How to Make Digital Identity a Success:
Insights and Learnings from Seven Digital ID Schemes

About the schemes

Commonalities & differences

- The schemes reveal a strong weighting toward private sector-led initiatives, with only one scheme, e-Estonia, being 100% government-led.
- All schemes aim to provide national ID services, with the exception of Verimi, which is planned to operate across borders.
- All schemes aim to deliver ID services that are legally recognised and enable secure digital transactions.
- While variations in use-cases are evident, all schemes typically focus on user authentication and digital signing services.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
Official name of the scheme	Alastria ID	itsme	e-Estonia	NemID	BankID	Verimi	Verified.Me, by SecureKey Technologies Inc.
Country	Spain	Belgium	Estonia	Denmark	Norway	Germany	Canada
Members / participants of the scheme	Cross-industry led	Bank and MNO	Government led	Bank and government led	Bank led	Cross-industry led	Cross-industry led
Format of the scheme (company, governmental body, non-profit organization, other)	Not for profit	For profit	Not for profit	Governmental body	For profit	For profit	For profit
Live since	Not live yet	2017	2002	2010	2004	2018	2019
Sectors where services are offered?	The Alastria members offer different services. Sectors include: banking & financial services, insurance, venture capital, logistics, telecoms, retail, education, legal, mining, construction. We have agreements to collaborate with treasury and digital admin- land registry, notary etc.	Four basic services: 1) Share ID data 2) Log in 3) Confirmation of an action 4) Sign documents with legally binding and qualified signature.	Multiple from governmental to municipal and private sector. Also, e-residency card program for non-citizens.	Various financial services offered by the banks, gambling sites, access to national e-post box, health information, registration of properties in official registers, tax declaration, access to self-service universe in the public sector called borger.dk, application to subsidies for students and un-employed workers.	Authentication and qualified signatures.	Verimi is an open platform and offers its services for all industry sectors, including regulated sectors such as banking & financial services, telecommunication, insurance, education, mobility, and also the public sector. Verimi provides different levels of identification and user authentication services as well as qualified electronic signatures (QES) and payment functionalities.	Verified.Me is a digital identity and attribute sharing network. The service simplifies identity verification processes.
Numbers of users (penetration of eligible population)?	Some proof of concepts deployed - not production services yet.	1,500,000 users, growing at 80,000 new users per month.	98% of the population of 1.3m citizens have national electronic ID cards (minors not included).	5.1m active users out of a population on 5.8m citizens (88%) penetration (over 15yrs old).	More than 4m; 93 % penetration (over 18 year old population).	N/A	N/A

Level of collaboration

Commonalities & differences

- Most schemes operate a collaborative model
- Typically, schemes are driven and coordinated by a single stakeholder.
- Top management has been consistently involved in both policy creation and steering of development.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
IF YES	YES	YES	YES	YES	YES	YES	YES
How is the collaboration organised? What types of organisations are involved?	Collaboration on the maintanance and development of the platform. Five people directly employed.	itsme is owned by four banks and three MNO. Banks deliver ID info, MNO's provide access to the SIM card and the secure element.	Initiated by governmental sector, but collaboration from the very beginning between government, telcos and banks. For example the Certification Authority of the PKI system has been managed by the private sector entity (banks&telcos) and once scheme was established multiple agencies and private sector actors have embraced the scheme and it has become very much collaborative.	Nets owns the Scheme apart from a few services (nemid.nu, PID, RID and LDAP search functionality). Nets has agreements with the banks and with DIGST. Nets is responsible for development, maintenance, and operation.	Solution is owned by the banks (and the mobile ID part by the telco). Collaboration between bank, telco and government.	Supported by alliance of international companies. Shareholders contribute expertise in financial services, mobility, e-government, media, telecoms, travel, technology, consumer devices.	Verified.Me is a service offered by SecureKey Technologies Inc. The Verified.Me service was developed in cooperation with Canada's major financial institutions.
At what level in the organizations is the collaboration agreed on?	Innovation departments, operations.	Board, members of executive committee.	Top executive levels in multiple governmental agencies and private sector companies.	Top level management	Board level	Board level	C-Suite and innovation departments.

