GIVING VOICE TO DIGITAL IDENTITIES WORLDWIDE

KEY INSIGHTS AND EXPERIENCES TO OVERCOME SHARED CHALLENGES

2021

SECURE IDENTITY ALLIANCE

onepoint.
beyond the obvious

PRODUCTION OF THE REPORT

This report has been produced by the Digital ID Working Group of the Secure Identity Alliance (SIA) and the onepoint team:

Members of the SIA Digital ID Working Group:
Kristel Teyras, Thales (Chair)
Marie Sophie Bellot, Pavlina Navratilova, IDEMIA
Olivier Dussutour, INGroupe
Fabian Bahr, Giesecke+Devrient
Mike Edwards, Veridos
Eric Piroux, Entrust
Andreas Zechmann, OSD

Members of the onepoint team:
Marie Alice Manderscheid, leader
Helene Le Héricy, leader
Corentin Marsily, consultant

RIGHTS AND PERMISSIONS

PHOTO CREDITS

Front cover:
Photo by Carson Arias on Unsplash

Additional:
Photo by Omar Albeik on Unsplash
Photo by HONG LIN on Unsplash

Back cover:
Photo by NeONBRAND on Unsplash

CONTENTS

EDITO 6

INTRODUCTION 9

Key terms and definitions 10

INSIGHTS 13

Insights overview 14
End user value propositions 16
Ecosystem & governance 24
Technology implementation 30
Go to market & promotion 36

INTERVIEWED COUNTRIES' DIGITAL IDs SCHEMES 43

Studied countries in Europe 44
Studied countries in Middle East & Pacific Asia 46
Studied countries in America & Africa 48

Australia, Queensland - Digital Licence App 50
Austria - Citizen Card and Mobile ID 52
Azerbaijan - Asan Imza 54
Canada - Verified.Me Identity Network 56
Colombia - New eID card and Mobile ID 58
Denmark - NemID and MitID 60
Estonia - e-Identity 62
France - FranceConnect 64
Italy - SPID 66
Liechtenstein - eID.li 68
Netherlands - DigID 70
Nigeria - NIN and Mobile ID App 72
Portugal - Chave Móvel Digital and Citizen Card 74
Singapore - National Digital Identity 76
United States, Arizona - MVD solutions 78

ADDITIONAL COUNTRIES' DIGITAL IDs SCHEMES 80
Belgium - ItsMe 81
Brazil - CPF ID Wallet App 82
India - Aadhaar 83
Latvia - eParaksts 84
Oman - Omanuna 85
United Kingdom - Gov.UK Verify 86

ACKNOWLEDGEMENT 89

EDITO

Stéphanie de Labriolle, Public Affairs & International Relations, SIA

Delivering on the promise of digital ID

Providing insights into how governments around the globe are unlocking the potential of digital ID to support the delivery of innovative and inclusive services for citizens, this unique global study reveals the guiding principles that are key to success.

As a not-for-profit global identity and secure digital services advisory body, Secure Identity Alliance (SIA) brings together public, private and non-government organizations to foster international collaboration, shape policy and provide technical guidance. We are committed to the sharing of best practice in the implementation of identity programs.

With demand for government issued digital ID schemes continuing to escalate, we commissioned this study to uncover the lessons learned from real-life digital ID deployments around the world – exploring the opportunities, the challenges, use cases, and what makes a winning strategy.

In partnership with onepoint, a consulting firm that enables public administrations to successfully architect their digital vision, we conducted research with stakeholders from 25 sovereign digital ID schemes around the world to identify the important questions governments will need to consider as they shape the course of digital ID programs in their countries.

Our findings show how, regardless of the digital ID ecosystem model that is adopted – centralized or federated– a number of common themes and guiding principles proved critical for driving usage, adoption and success.

Alongside highlighting global examples of best practice, we hope the insights contained in this study will enable governments to develop digital ID programs that are safe, accessible, and socially beneficial – together with the policies that support and foster good digital ID.

Kristel Teyras, Chair, Digital ID Workgroup, SIA

Digital identity – learning from others

Around the globe, digital ID projects are gaining momentum. From identity to driver license and e-passports, physical documents are digitalising onto mobile at fast pace.   Those new forms of digital ID are enabling us to access critical public eServices and health records, travel, conduct business, onboard new service providers and protect our identity in every part of our daily life.

Responsible for driving the development and adoption of secure, trusted, effective and inclusive services, the SIA Digital ID Working Group is at the forefront of guiding governments on how to enable secure ID and verification mechanisms and establish the technical specifications for the creation of digital identities.

The recent COVID-19 crisis has further strengthened the case for digital ID schemes that allow citizens to prove their identity and seamlessly access public and private sector services digitally. This research provides the critical insights governments need to inform their strategies as they prepare to accelerate national digital ID programs and 'build back better' after the pandemic.

With the uptake of digital ID now at a crucial tipping point, mobile ID is set to become the primary source of digital ID onboarding, verification and authentication for over 3 billion people by 2024.[1] Next generation mobile ID technologies that support both online and in-person identification are already helping to propel pro new era of innovative trusted ID services that are redefining how people interact with public authorities and private sector players.

