial services sector. A basic digital identity, comprising a username, password, device, phone number, and DNI, can be enhanced with additional verification through eIDV. This upgrades the level of assurance from 'medium' to 'substantial' or 'high'. Once the eIDV process is complete, the identity of the user is considered verified and onboarding complete. Each customer then uses its own means to authenticate the user for further transactions.

Signicat in Spain

In 2021, Signicat acquired Electronic IDentification, a Spanish digital identity pioneer and a world-leading provider of asynchronous video identification services. This eIDV system (VideoID) provides a robust, scalable solution to meet the increasing demands of digital verification across various sectors.

Developed to supplement video identification, the Qualified Electronic Signature (QES) service generates a strong and fully digital eIDV and signing flow that can be used to onboard users and have them sign a document (i.e. a contract) at the highest level of assurance in the same flow. This process can be combined and strengthened with multiple other Signicat products.

Companies can create their own eID using Signicat's ReuseID solution that allows onboarding with VideoID at different levels, includes step-ups and supports authentication and signing. It can be used by customers in need of a more flexible solution and can be white labelled.



Sweden

90%

of the Swedish population regularly uses eIDs, highlighting the country's advanced digital maturity.

96%

of Swedes actively use e-government services.

No. 4

in the EU on the 2022 Digital Economy and Society Index and No. 9 in digital public services, Sweden shows high digital maturity and is well-positioned to bring key public services online before the 2030 Digital Decade target.

The digital eID ecosystem in Sweden has been dominated in recent years by **BankID**, but now **Freja eID** has established its position as a challenger. **SITHS** is an eID primarily for healthcare professionals. Players such as **Svenska Pass, ZealID,** and **Truid** are small but also contribute to the digital authentication landscape. **Efos** and **NetID** are other eIDs for professional use.

Swedish eID regulation is similar to Norway with a light regulation of private actors. Adherence to defined requirements and approval by the Agency for Digital Government (DIGG) is required for an eID to be accepted for public services. BankID, Freja eID, SITHS, Efos, NetID and Svenska Pass are approved by DIGG. Svenska Pass and Efos are the only actors approved at level 4[3], the highest level in Sweden, Svenska Pass for personal eID and Efos for professional eID.

Types of eID solutions

- In Sweden, the eID landscape has long been dominated by **BankID**, a widely used solution owned and operated by banks. Nearly 100% of adults in Sweden have a BankID. BankID is primarily app-based (other alternatives exist). Sweden has its own assurance levels for eID, where BankID is at level 3, which is close to eIDAS 'high' but is translated to eIDAS 'substantial' when used outside of Sweden.

- In recent years, BankID has faced competition from **Freja eID**, an innovative app-based alternative. Freja eID offers multiple levels of assurance from eIDAS 'low' to Swedish level 3. Freja eID has a broader reach than BankID, as it caters to citizens of multiple countries, including foreign nationals resident in Sweden, who do not have a Swedish national identification number. Freja eID also covers professional use cases, which BankID does not cover.

- **SITHS** serves as an employee eID and is primarily used in the healthcare sector. SITHS is issued by Inera AB and approved by DIGG. SITHS is closely tied to registers of healthcare professionals and their authorisations to ensure that only authorised personnel can access sensitive medical information and systems.

- **ZealID**, which has a small number of users, is the only Swedish eID to offer qualified signatures. BankID and Freja eID both provide signing but in a non-standard way. SITHS does not have signing, whereas for BankID and Freja eID signing is provided as a value-added service.

- **Truid** delivers tailored eID solutions for healthcare, finance, and government, ensuring secure access to sensitive information.

[3] The Swedish trust framework describes the levels of assurance for authentication as 1-4, with 4 being the highest. Level 4 corresponds with eIDAS level 'high', level 3 with 'substantial'.