How are the schemes used?

Commonalities & differences

- Authentication to e-banking is the by far most prominent service.
- Enrolment is, for the most, part performed online with e-Estonia being the notable exception; this is also only scheme providing physical token (identity card) to represent digital identity.
- Existing banking credentials are being widely used as the principal means of initial identification.
- The inclusion of access to health records, together with other governmental services like taxes and benefits, is notably supported in the Nordic markets of Denmark and Norway, unlike elsewhere.
- Approaches to managing costs vary. Norway's BankID used cost savings as an initial jumping off point, whereas the government-led e-Estonia scheme mandates that users pay €25 charge at a police station in order to obtain the validation required to enrol. It is also important to note, however, that in Estonia's case the physical identity card provided is also a valid travel document.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
Which services, enabled by digital ID, are used most frequently?	Not live yet	Transactions: 33% Gov, 66% private Public sector: Authentication. Private sector: KYC, Bank & insurance login, payment orders & payment confirmation and document signing. Operator: KYC, Subscription change, helpdesk. Health: access to sensitive data	Online/mobile banking - 99% banking services apply digital ID. Digital signatures feature heavily. - Social security services, including e-prescriptions and I-voting (44% of users voting applied digital identity in the last elections). - 99% of public sector services can use e-identity. - 67% of the citizens actively use digital ID cards. - Loyalty features available on digital ID identity cards. Merchants integrate loyalty schemes.	Total number of transactions pr. month: 70 m Bank: 40 m equivalent to : 58% Private: 15 m equivalent to: 21% Public: 15 m equivalent to: 21%	Private sector most popular. - Authentication to internet banking & payment services. - Access to different bank accounts. Same digital ID applicable to governmental services. Govermental services in second place. -Customer authentication. - Users can alter destination account for receipt of government money and order doctor appointments and prescriptions. - Government uses digital postbox to send information to the public e.g. military information to youth, cancer registration and health checks etc.	Private services established, public services in development. - Customer account creation, e.g. transfer of verified data in regulated sectors (AML-compliant onboarding) -Account aggregation - Secure single sign-on, inc. bank account login, customer accounts etc. - AMLD and eIDAS-compliant ID and verification to facilitate "one-click registration" - Authentication, incl. PSD2 compliant 2FAaaS. - Payments (guaranteed direct debit). - Digital signatures, incl. qualified electronic signatures (QES).	N/A
What are the reasons for users (consumers / businesses) to use digital ID instead of physical services or other means?	All members can create services they believe will be useful for their customers.	**New services:** corporate access management for remote working, IoT (not really protected today). Today people are using Itsme to make their lives easier.	Digital identity allows for attributes, which pysical ID doesn't. **New services:** public transportation and parking, significant cost-benefit in e-banking	Mandatory consumer adoption due to public sector digitalization (to reduce cost). Broader, more convenient access delivers a win – win situation. Mandatory Digital Post services for citizens and business is an example of the digitisation initiatives.	Digital services are more efficient and available 24/7.	Convenience for consumers (B2C) and conversion for businesses (B2B). **New services:** Digital/online verification services and improved digital processes (one-click registration) facilitate simplified customer on-boarding and check-out procedures, via stored and re-used (verified) digital identities.	Time savings. Increased privacy, security and convenience.Seamless UX that is as safe as it is easy to use. Cost savings (for service providers). 50% reduction in onboarding process, tens of millions saved if 15% shift service provider interactions from physical to online.
What was the focus of the product launched – providing services to businesses or to consumers?	Enabling businesses to provide services to consumers - businesses first.	Consortium of big players. You need a few big use cases – banking use cases and the government. Once you have the number of users, you can start attracting new partners.	Both	Consumers to get the critical mass of user in the system.	Both, but we have more services to consumers than to businesses.	Both, businesses and consumers (two-sided market).	Businesses first?
Enrolment processes; how is it done, what requirements?	Enrolment via one of the services providers on Alastria.	Completely mobile process, rooted to banking app. Confirm identity info via bank credentials. Choose PIN code and activate with touch and face ID.	Obtain five year validation from police, costing 25 EUR. Re-applying can then occur online. Minimum age: 15 yrs old.	Remote and physical enrolment is done based on KYC.	Through internet bank customer proofing. Physical presence and a valid passport is required. The customer data is verified though the bank's customer database and/or Norwegian citizens registry. BankID Merchant certificate obtained via an online portal provided by Vipps (former BankID Norge). Bank issues based on the required KYC and AML.	Account creation completed online, login requires username password. Consumers and businesses can choose from a selection of different online identification services, i.e. eID, (e.g. new German ID card), Video-Ident, Bank/AML-Ident (re-use of existing identification), as well as auto ident and photo ident for use cases that do not require AML compliance.	Download the app or use within a web browser, and follow a step-by-step process for users to connect with their financial institution.