To deliver on the promise, however, the findings from this research highlight the vital importance of initiating mobile ID schemes that are built on a robust and trusted digital identity framework.

Yannick Ragonneau, Partner, onepoint

As transactions move from the physical to the digital world, trusted digital identity is now the cornerstone of a new and growing range of public services. In this report, we give voice to the leaders of the most innovative and challenging identity-led projects across the world – leveraging their 'on the ground' insights and perspectives to help public and private policy makers understand the art of the possible, and to inform and shape their own programs.

Working in collaboration with the Secure Identity Alliance, onepoint identified 25 diverse identity projects around the world and conducted one-to-one interviews with the program leaders. We wanted to do more than simply report on their programs, we wanted to understand their unique design and deployment challenges, the individual success factors and, with multiple paths to delivering Digital ID, why they chose their particular route forward.

This approach, we believe, offers a much richer source of insight for both public and private organisations – particularly with the speed of evolution, and as governments seek to develop platform approaches that open up information systems to an extended ecosystem of third party providers.

Having conducted and analysed these expert interviews, we brought these learnings together to develop 13 key insights to inform policy-making across the planning and deployment lifecycle: from end user value proposition and ecosystem and governance, to technology implementation and go to market and promotion.

Ultimately, the continued evolution of the digital ID market, and the success of the numerous public and private programs, relies on the ability of the entire community to effectively collaborate, share best practices and learn from one another. By giving voice to digital identities around the world, we hope this report will contribute to this effort.

[1] *Juniper Research, Why Digital Identity Is Critical To Post-Pandemic Society, Nick Maynard and Susan Morrow, 2020*

INTRODUCTION

A HANDS-ON FEEDBACK AND BEST PRACTICES BASED STUDY

The Secure Identity Alliance (SIA), in partnership with onepoint, combined their competencies and experience to produce a global study on national digital and mobile identities worldwide : **"Giving voice to digital identities worldwide, key insights and experiences to overcome shared challenges".**

The SIA and onepoint consider Digital Identity as a **driver for social and economic inclusion, an opportunity to provide equal, fast and convenient access to public and private services.** As such, focus and priority was given to national Digital and Mobile Identities that are **government-driven and/or government regulated.**

National Digital ID schemes vary by country based on a multitude of criteria such as cultural specificities, structured ecosystems and governance, technological infrastructure, legal and institutional framework, security and privacy requirement, etc. Well aware that there is no "one and unique" digital identity scheme to replicate and implement, there are **best practices and useful insights** that can be shared.

The aim of this report is twofold:

1 **Highlight the Digital ID schemes specificities,** deep dive into **innovative use cases, governance & processes, technological choices, and go-to market strategies.**

2 Understand the **drivers and rationale** that underlie the decision-making, and benefit from **hands-on feedback and best practices** from key actors.

THE INSIGHTS THAT HAVE BEEN IDENTIFIED ARE BASED ON SIA AND ONEPOINT'S RETURN OF EXPERIENCE, OFFICIAL AND DOCUMENTED ANALYTICAL SOURCES, AS WELL AS A CROSS ANALYSIS OF 25 INTERVIEWS WITH KEY INTERNATIONAL ACTORS AND COUNTRY REPRESENTATIVES. GIVING VOICE TO COUNTRIES' AND ORGANIZATIONS' EXPERIENCES WAS A LEITMOTIF THROUGHOUT THE ENTIRE WORK EXPERIENCE, AND IT WAS ESSENTIAL THE REPORT REFLECTED THIS PREFERENCE.

PRESENTATION OF BOTH STRUCTURES

SECURE IDENTITY ALLIANCE

A not-for-profit organization, the Secure Identity Alliance brings together public, private and non-government organizations to foster international collaboration on the provision of legal and trusted identity for all and the development of inclusive digital identity services necessary for sustainable, worldwide economic growth and prosperity. Its Board Members are IDEMIA, IN Groupe, Thales and Veridos.

www.secureidentityalliance.org

onepoint. beyond the obvious

Onepoint architects enterprise transformation accross companies and public agencies, guiding its clients from the definition of the strategic vision to its technological implementation. Onepoint has been appointed to provide its views and experience on innovative Digital Identity models worldwide.

https://www.groupeonepoint.com/en

KEY TERMS AND DEFINITIONS

DEFINITIONS

Attribute sharing

Attributes can be disclosed along with their respective terms of usage determining what authorized purposes it is meant for. Users have fine-grained control over all attribute sharing.[1]

Authenticator

An authenticator, or authentication factor is an object used in authenticating the identity of an individual. Authentication factors may be something the user knows (a password or PIN), something he/she has (a card or a physical document or a device e.g. a mobile) or something the user is, a measurable physical characteristic of the signer, such as a facial image or fingerprint.