Signicat in Sweden

Signicat opened an office in Sweden in 2008, two years after the company was founded. Since then, Signicat has had a strong presence in Sweden, offering BankID, Freja eID and SITHS for both authentication and signing. Signicat also supports different 'flavours' of the eID methods, such as executing transactions in a payment context, allowing descriptive texts to be part of the authentication, animated QR codes or initiating authentication or signing in phone calls.

Recently BankID has started to add services that Signicat also introduced, such as the ID card in the BankID app that can be used to identify the user in a physical environment, for example when an age check is needed for a parcel delivery.

Given BankID's restriction on identity switching—if a user is onboarded by BankID, the service provider must continue to use BankID for that user's authentication—eIDV is an appealing alternative to circumvent this restriction. Signicat's ReuseID provides a reusable solution for consistent identity verification across services.

In addition to the eID solutions, Signicat offers international scope and comprehensive solutions such as VideoID that allow companies to identify all users, not just those with an eID, by providing strong identity proofing solutions. The platform also supports various data verification services in Sweden, which draw on data from population and business registers.

UK

The UK lacks a national eID scheme, but eID growth is anticipated, supported by the UK Digital Identity and Attributes Trust Framework for a secure, adaptable system.

No. 11

in the 2022 UN E-Government Survey, the UK leads in e-government services. Since 2011, the Government Digital Service has advanced public service digitalisation, including online court proceedings.

According to the EU Commission's Digital Economy and Society Index (DESI) league tables, the UK ranks high in terms of connectivity but not as high as the top-tier Nordic countries.

Unlike many European counterparts bound by the eIDAS regulation, the UK has no national eID scheme and faces no immediate imperative to adopt one. Although there have been attempts to create such a scheme in the past, particularly by the government, most stakeholders have remained resistant. The Government closed down GOV.UK/Verify in 2022. Rather than a government scheme, the UK has chosen to set standards and a certification scheme through the UK Digital Identity and Attributes Trust Framework. This is still formally in review as the 2024 government change delayed the process.

A wide variety of high-quality identity verification solutions have enabled private sector organisations to verify customer identities digitally. These largely require the user to use official documents, such as a driver licence, combined with other sources proving address, credit rating etc. for an eIDV-type of onboarding. They rarely are suitable for reuse. Such systems are largely powered by the major Credit Reference Agencies (CRAs), which have compiled in-depth historical customer profiles detailing UK consumers' interactions with financial services firms. This creates a digital footprint of their identity attributes, which is overlaid with government records, such as the Electoral Roll.

The main factors that have prevented the UK private sector from developing a unified eID scheme are the complexity of coordinating multiple stakeholders, the commercial framework, and lack of compelling consumer push to deploy such solutions. Private sector organisations are also able to manage their own risk assessments and identity solutions independently, while complying with AML requirements, without the need for a national eID. Less than 1% of UK citizens use the methods available but a few are noteworthy.

- **Select ID** is one of the more recent schemes and was launched by TISA, The Investing and Saving Alliance, a membership organisation in the financial sector. The scheme ensures digital ID providers meet the regulatory guidance for AML/KYC ID proofing and due diligence requirements within financial services. The ID providers are certified to the UK Digital Identity and Attributes Trust Framework. Select ID allows consumers to choose their preferred digital ID provider. As this was recently launched (May 2024), uptake is still very limited, but it shows potential.
- **OneID** is another provider in this space that utilises Open Banking to obtain user details from their bank with the users' consent. This provides a good coverage of attributes needed for onboarding and authentication.
- Since the demise of the GOV.UK/Verify solution, the public sector services have switched to **GOV.UK One Login**. This can be used to access and use some government services and features, but the take-up and level of assurance of this email-based solution is still left wanting.

Signicat in UK

Signicat established an office in the UK in 2022 through its acquisition of Sphonic.

