UBISECURE®

onfido

Europe's digital identity landscape

A report from Ubisecure and Onfido

Contents

— THIS REPORT IS BROUGHT TO YOU BY:

→ **Ubisecure** – a European specialist Customer Identity and Access Management (CIAM) solutions provider.
→ **Onfido** – a global identity verification and authentication provider.

Ubisecure and Onfido are in partnership to provide a combined solution stack for customers, whereby Onfido will effortlessly and securely verify a user identity at the onboarding stage, with Ubisecure's technology enabling seamless ongoing management of that identity.

Find out more at **ubisecure.com/partner-directory/Onfido**.

February 2021

Why is digital identity important?

Digital identity creates opportunities. To what degree an organisation embraces digital identity can greatly affect its customer acquisition and conversion rate, operational costs, and regulatory compliance. For example, utilising an existing identity can be key to optimising a customer's initial registration process, where typically **45%** of users will give up if the registration process is too complex or time consuming.

Positive consequences of digital identity best practice include:

- Enhanced user experience – also beyond initial registration to all ongoing authentications.
- Greater security – avoiding data breach and identity fraud/theft by increasing trust in user identity assertions.
- Compliance to regulations – such as GDPR with its consent management requirements.
- Privacy by design – avoid requesting and storing unnecessary personally identifiable information (PII).
- Increase operational efficiencies – digitalise otherwise support-heavy processes, like sub-user management.

Many of these benefits are further realised with the use of one or more **identity providers**, where the registering user does not need to create a new identity for the service. Rather, they connect an existing identity from a trusted third-party organisation.

VERIFIED IDENTITIES

In this report, we look at verified national-level digital identities of individuals. These are typically issued by governments or organisations that have conducted some level of Know Your Customer (KYC), such as banks and mobile operators.

There is high demand among third party organisations to leverage these verified identities for user authentication to their online services, since it offers stronger assurance that the user is who they say they are than unverified identities (such as social media logins). This is important for all kinds of services, and particularly in regulated industries and/or when creating high value accounts.

Current state of digital identity in Europe

It's no secret that the state of digital identity in Europe varies widely from country to country. The Nordic countries, where Ubisecure has its original roots, are world-renowned for their maturity in the digital identity space, with countries like the UK contrastingly slow to achieve widespread adoption of any national-level digital identity.

Here we put a spotlight on four countries – Finland, Sweden, Germany and the UK - highlighting what identities and identity schemes are in place, their respective advantages and disadvantages, and real-life use cases. This draws on Ubisecure and Onfido's long experience in deploying identity solutions throughout Europe, enabling the use of a variety of verified digital identities in both the private and public sector.

FINLAND

> Finland is seen as a global pioneer in digital identity

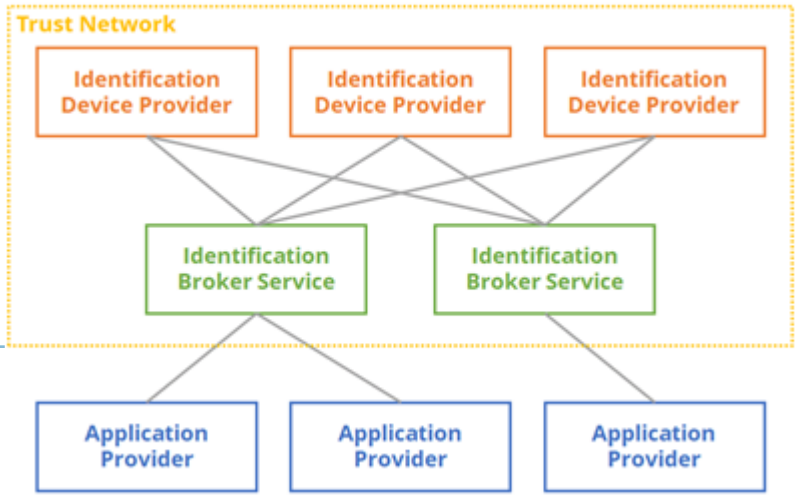
In Finland, the ability to digitally assert your identity is almost taken for granted, with its national level schemes well developed and integrated into most online services. Just as nearby Estonia is world-renowned for its digitalisation successes, as are many of the Nordic countries, Finland is likewise seen as a global pioneer in digital identity.

The Finnish government launched a nationwide identity management system to enable the strong identification of individuals and organisations. Owing to widespread acceptance of this government-led scheme, the programme saw significant uptake, ultimately resulting in a **99%** reduction in the cost of citizen interactions by moving to an online service vs. a physical point of service. Find out more in **this case study**.