Biometrics

A measurable physical characteristic or personal behavioral trait used to recognize an applicant's identity, or verify their claimed identity. Facial images, fingerprints, and iris scan samples are all examples of biometrics.[2]

Credential

A document, device or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, usernames and passwords, SIM cards, etc. A digital attestation (signed or not) can stand for a credential too, as well as a biometric identifier, once it has been registered with the identity provider.

Digital authentication

The process of verifying a person's digital identity using one or more factors or credentials in order to establish that they are whom they claim to be. Authentication is therefore a process of establishing confidence in a person's digital identity.

Digital identification

The process of unambiguously validating a person's attributes and characteristics—including uniqueness—in order to establish his or her digital identity.

Digital identity or Electronic Identity (eID)

The terminology used throughout this document to refer to a set of electronically captured and stored attributes and credentials that can uniquely identify a person. It can take the form of an electronic card, a mobile app, a hardware token, etc.

Digital identity scheme

A system that enables unique natural persons to prove, unambiguously and securely, who they are during digital transactions and to empower them to assert their legal rights in a digital context. The system is based on digital transactions (identification, authentication, digital signature, etc.) made between users, with identity provider(s) and service providers that can be public and / or private. It follows national and/or international rules, processes and relies on specific technologies. A Digital Identity Scheme is laid on a Trust Framework. Eg. All notified digital identity schemes in Europe are laid on the eIDAS Trust Framework.

Digital ID wallet

A secure mobile wallet app which hosts a range of digitized identity documents and credentials, which is based on ISO 18013-5 standard, put the end user in control of his data and can be checked through an ID verifier app.

Electronic signature

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, assurance of data integrity and signatory non-repudiation.[3]

eSIM

eSIM is short for Embedded Subscriber Identity Module, or Embedded SIM. The user only needs to download and activate his profile onto the eSIM to start using it.

Federated Identity

Federation is a process that allows for the conveyance of authentication attributes and subscriber attributes across networked systems. In a federation scenario, the verifier is referred to as an Identity Provider, or IDP. The Relying Party (RP) is the party that receives and uses the information provided by the IDP.[4]

Government-driven centralized system

A government-led national system that provides digital identities and verified credentials that are stored and controlled by a single central authority, based on a unique national identity database and defined by a legal framework.

Identity Provider

An entity - for instance: a government agency or private firm - that issues and manages identities, credentials, and authentication processes throughout the identity lifecycle.[5]

Know your customer (KYC)

General term used to refer to those regulations requiring organizations to perform due diligence in establishing a customer's identity.[6]

Level of assurance (LoA)

A level of (identity) assurance is the certainty with which a claim to a particular identity during identity proofing, authentication and federation can be trusted to actually be the claimant's "true" identity. ISO/IEC 29115 and NIST SP 800-63-3A defines Identity Assurance Levels for the issuance process to describe how well a person has been identity proofed and how well the mobile eID-document is bound to the person that possesses the mobile device.

Level of Confidence

The amount of confidence a verifying entity may place or the issuer may convey on the mobile eID document; it depends on four factors being identity proofing, device-credential binding, data freshness and holder authentication.[7]

Mobile identity

A digital identity provided via mobile networks, data and devices.

Public Key Infrastructure (PKI)

A set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys. PKIs are the foundation that enables the use of technologies, such as digital signatures and encryption, across large user populations. PKIs deliver the elements essential for a secure and trusted business environment for e-commerce and the growing Internet of Things (IoT).[8]

Relying Party or Service provider (SP)

An organization or firm that needs to verify the identity of the end-user. This entity relies upon the credentials and authentication mechanisms provided by an ID system, typically to process a transaction, to enable the provision of a digital service or to grant access to information or to a system.[9]

Single Sign-On

A centralized session and user authentication service in which one set of login credentials can be used to access multiple applications.

Trust Framework

The "rules" underpinning federated identity management, typically consisting of: system, legal, conformance, and recognition.[10]

Unique Identification Number (UIN)

A number that uniquely identifies an individual and can be used to link an identity across databases and systems in both the public and private sector. National identity providers may issue a UIN to citizens and residents for their lifetime.

ABREVIATIONS

API: Application Programming Interface
eID: Electronic Identification
HSM: Hardware Security Module
ICT: Information and Communication Technologies
IDP: Identity Provider
IoT: Internet of Things
ISO: International Organization for Standardization
KBA: Knowledge-Based Authentication
KYC: Know your customer
LoA: Level of Assurance
MDL: Mobile Driver License
MNO: Mobile Network Operator
NFC: near-field communication
NIN: National Identity Number (may or may not be unique, i.e., a UIN)
OTP: One-Time Password
PKI: Public Key Infrastructure
PPP: Public Private Partnership
QeS: Qualified Electronic Signature
RFP: Request For Proposal
ROI: Return On Investment
SIM: Subscriber Identity Module
SP: Service Provider
SSI: Self Sovereign Identity
SSO: Single Sign-On
UI: User Interface
UX: User Experience