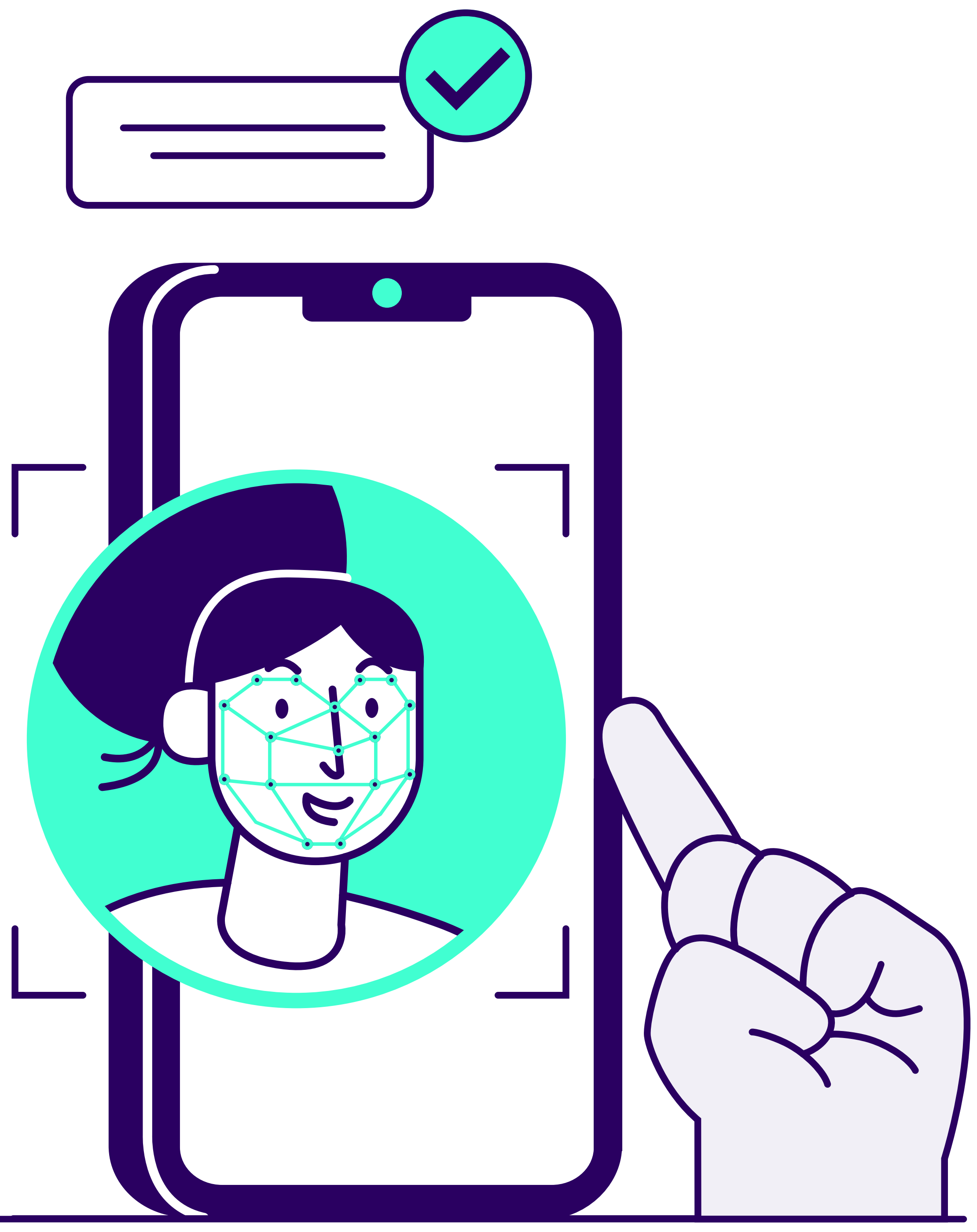
The interoperability of EU eID systems with the UK poses a significant challenge, particularly with the UK's non-alignment with the EU's eIDAS regulation following Brexit. However, UK firms have the ability to engage with European eIDs to facilitate cross-border verifications through Signicat, offering one single integration point for customers to access the world's largest eID hub of 35+ eIDs.