Marketing

Commonalities & differences

- With the exception of Alastria, all schemes see the value in branding the scheme as an individual entity. e-Estonia has established both local and international brand names which it says has assisted in raising awareness of the scheme.
- Broad variations in the schemes approaches to marketing are apparent, ranging from no requirement at all (due to participating stakeholders managing the communication) to fulsome marketing designed to drive adoption.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
Does Digital ID require a unique brand name? (e.g. creating a separate entity like Itsme in Belgium and branding under that name)	Don't know - too early to take a view.	Yes	Yes. There are international and local brands that have helped establish the service.	Yes	Yes	Yes	Yes
Do you run any marketing for the Digital Identity? Or for the services enabled by Digital Identity?	Alastria members to do the most marketing by positioning the service with their customer.	Position the brand but no marketing campaigns have yet been done. Partner enrolment and support raises awareness.	Some - aimed at the 1/3 of the population that are not using the electronic identity cards. Also some marketing for new services, like i-voting and for e-residency.	None. The banks and DIGST communicate about the solution. Nets supports these activities and communicates to private service providers.	Some - recently for digital signing to engage youth and create critical mass.	Yes, for digital ID as well as connected use cases at the side of our partners through advertising campaigns.	Fullsome marketing and communications to launch Verified.Me. Success relies on consumers signing up for and using the service. Marketing is a key vehicle to achieve this.
Who would be the right target groups for the marketing (consumer, service providers)?	Service providers.	Unspecified. So far the scheme has more demand for business partners than it can handle.	Consumers and service providers.	Both consumers and service providers.	Primarily consumers and then service providers.	Consumers and service providers.	Consumers and service providers.
What is the main focus in marketing? Usage/brand/simplicity/?		N/A	Usage and benefits.		Simplicity, security and use cases. Your digital identity (passport).	Conveying convenience and security as well as trust (e.g. no tracking, no data selling).	Education on the service

Monetisation

Commonalities & differences

- All schemes rely on service provider fees for commercial support.
- None directly monetise user data, however, some provide identity data to merchants to enable ID verification. Verified.Me acknowledges that trusted third party service providers may monetise this data subject to informed user consent.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi GmbH	Verified.Me
What is the business model you are using – per use fee, (monthly/annual) subscription fee, per transaction or other models?	Not for profit. The network is free for members until a certain level, analyzing if then members must pay per transaction. Membership fees – NGO & academia free of charge, €500 (startup), €5000 for medium sized companies, €10 000 for large.	Service providers bear the cost. Customer per-transaction fees were trialled then dropped - they detered engagement. Annual subscription model for for unlimited usage now opted. The range of fees is large: the scheme has a regressive tariff depending on the number of users.	Government invested in the infrastructure (ID card issuance, public service acceptance, underlying IT). Est. 2% GDP saving annually. Certification body charges fees from banks and service providers on a per query basis.	Private Service Providers pay 0.13 EUR pr. transaction or 0.43 EUR per user/year. Public and banking sectors have specific contracts and pay for development, maintenance and operation.	Vipps handles sales and distribution to merchants and public sector service providers. Transparent price list for merchants inc: certificate, monthly subscription and transaction fees. public sector pricing agreed via dedicated service contracts.	Fee for business users (var. monthly + per transaction). One-off compensation for ID providers (per user), when contributing an identity to the platform.	The application is free for consumers to download, through their App store or Google Play. Data rates may apply.
Who pays for the service: consumer, service provider or others?	Service povider	Service provider	Service provider	Service provider	Service provider	Service provider	Service provider
Are you monetising data, any examples?		No. As a Trust Service Provider there is potential to enrich data capture, but not to monetise.	Not for governmental bodies. Private sector can collect information e.g. on logins to banking services, but it is not known whether this data has any relevance for monetization.	No	No.	No.	No neither collecting nor monetising consumers' data. Trusted connections may collect/monetize but only with user's informed consent.