Organizations, regulations and standards/ protocols

eIDAS: Electronic Identification, Authentication and Trust Services
FIDO: Fast Identity Online – the FIDO Alliance is an industry body building standards for authentication of individuals using mobile technology
ICAO: International Civil Aviation Organisation
NIST: National Institute of Standards and Technology
OAuth: Standardised protocol for sharing authorisation tokens
OECD: Organisation for Economic Co-operation and Development
OpenID Connect: Standardised protocol for federated identity built on OAuth
OSIA: Open Standards Identity APIs

[1] Secure Key, *https://www.securetechalliance.org/resources/media/scag13_preconference/09.pdf*

[2] Richard Kissel (May 2013). Glossary of Key Information Security Terms. NIST Retrieved from: *http://nvlpubs.nist.gov/nistpubs/ ir/2013/NIST.IR.7298r2.pdf*

[3] NIST SP 800-12

[4] NIST 800-63-3, https://pages.nist.gov/800-63-3/sp800-63c.html

[5] World Bank, GSMA and SIA paper : Towards Shared Principles for Public and Private Sector Collaboration https://openknowledge.worldbank.org/handle/10986/11866

[6] Caribou Digital, Private-Sector Digital Identity in Emerging Markets, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2016.

[7] ISO/IEC 23220-5 (still at working draft stage)

[8] Thales, What is Public Key Infrastructure (PKI)?, *https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki*

[9] Adapted from NIST 800-63:2017, ID4D Draft for consultation.

[10] NIST IR 8149

DEEP DIVE INTO GLOBAL INSIGHTS

INSIGHTS OVERVIEW

END USER VALUE PROPOSITIONS	COUNTRY USE CASES	
INSIGHT #1 CONSIDER DIGITAL IDENTITY AS A DRIVER FOR INCLUSION AND DIGNITY	> FRANCE > AZERBAIJAN > AUSTRALIA, QUEENSLAND	16
INSIGHT #2 DESIGN PRIVACY TO PROTECT, FIRST AND FOREMOST, THE PERSON	> AUSTRALIA, QUEENSLAND > AUSTRIA > CANADA	18
INSIGHT #3 FIND THE RIGHT BALANCE BETWEEN USER EXPERIENCE AND SECURITY	> ESTONIA > USA, ARIZONA > SINGAPORE	20
INSIGHT #4 INVOLVE END-USERS THROUGHOUT DIGITAL ID DEVELOPMENT & IMPLEMENTATION	> AUSTRALIA, QUEENSLAND > DENMARK	22

ECOSYSTEM AND GOVERNANCE	COUNTRY USE CASES	
INSIGHT #5 FOSTER PUBLIC AND PRIVATE COLLABORATION FOR FINANCIAL STABILITY	> INDIA > DENMARK > ITALY	24
INSIGHT #6 SET UP INTERGOVERNMENTAL AND MULTIDISCIPLINARY TASK FORCE TO LEAD DIGITAL IDENTITY	> COLOMBIA > NIGERIA > FRANCE	26
INSIGHT #7 GET INVOLVED IN INTERNATIONAL REGULATION & STANDARDIZATION BODIES	> AUSTRALIA, QUEENSLAND & ARIZONA > LATIN AMERICA > NIGERIA	28

TECHNOLOGY IMPLEMENTATION	COUNTRY USE CASES	
INSIGHT #8 THINK MOBILE FIRST	> LIECHTENSTEIN > AZERBAIJAN > ITALY	30
INSIGHT #9 IMPLEMENT AGILE AND ITERATIVE PROCESSES – AND BE EXPLICITE ABOUT IT	> AUSTRALIA, QUEENSLAND > FRANCE > SINGAPORE	32
INSIGHT #10 IMPLEMENT ADPATIVE & MODULAR INFRASTRUCTURE TO BRIDGE PAST AND FUTURE	> DENMARK > INDIA > CANADA	34

GO TO MARKET & PROMOTION	COUNTRY USE CASES	
INSIGHT #11 PROVIDE USEFUL & RECURRING SERVICES BY PIGGYBACKING ON PRIVATE SECTOR	> PORTUGAL > FRANCE > DENMARK	36
INSIGHT #12 PROVIDE A SECURE, EASY AND MULTIPLE ENROLLMENT PROCEDURE	> FRANCE > ITALY > PORTUGAL	38
INSIGHT #13 DESIGN A CUSTOMIZED STAKEHOLDER CAMPAIGN TO BOOST ADOPTION	> NETHERLANDS > AUSTRIA > SINGAPORE	40

INSIGHT #1

CONSIDER DIGITAL IDENTITY AS A DRIVER FOR INCLUSION AND DIGNITY

Worlwide, nearly one billion people lack a legally recognized form of identification such as birth certificates and ID cards (World Bank, 2020). They are consequently deprived of basic services and socio-economic participation, financial inclusion, and their democratic rights. In the vast majority of countries, proof of identity is a mandatory step to open a bank account, register for a school, apply for social benefits, rent a flat, find a job, etc. The COVID-19 pandemic has further demonstrated to governments, businesses and citizens the key role of digital identity as a foundational socio-economic safety net and the importance of having the infrastructure ready and available. For example, registration and use continued at least at the same pace or increased twofolds in countries like Azerbaijan or Italy.