Signicat has the eIDVs technology (with VideoID and PictureID) to identify any individual with the desired level of assurance in the UK, plus verify/enhance/corroborate that data with 200+ data sources on its platform. Signicat can also orchestrate this process according to customer needs using our RiskFlow and Mint orchestration platforms.

With the likely growth in eID solutions in the UK through the Digital Attributes framework, Signicat will be pivotal in being able to support multiple solutions and methods, allowing firms to trial and explore such services and enable customer choice.

Specifically for the UK where reusable identities are rare, ReuseID, Signicat's solution that allows for onboarding at different levels, step-ups and supports authentication and signing. It can be used by customers in need of a more flexible solution and can be white labelled.

Signicat is part of Select ID, where we are involved in the fintech working group: TISA Digital ID Working Group.



The future of eID, eIDV and identity

Navigating Europe's digital identity crossroads: The Digital Identity Wallet

This guide is timely as digital identity in Europe is on the cusp of a great change. By late 2026 at the latest, all EU member states must ensure that their citizens have access to a free digital identity wallet. That's mandated by the recently adopted revision of eIDAS, the EU Regulation on electronic identification and trust services.

The EU Commission's goal is that 80% of the EU population will have a European Digital Identity Wallet, EUDIW for short, by 2030. The EU Commission aims for 80% of the EU population to have a EUDIW by 2030. This ambitious goal comes with a substantial budget allocated for testing the EUDIW scheme, including four large-scale pilots with a total budget of €74 million until autumn 2025. Signicat plays a key role in two of these pilots, the EUDI Wallet Consortium (EWC) and the Nordic-Baltic eID Project (NOBID). These pilots, focusing on areas like cross-border payments and travel, leverage Signicat's expertise in digital identity to test and refine secure, user-friendly solutions across Europe. Signicat is also heavily involved in the development of standards for the EUDIW.

If successful, the EUDI Wallet scheme will change Europe's identity landscape, such that most citizens will have an eID that can be used nationally and cross-border. There are great opportunities for organisations to ride the wave of interest and adoption of the new EUDIW, for example to expand internationally and attract new customers in new markets. But opportunities and risks exist in the same future.

The EUDIW won't be merely 'another eID'. It's designed to offer improved privacy and user control. It will provide a secure way to share not only identity information but also additional data, such as driving licences, medical prescriptions, and academic qualifications. The wallet can also act as a repository for payment details, airline and train tickets, and much more.

The eIDAS regulation defines three assurance levels (quality levels) for eIDs: high, substantial, and low, where the latter is not much referred to. Many European countries have eID infrastructures mostly at the substantial level, e.g. Denmark, France, Finland, Italy, the Netherlands, Poland, and Sweden. Some countries have chosen mainly the high level, e.g. the Baltic countries, Belgium, Germany, Iceland, and Norway. The EUDIW will be at a high level, and current schemes will need to consider elevating their security.

Embracing a future full of opportunities

Prediction is hazardous, so the Danish proverb goes, especially about the future. However, the fragmented digital identity landscape will likely take a while to come together. The EUDIW will coexist with other eID systems for a while, rather than become the winner-takes-all European wallet immediately. So, while the EUDIW could potentially solve eID in Europe, this may take some years and the outcome is by no means certain.

Public and private sector organisations cannot rely on the EUDIW being the only eID. They must be prepared for, and support, all the ways users may wish to access their services, namely EUDIWs and eIDs as well as eIDV systems. This involves devising a strategy and working with expert partners equipped to deal with this complexity.

Signicat is already the trusted provider of integrated digital identity solutions with a global reach in identity proofing and KYC/KYB, trust orchestration, authentication, and digital signatures. Naturally, this includes Europe and support for the EUDIW scheme.