Yet most of Finland's verified identities are not government-issued but originate from the private sector. They result in the secure delivery of (for example) your government-issued social security number, but the schemes are set up, managed, and delivered by large organisations, banks, telcos etc. A government-issued national identity card does exist in Finland but, in common with most national identity schemes, has adopted a PKI-/smart card-based approach, requiring non-trivial infrastructure (smart card readers) at point of use. It consequently has limited uptake.

The Finnish Trust Network (FTN) was formed in 2017 to replace TUPAS, which came to an end in October 2019 as it was no longer compliant with EU eIDAS

regulation and Finnish law. The FTN is a framework which allows application providers to enter into a single contract, with a single integration, to make use of multiple identity providers (including banks and telcos – resulting in a bank ID and mobile PKI). This Finnish scheme means that app providers don't need to make multiple contracts for their multiple identity provider needs. Instead, app providers sign a single contract with, and integrate with, a single identity brokering service.



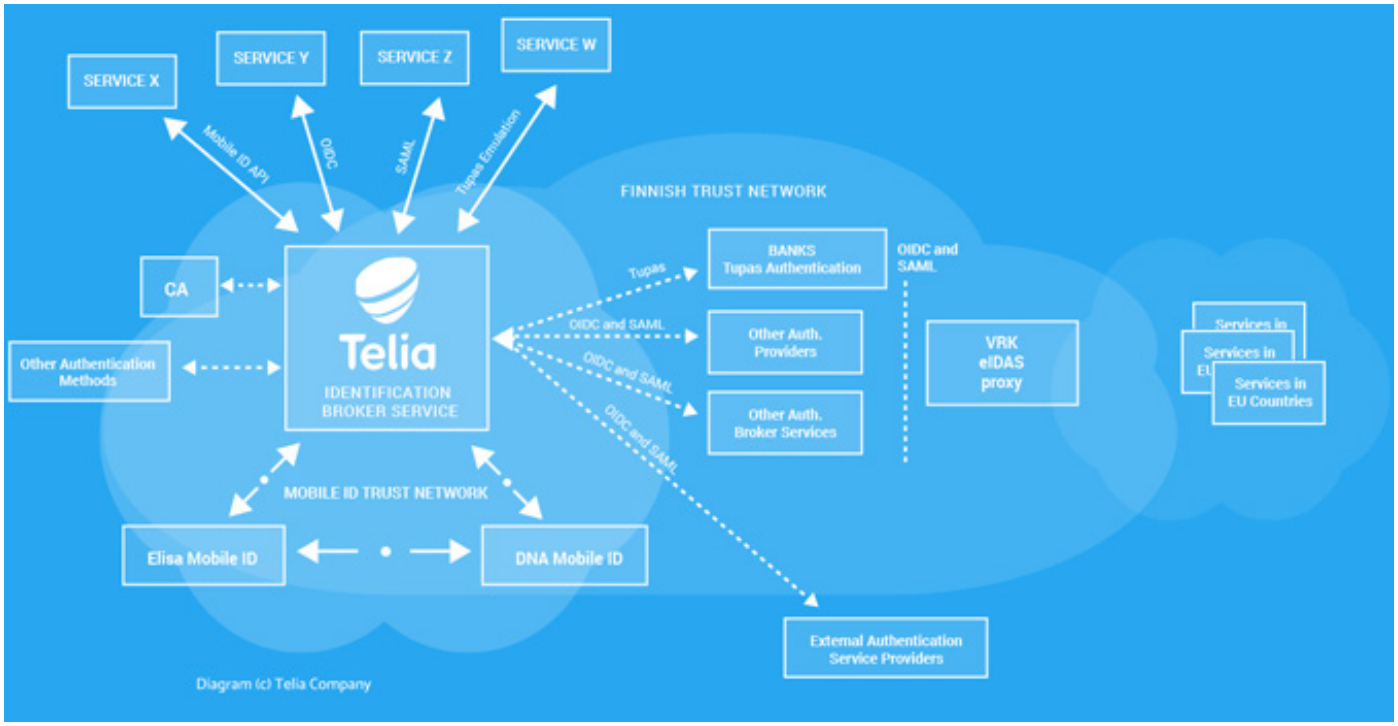
Finnish Trust Network (FTN) structure

The identity providers are required to implement multi-factor authentication (MFA) to strongly identify users, representing a verified identity which typically contains a user's name and Finnish personal identification code (HETU). The same resultant identity (and level of security) is created regardless of which identity provider is used. Identity brokers are then expected to pass this information through to application providers, which can be any service that signs up to a brokering service as part of the scheme.