By opening access to online public and private services 24/7 to all in a secure, transparent and immediate way, digital identity is increasingly seen as a way to improve inclusion and dignity issues. As access to all is the pre-condition for inclusion, all digital ID's face common concerns and challenges: how can digital ID address the entire population, and can it? How to provide access to people with disabilities and to those who live in areas with no internet coverage?

"It is important to recognize that there will always be someone out there who can't manage the solution. So no matter how digitalized we get, we still need to supply a way for them to interact with the public sector."

Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

WHAT DO THEY THINK ABOUT LEGAL IDENTITY & INCLUSIVITY?

Sophie KWASNY, Head of the Data Protection Unit of the Council of Europe

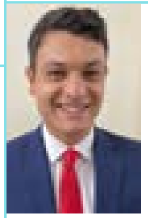
"Many consider that one of the Sustainable Development Goals is to have **digital identity** for all, which is a misunderstanding. The objective is to have **legal identity** for all, which is a fundamental component to exercise our rights. Digital tools should come as enablers for individuals to exercice their rights, but should in no way be a condition to access, for instance, public services."

Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)

"We are looking for credentials that can help with dignity, so that everybody doesn't have to know that you are under public assistance. Our goal is to help people access benefits without making them so visible in their access to these benefits."

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

"People with no identity lose their dignity. They have no access to social services, public transports and all the services that you and I take for granted. Identity here is about individual dignity."



Andrea Spallacci, Project Leader, Agenzia per l'Italia Digitale (AgID)

"Right now, SPID is not available for minors - even if several public and private services are designed specifically for them. We are working on a solution involving the authorisation by parents. Moreover, since some associations of disabled people have asked for solutions to help them in the authentication process, we are studying more inclusive solutions, because SPID should not be an obstacle."

USE CASE #1

CARERS AND E-REPRESENTATION FOR PEOPLE IN NEED IN FRANCE

In France, around 13 million people face difficulties with digital tools because of accessibility problems or disabilities. To address the issue, the French public federated digital identity scheme, FranceConnect, is testing a new service, Aidants Connect, to provide electronic representation for people in need.

Aidants Connect enables authorized professional carers to carry out administrative procedures online, securely, and legally, on behalf of people facing difficulties with digital tools. In practical terms, carers help users create their online accounts, define the procedures for which the representation is needed, and proceed to electronically sign a mandate online. Currently being trialled in 13 public and social organizations, the service will be extended to the rest of the country if it proves successful.

USE CASE #2

VERBAL SOLUTIONS IN AZERBAIJAN ENSURING DIGITAL INCLUSIVITY

To be inclusive and address less tech-savvy individuals, the Mobile ID in Azerbaijan includes 9 services based on verbal solutions and call centers.

These services are popular in rural areas, in particular for tax declaration services. Users can complete their tax declaration without filling anything. They call, answer questions and sign electronically. Currently, these services are provided by human agents, with Artificial Intelligence being considered for the future.

USE CASE #3

DIGITAL ID WALLET HELPS VICTIMS OF DOMESTIC VIOLENCE IN QUEENSLAND, AUSTRALIA

In Queensland, Australia, the digital licence application, which also serves as a digital ID wallet, has played a key role in helping women respond to domestic violence. In a country where one in four women face domestic violence, and more than half leave their partners without their identity documents, digital ID has helped them access social services within the day, when it could take up to 4 months to renew a physical ID document.

"It can take up to 4 months to renew a physical ID document, a time when women and their children are vulnerable. Now, if a woman leaves their partner, she can ring us, or use a facial recognition camera, and they can start there new life right away on the same day."

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

INCLUSION AND DIGNITY CAN BE ADDRESSED IN SEVERAL WAYS

1 Consider the country and region's socio-economic context to select the relevant technology and credential: A mix of hardware and software tokens and Digital ID solutions can, in some cases, enable better inclusivity.

2 Consult and take into account the needs of specific populations to develop inclusive solutions and processes (verbal solutions based on call centers, reverse QR codes, native accessibility functions for older populations, offline validation, etc.), and maintain physical alternatives.

3 Consider digital ID as an opportunity to increase human dignity and think of new ways to provide less intrusive and discriminatory credentials.

INSIGHT #2

DESIGN PRIVACY TO PROTECT, FIRST AND FOREMOST, THE PERSON

"Who owns our data, who can acces it, and what is it being used for?" These questions are asked on a recurring basis by increasingly privacy-aware citizens. To address these concerns, governments are increasing thinking about new models, such as decentralised models, allowing users to distribute and share only the necessary data to validate their identities and access online services. Technology is also rapidly evolving towards increased data protection: privacy by design, data privacy tools, data filters between identity and services providers, decentralized databases, etc.