The best way to predict the future is to invent it. Or help shape it at the very least. So, organisations are advised to partner smartly with providers, such as Signicat, who can support their present and future needs. And to think big, start small but start now.

References

1. Country overview (2023). https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Country+overview
2. Digital Decade DESI visualisation tool (2024). Access to e-health records, Digital public services for businesses, Digital public services for citizens, E-Government users https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators
3. Discover EIDAS (2023). https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
4. EID in Denmark (2024). https://en.digst.dk/systems/mitid/eid-in-denmark/
5. EIDAS Dashboard (2024). https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/ES
6. Electronic identification - The case of Finland (2023). https://www.sciencedirect.com/science/article/pii/S0740624X23000394
7. FranceConnect franchit le cap des 40 millions de citoyens connectés en juin 2024 (2024). https://www.numerique.gouv.fr/actualites/franceconnect-franchit-le-cap-des-40-millions-de-citoyens-connectes-en-juin-2024/
8. GOV.UK Verify (2024). http://gov.uk/verify
9. ICT usage in households | Statbel (2023). https://statbel.fgov.be/en/themes/households/ict-usage-households
10. INE - Instituto Nacional de Estadística (2023). Uso de identificación electrónica (eID) para acceder a servicios online por motivos particulares, en los últimos 12 meses por características socioeconómicas y tipo de servicio prestado. INE. https://www.ine.es/jaxi/Datos.htm?tpx=60760
11. KIR (2024). https://www.kir.pl/en
12. Latvia Continues to Lead in Public Service Digitization and e-Identity Usage within the EU (2024). https://www.varam.gov.lv/en/article/latvia-continues-lead-public-service-digitization-and-e-identity-usage-within-eu
13. Logius | DigiD door de jaren heen (2023). https://www.logius.nl/domeinen/toegang/digid/digid-door-de-jaren-heen
14. Majority of Lithuanian adults use SK's authentication tools (2022). https://www.skidsolutions.eu/news/majority-of-lithuanian-adults-use-sks-authentication-tools/
15. Nutzung und Akzeptanz staatlicher digitaler Identitäten. eGovernment MONITOR (2024). https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2024-eID/D21_Digitale-Identitaet_eGovMON2024.pdf
16. Runchi, M. (2024). Spid sta per scomparire: le date in cui smetterà di funzionare e cosa lo sostituirà. QuiFinanza. https://quifinanza.it/pubblica-amministrazione/spid-it-wallet-2024/803254/
17. Statista. (2024). Share of people using digital proof of identity via the internet in Poland 2020. https://www.statista.com/statistics/1218655/poland-share-of-people-using-digital-proof-of-identity-via-the-internet/
18. Strategy & (2024) eID Country Report. https://www.strategyand.pwc.com/de/en/industries/public-sector/global-eid-country-report-2024/strategyand-global-eid-country-report-2024.pdf
19. The Digital Economy and Society Index (DESI) (2022). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/desi
20. United Nations - The 2024 Revision of World Population Prospects (2024). https://population.un.org/wpp/
21. Use of electronic identification (eID) by area of use. Year 2023 - Statistikdatabasen (2023). https://www.statistikdatabasen.scb.se/pxweb/en/ssd/START__LE__LE0108__LE0108N/LE0108T80N/table/tableViewLayout1/
22. Use of electronic identification (eID) in the last 12 months, by sex and age (per cent) 2023. Statbank Norway (2021, September 23). SSB. https://www.ssb.no/en/statbank/table/14033/tableViewLayout1/
23. Vorteile der ID Austria für Service Provider (2024). oesterreich.gv.at - Österreichs Digitales Amt. https://www.oesterreich.gv.at/id-austria/Vorteile-der-ID-Austria-f%C3%BCr-Service-Provider.html#FAQ_Zahlen

Signicat

A trusted digital world

signicat.com