The FTN is regulated by the National Cyber Security Centre Finland (NCSC-FI) at Traficom (the Finnish Transport and Communications Agency) and standardises minimum levels of data protection for users and service providers. However, one disadvantage of the scheme is that the FTN also sets the maximum pricing of each authentication, which encourages every provider to charge this (and is relatively high compared to e.g. the Swedish BankID - which we'll cover in the next section). Nevertheless, the overall costs of using the FTN are less than they were pre-FTN, and the expectation is that as usage increases the transactional cost will decrease over time.

Telia Company, a Nordic and Baltic telecommunications provider, was one of the first to take part in the FTN with its Telia Identification Broker Service (TIBS). The award-winning solution has Ubisecure's Identity Platform at its core and provides

a cross-border one-stop service for customers' strong authentication needs. Find out more in **this case study**.

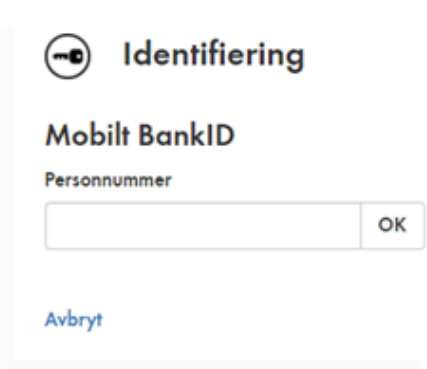


Telia Identification Broker Service (TIBS) structure

SWEDEN

> The predominant verified identity used in Sweden is BankID

The predominant verified identity used in Sweden is BankID – a solution developed by a number of large banks for use by members of the public, authorities and companies. Users obtain the ID through their bank, provided they have a Swedish national identification number, and it results in the same identity regardless of the bank that issued it. This is then leveraged by third party service providers needing identity verification. The scheme estimates that it has 8 million active users – a significant uptake given Sweden's population of 10.23 million, therefore representing almost all of Sweden's adult population.

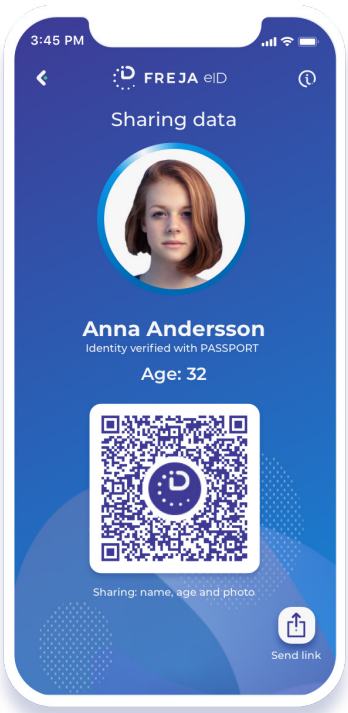


Sign in to Ellevio with BankID

One such service provider offering authentication with BankID is Ellevio, a leading national energy company in Sweden. A customer can select to log in with their BankID or Mobile BankID app, starting with their national ID number - – see screenshot.

Unlike the Finnish bank ID (FTN service from participating banks), Swedish BankID does not define the price of each authentication. This free competition means that the cost per authentication in Sweden is much lower, which is advantageous for service providers leveraging BankID for identity verification.

Freja eID mobile app



However, there are also disadvantages to Swedish BankID. Whilst Finland's bank ID can be used for account creation only – with subsequent logins authenticated via other means – Swedish BankID must be used for both account creation and subsequent logins, which could be seen as restrictive and the authentication expense needs to be paid each time by the service provider. Further, BankID has historically been difficult to broker as the banks have required contracts with the end users, not just via the brokering service, proving a barrier to greater adoption.

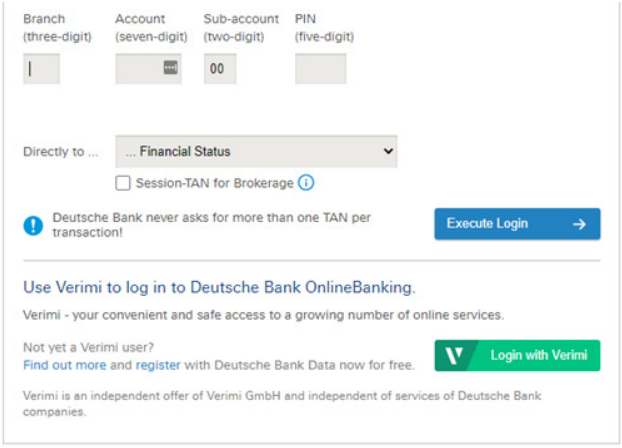
Freja eID is another well supported verified identity in Sweden. Freja is a mobile app which can be used as a personal ID in users' private and professional lives (provided their company has signed up with Freja eID). There are no public statistics on the number of active accounts, but as it holds the 'Svensk e-legitimation' quality mark - issued by the Swedish government's Agency for Digital Government DIGG – it could be better suited as a verification method for government use cases than BankID.