While trust and privacy mecanisms are necessary, designing the legal and regulatory framework to protect individuals should come first. The growing efficiency of technologies such as facial recognition and the increased flow of personal data across borders reinforces the relevance of a common and harmonized understanding of data protection. The Council of Europe promotes the generalization of the Convention 108, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, protecting individuals, their rights and fundamental freedoms, and in particular the right to the respect for privacy. Today, countries worldwide consult the Council of Europe for regulatory and methodological support, yet too many continue to design and implement national digital identities without data protection frameworks and legislation.

"The biggest question we get from our customers, 100% of the time is: What are you doing with our data?"

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

"In Kenya, civil society shut the digital ID project because of a lack of safeguards and data protection legislation."

Peter Kimpian, Data Protection Unit at Council of Europe

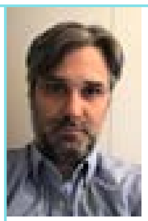
WHAT DO THEY THINK ABOUT DATA PROTECTION?

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products, GovTech Singapore

"I often ask people to consider how "private" their current methods of sharing data are. When applying for a loan or a credit card, individuals must send dozen of documents, containing more personal information than required, to an employee or banks intermediary. Digital means of data sharing through explicit consent of individuals allows people to share only required data, bypassing intermediaries, and provide digital traceability of the consent and the purpose of such data sharing. It is in fact more privacy-enhancing than sharing whole physical documents."

Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)

"Canada is a very privacy-focused country. We believe that people can make choices about data, that they have agency and can make decisions about how their data is shared and for what purpose."



Peter KIMPIAN, Data Protection Unit at Council of Europe

"We are discussing openly with our Chinese partners and there is clearly an interest today. China has passed a law on the protection of privacy and has just passed one on data protection. They looked into GDPR. We must continue open cooperation even if we had differences at the beginning. There is only one future, and that is to guarantee an appropriate level of protection for individuals everywhere in the world, while facilitating the flow of data, by converging to international standards that already exist."

Sophie KWASNY, Head of the Data Protection Unit of the Council of Europe

"If the different regions of the world want to continue to exchange, there will have to be a common understanding. Our modernized Convention 108 is acceptable to all democracies."

USE CASE #1

ATTRIBUTE SHARING FOR DATA CONSENT IN AUSTRALIA

The Queensland Department of Transport and Main Roads launched a mobile application, the Digital Licence App, currently in the trial phase since the first half of 2020. The App serves as a digital ID wallet storing a large range of digital documents in a single secure vault. The objective is to promote a distributed consent model of identity, where users are trusted to distribute and share their data to access a range of government e-services online or for physical identification.

Users control the information they share with others and determine the information they want to display. If a user wants to prove their age, he/she can use the app to only disclose the attribute "I am older than 18", with a QR code validated online by the verifier. The credential will not display the Digital licence holder's name, date of birth, or where he/she lives.

USE CASE #2

SECTOR SPECIFIC IDENTIFIERS IN AUSTRIA

The Austrian eID program implemented strong privacy and security mechanisms from the start. All citizens and residents are given a Central Register of Residents (CRR) number, but there is no requirement to get a physical identity card. Instead, Austria has a virtual Citizen Card (CC) that can be installed on several devices based on a technology-neutral approach: smartcards, USB devices, or mobile app.

One of the key privacy aspects of the Austrian scheme is the service-specific identifier. For the same individual, each service provider uses a different identifier cryptographically derived from the CRR number. This prevents the matching of individuals across their use of services and enables the simple revocation and replacement of encrypted identifiers in cases of fraud.

USE CASE #3

A TRIPLE BLIND PRIVACY USING BLOCKCHAIN IN CANADA

Verified.Me, along with Government Sign-in by Verified.Me, both follow the triple blind approach: no one in the identity network has access to the complete picture of the users' transactions: not the government, the banks nor the operator.

Launched for the private sector in 2019, Verified.Me uses blockchain for authentication, which was instrumental in implementing the triple blind identity information sharing. The Verified.Me trusted network and encrypted hash guarantees that the data comes from a trusted source, that it has not been altered, and that the data is being presented by the person it belongs to.

"Without blockchain, it is difficult to move data from A to B without putting the network at risk, because it is going to see a lot of data, risks being data harvesting and becoming a target for breach."

Andre Boysen, Chief Identity Officer, SecureKey Technologies Inc.

DATA PROTECTION SHOULD BE LEGAL BEFORE TECHNOLOGICAL

1 Start by designing and implementing data protection regulation and independant control bodies before deploying digital identity. International Organisations, such as the Council of Europe, offer useful guidance and resources.

2 Respond proactively to data concerns with protection mechanisms designed "natively" (privacy by design, attribute data sharing, etc.) and provide users with tools for monitoring and managing their data (data privacy tools).

3 Avoid centralization of data within a unique database: the ownership of all identities can be shared between public and/or private identity providers, based on users' consent. To guarantee privacy, the data can be exchanged across a system of joined-up databases following standardized protocols.