Cross border potential & regulatory considerations

Commonalities & differences

- All schemes based in Europe must abide by EU regulations including GDPR, eIDAS, PSD2 SCA, AML5 and others. Verified.Me operates according to Canada's Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).
- All schemes must also operate in compliance to domestic regulations.
- Nordic schemes have been specifically designed to be domestic-only services. Others have either been designed to be open to cross border integration, or are exploring their potential.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
Did you consider this to be cross-border? If so how?	Focused on Spain, but blockchain is innately cross-border. Alastria is a member of EC's International Association for Trusted Blockchain Applications (INATBA) and is participationg actively on EBP's EBSI project in particular as coconvenor of ESSIF (European Self Sovereign Identity Framework) use case.	Conceived initially as a national initiative but developed with cross-border potential. Test market will be Luxemburg. Also looking at other markets in Europe.	In the beginning designed for Estonia internally only; step by step by adjusting the Estonian file type carrying signatures to an internationally adjustable format the crossborder aspects became more relevant. Compliant with EU regulation, including eIDAS.	Not applicable - Danish solution.	Not applicable - Norwegian solution.	National scheme but potential to internationalise.	Has plans to launch the service in countries outside of Canada.
Are there cross-border aspects to be considered? Challenges?		How to establish critical mass in the new market? Finding common use-cases and positioning for adoption.	Maturity of the infrastructure and acceptance varies within EU. Some countries are more private sector driven and others public sector.	Compatibility issues in tech, standards, civil registration numbers, assurance levels, evaluation criteria. Culture and historical issues impact cooperation and trust in governmental institutions. Local presence also needed.		Challenges include: • different applications of eIDAS regulation. • different national regulatory requirements. • different national ID-documents. • different status quo of digitalisation of public sector services.	Identity is sovereign: every country wants service to be accountable locally rather than via an offshore corporation. Second, identity is cultural: what works in one country will seldom work unchanged in another. Understanding the nuance in identity management between countries is key.

Technology choices

Commonalities & differences

- All schemes have based their solutions on either Public Key Infrastructure, or blockchain technology.

	ALASTRIA	ITSME	e-ESTONIA	NemID	BankID	Verimi	Verified.Me
Have you made technology choices for your scheme?	Blockchain	Public Key Infrastructure and Open ID Connect protocols. Utilises the secure element.	Public Key Infrastructure, utilises SIM secure element and IOS/Android. Cards have RFID capablilty.	Public Key Infrastructure	Public Key Infrastructure	Public Key Infrastructure	Verified.Me is built on top of the IBM Blockchain Platform which is based on Linux Foundation's open source Hyperledger Fabric v1.2, and will be interoperable with Hyperledger Indy projects. Industry-standard federation protocols.
Was technology a factor in your decision to implement your scheme?	Yes, to provide a secure and privacy enforcing solution.		Yes, but services, security and simplicity were also driving factors.	Yes – it was important to encompass the requirements from both the banks and the government.		No	Yes Blockchain is a key factor in providing trust, privacy and security.