GERMANY

Germany is renowned as a privacy-focused society, most notably as the driver of Europe's General Data Protection Regulation (GDPR). This has meant that digitalisation has historically happened somewhat slower than in more readily "trusting" cultures, as seen in the Nordics.

> **Digitalisation in Germany has been slower than in the Nordics.**

As mentioned earlier with Finland, Germany's physical national identity card has the possibility for a digital component, but as it originally relied on the purchase of a physical card reader, uptake has been limited among users and services. Even now with the availability of a mobile app reader, the level of demand is not yet at the point of driving mass adoption.



Log into Deutsche Bank with Verimi

Other verified identities include Verimi – a joint venture of several German organisations for a portable strong identity between services, including Allianz, Axel Springer, Bundesdruckerei, Daimler, Deutsche Bahn, Deutsche Bank, Deutsche Telekom, Giesecke & Devrient, Lufthansa, Samsung, and Volkswagen.

A similar solution is yes®, which relies on bank-based authentication.

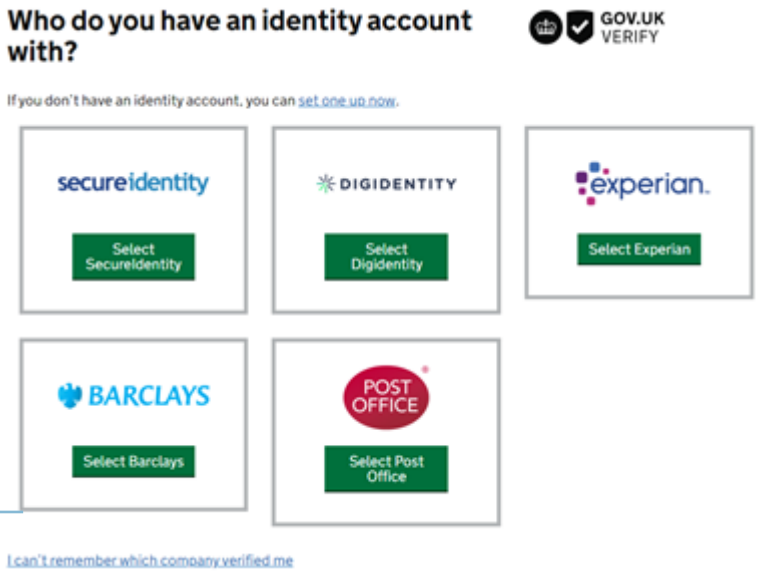
Deutsche Post (Germany's national postal service) also has its own identity scheme, POSTIDENT, in which it verifies users based on their physical identity documents, creating a verified digital identity which can then be used for onboarding in other services, such as Vodafone and Commerzbank. The eID can be created by verifying your identity in-branch or online via video chat, but always involves a Deutsche Post staff member manually checking documents (for every use) which restricts the process to working hours. Further, the in-branch option has the highest support for international identity documents.

UK

The UK has been slow to adopt any national level digital ID, with the few available schemes largely fragmented.

The UK has been slow to adopt any national level digital ID, with the few available schemes largely fragmented.

The UK government launched GOV.UK Verify (aka Verify) in 2016 as a way to strongly authenticate UK residents accessing government services. Users sign up to Verify with one of their verified accounts in one of five identity providers who already carry out advanced KYC - Barclays bank, Digidentity, Experian, Post Office, SecureIdentity. As of 2020, Barclays, Experian and SecureIdentity decided not to continue their contracts with Verify – leaving Digidentity and the Post Office as the only active participants.



Sign into GOV.UK services with Verify

The scheme has seen a very low uptake, with 7.5 million accounts as of writing in December 2020 compared to a population of 66.6 million (c. 11%). This is partly due to cultural attitudes; government led initiatives have been met with mistrust among much of the UK population over how their data will be used and

protected. Perhaps it is also in part due to the way that Verify was positioned as an optional scheme, without sufficient public education on the benefits of such a solution. There are also widespread criticisms of the Verify scheme itself. Not least, it is only aimed at identifying individuals, not organisations, which misses out on a great opportunity (see earlier Finnish government example). Even then, the success rate in verifying individuals is only **46%**.