4 To avoid explicit user data being shared within the ecosystem, implement information filters between service and identity providers with end-to-end encryption or a gateway that guarantees a maximum level of privacy for the users.

INSIGHT #3

FIND THE RIGHT BALANCE BETWEEN USER EXPERIENCE AND SECURITY

Today, two systems of thought coexist and create a tension between a seamless user experience and higher levels of security:

> a common and pre-agreed level of security and guarantees for countries who wish to have interoperable Digital IDs with cross-border recognition by following trust frameworks such as the eIDAS regulation in Europe or the Pan-Canadian Trust Framework in Canada launched by the DIACC (Digital ID & Authentication Council of Canada).

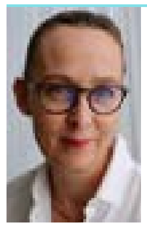
> a market-based level of security, set by actors like Google and Facebook who provide online identity services and set standards for worldwide user experience. These services are simple and easy to use, with full access and availability at any time, anywhere and on any device, with low authentication requirements.

The eIDAS experience shows that some member states take a very defined approach to security, whereas others are more flexible. Finding the right balance between a seamless user experience and high security standards is key for wide digital identity adoption but it remains a challenge, especially in countries where digital identity is not mandatory.

"For many small services, you don't need to have strong levels of security. The question resides in defining what "small" means."

Eric A. Caprioli, Lawyer at the Court, France Representative UNCITRAL/CNUDCI

WHAT DO THEY THINK ABOUT USER EXPERIENCE AND SECURITY?

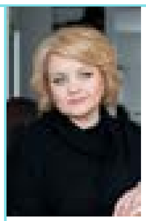


Valérie Péneau, Director of the interministerial program France Identité Numérique

"Start by getting users on board with a simple application, and gradually secure them. On the one hand, service providers have difficulties positioning themselves on the different levels of guarantee and, on the other, the ecosystem use is not ready for a high level of security."

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products GovTech Singapore

"With technology advancement, it is now possible to improve security and user experience at the same time, for example, our SingPass mobile digital token is more secure than passwords or SMS, and easier to carry around and use compared to hardware tokens. We also design our digital identity platform to offer multiple authentication factors so that relying parties can choose to layer on more authentication factors if the transactions are considered more sensitive. We let our relying parties assess the risk profile associated to their own use case."



Jana Krimpe, Azerbaijan Public Private consortium representative

"In Azerbaijan, we decided not to implement a diverse set of solutions with different levels of assurance: it will take twice the energy to explain the difference to people who do not like to change instruments too often. They do not understand why they can use one password to access one service and why it does not work for another one. We prefer to go through this procedure only once and ensure that people have all the instruments they need and that these can be used everywhere."

Andre Vasconcelos, eID Advisor to the Board of Directors, Administrative Modernization Agency, Portugal

"For the citizen card, we mostly focused on security, for the Digital Mobile Key (CMD), we kept the same security requirements but focused more on the user experience. The only requirement, which everyone has, is a mobile phone with an associated PIN, on which users receive their OTP via SMS. Nowadays, it is also possible to use biometrics to replace the second factor authentication such as OTP, easier than copying the OTP from one device to another."

USE CASE #1

A RISK PROFILE PER USE CASE APPROACH TO SECURITY IN ESTONIA

Estonia is one of the most digitally integrated societies in the world, with three interoperable digital ID scheme (ID-Kaart, Mobiil-ID, Smart-ID). For public services, only a few transactions still require a physical presence and cannot be done online, such as registering a wedding or buying a house.

Given the high sensitivity of some use-cases (e-voting, access to medical data, or bank transfers), the Estonian Government requires a face-to-face enrollment. It has also developed user journeys based on an acceptable risk. For most daily use cases, the Government takes advantage of the wide range of authenticators at its disposal to ensure the security of transactions, and guarantees the best user experience by leaving the choice to the user. Currently, to access public and private services online, users are free to use an app (Smart-ID), a smartcard with a card reader (ID-Kaart), or a smartphone equipped with a PKI-compatible SIM card (Mobiil-ID).

USE CASE #2

A SCORING APPROACH FOR AUTHENTICATION IN ARIZONA

To ensure an optimal level of security without degrading the user experience, the Arizona Department of Transportation (ADOT) uses a different approach than the binary yes/no approach to authentication.

A risk score is created for each interaction, based on what is known about the user, if the user has done any enhanced authentication and when. The risk score is partly based on a fraud detection tool which provides information about the connection (type of device used, location, cash prepaid phone, device linked to fraud, etc.).

If the transaction does not have a sufficient score, a higher level of authentication will be required before proceeding. Enhanced authentication tools include facial recognition or knowledge-based authentication (KBA).

"We require different authentication strategies, up to the highest one - using biometrically authenticated digital identity tied to the smartphone. That allows us to only go as far as we must to not inconvenience our customers."