Verify largely replaced the UK's Government Gateway – its original 2001-launched identity scheme that is still in use only by the tax authority (HMRC). The National Health Service (NHS) also has its own closed identity system. However, although it was part of the original plan for Verify, there is still no option for non-government service providers to make use of any of these verified identities for onboarding/authentication.

In 2020, as a result of the pandemic, the UK government launched a Self-Employment Income Support Scheme. With 2.6 million people making a claim, it emerged that 1.4 million of those had no prior digital identity credentials to pass through HMRC's identity verification service. With this sharp increase in demand for digital IDs, not only for this specific scheme but across all public sector organisations, a call for evidence was published around updating existing laws on identity checking to enable digital identity to be used as widely as possible. Watch this space.

Benefiting from identity verification even when digital identity schemes are not commonplace

Existing identity schemes can provide that all-important trust in who exactly is accessing your service(s) – helping you avoid costly data breaches, regulatory fines and loss of good brand reputation. Though, as we've seen, availability and adoption of identity schemes varies widely throughout Europe.

Where existing national-level IDs do not exist, either because of technical unavailability or local cultural resistance, other methods of identity verification are needed to ensure an equivalent level of trust. Without verified IDs, service providers risk unauthorised access to their service, with **80%** of security breaches caused by weak or stolen passwords.

However, to provide a best-in-class solution, identity verification should also be a frictionless experience for users, the majority of whom have good intentions when accessing your services. Not balancing security with a good user experience results in abandoned registrations and low service uptake/loyalty –

again, **45%** of users give up if the registration process is too hard.

INTRODUCING ONFIDO

To solve the challenge of disparate identity schemes, Onfido enables businesses to see the real identities of their customers. It does this by enabling a customer to submit a photo ID and selfie from their computer or smartphone. Onfido then combines the best of AI and human experts in a hybrid approach to assess if the ID is genuine, and that the photo matches the selfie.

> With Onfido, strong verification can be achieved - regardless of whether a national identity scheme is in place.

In this way, strong verification can be achieved by verifying over 4,600 document types globally, regardless of whether a national identity scheme is in place.

Onfido's analysis classifies every check as either 'clear', 'caution' or 'suspected' so a business' fraud team knows exactly what action to take. By anchoring the identity lifecycle in trust, a business can stop fraud, increase automation, and re-authenticate the user with a biometric at high-risk moments as required.

IDENTITY VERIFICATION USE CASES

Onfido's document and biometric verification brings identity fraud mitigation, as well as frictionless customer experience and reduced operational costs, to a number of use cases.

Examples include:

- Customer onboarding – make sure you can see your user's real identity, in

the form of a government ID and biometric.

- High-risk moments - an initial identity verification during onboarding creates a trust anchor, which can be used to tie a user back to their account throughout their identity lifecycle for frictionless ongoing authentication.
- KYC and AML – meet core components of your identity regulatory requirements.
- Age verification – don't rely on self-reporting, digitally extract date of birth from a government-issued ID.
- User verification – sometimes onboarding isn't the right time for verification. Step-up verification means users can opt in at any point to elevate their status (such as displaying a visual flag: blue tick/verified badge etc.)

Planning your organisation's use of digital identity

To learn more about the identity schemes that may be available in your region, get in touch with Ubisecure. We have wide experience and extensive support for the dozens of European digital identity programmes.

Where identity schemes do not exist, Onfido can help. To integrate Onfido authentication to your service, Onfido and Ubisecure provide a joint solution to enable Onfido identity verification in your service alongside ongoing management of identities with Ubisecure's Customer Identity and Access Management (CIAM) solutions.

Find out how Onfido and Ubisecure can help you leverage verified identities for strong authentication, regardless of the state of identity in your business region(s).

CONTACT US AT:

UBISECURE.COM/CONTACT

SALES@UBISECURE.COM

About Onfido

Onfido is building the new identity standard for the internet. Our AI-based technology assesses whether a user's government-issued ID is genuine or fraudulent, and then compares it against their facial biometrics. That's how we give companies like Revolut, Zipcar and Bitstamp the assurance they need to onboard customers remotely and securely. Our mission is to create a more open world, where identity is the key to access.

For more information, visit: **onfido.com**.

About Ubisecure

Ubisecure provides feature-rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS, Cloud, or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

For more information, visit: **www.ubisecure.com**.