Eric Jorgensen, Motor Vehicle Division Director at Arizona Department of Transportation, USA

USE CASE #3

FACE RECOGNITION AS A SERVICE IN SINGAPORE

When SingPass was launched in 2003, it provided a ID/Password credential for citizens to access all government online services. However, passwords are often forgotten. To address the issue, GovTech has introduced other form factors for authentication, such as the SingPass Mobile app. In addition, GovTech is also piloting face verification for physical and remote authentication. The objective is to provide an additional form factor to increase security and ensure a better user experience - one that is less cumbersome than passwords and SMS OTP, for example.

The face verification service is currently piloted at the service centres of major government agencies such as the tax authorities. One of Singapore's largest bank is also using the face verification as-a-service for onboarding users to their mobile platform. Relying parties that make use of this face verification as-a-service provided by GovTech Singapore will only receive a matching score and will not receive any personal identifiable information. The initial pilot results were encouraging and more relying parties are on track to adopt this.

DIFFERENT STRATEGIES ACCORDING TO MANDATORY OR OPTIONAL DIGITAL IDENTITIES

1 In countries where digital ID is optional, and where user experience will determine adoption rates, it is vital to provide user-friendly options and progressively adapt the level of security.

2 When digital identity is partially mandatory, some countries (including Azerbaijan) have found it easier to start right away with high levels of security for all services, to "break user habits".

3 In countries where digital maturity is already high, adopt a use-case approach and adapt each use case to the level of security required, like in Estonia or Singapore.

INSIGHT #4

INVOLVE END-USERS THROUGHOUT THE DIGITAL ID DEVELOPMENT & IMPLEMENTATION

The end-user value proposition of the Digital Identity is critical for citizen and business adoption and widespread takeup. Users - or rather customers - need to percieve an immediate interest and value in the use case provided, whether it is in terms of time efficiency, reduced costs, or simply more flexibility. The user experience should be frictionless, with a friendly user interface.

Governments and Digital ID project teams are accepting to challenge their initial perception of their "customers" and are looking for new ways to better understand these new expectations and standards, and translate them into their own services and experiences. Mindsets, tools and methods are shifting towards more "citizen centricity" to make sure user needs and expectations are taken into account from the design of the solution to the development and the implementation.

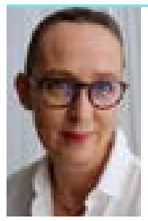
> "Co-design is one of the ways to go to get buy-in from your citizens."
>
> Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

WHAT DO THEY THINK ABOUT USER CENTRICITY?

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

"We had to rethink who our customers are and realized there was so much that we hadn't understood. We released our first drivers licence in 1910: now, our customers are different."

"Set up a true codesign process: not just sending a survey, getting feedback but meaning having your customers to COME IN, touch, feel, and work through the use cases in a relational way. We saw that there was so much that we didn't understand in relation to cultural aspects because we were not in a dialogue, a proper co-design."

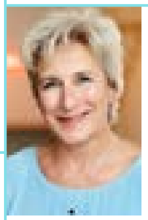


Valérie Péneau, Director of the interministerial program France Identité Numérique

"Recruiting UX designers from the start makes it possible to systematically combine the search for optimal ergonomics with security requirements."

Lionel Fouillen, Partnership Relations Manager, FranceConnect

"In order to guarantee the promise of simplified connection to public services, we support our partners by offering them UX recommendations to build quality user journeys. Before going into production, we check the user journey and how it is implemented. We take a look at the technical, security, and UX aspects of the service."



Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

"So whenever we develop something, we actually take specific population groups in from the very beginning in order to make sure the requirements important for them are taken into account in our tenders and into our development."

USE CASE #1

DIGITAL ID CO-DESIGN PROCESS IN QUEENSLAND, AUSTRALIA

The Customer Orientated Registration and Licensing (CORAL) program is in charge of the conception, development and roll-out of the Digital Licence App for Queensland (Australia). For the purpose of the program, the team designed a "Digital Playbook" explaining the different necessary steps to design a user-centric digital solution. Since the beginning of the project, a wide variety of customer groups and stakeholders (indigenous, business, regulatory and lobbying groups) have been involved to co-design, collaborate and prioritize suitable outcomes to deliver the Digital Licence App, ensure user experience as well as the inclusivity and accessibility of solutions and services for specific population. These groups also participated in the evaluation and selection of vendors.

The app was in trial early 2020 in the Fraser Coast region, where users were invited to prioritize new features for future versions.

USE CASE #2

DENMARK BRINGS TOGETHER THE ELDERLY AND VISUALLY IMPAIRED FOR CREDENTIAL DESIGN

The Danish Government department charged with developing the MitID solution (third generation of the national digital ID) is working alongside associations to design adapted solutions and involve them in user tests. They will design a specific token for the elderly and visually impaired, where the code will be read aloud and have an attached headset. The token is also a little larger and easier to handle.
During the implementation phase, they also rely on a networks of teachers, via the municipalities, to teach the elderly how to use the whole digital infrastructure and online public services.

> "When you have a solution on which you want to build an entire public digitization, you need to think of the groups in the society who are not the easiest ones to take up on this and you have to apply solutions for them."
>
> Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

CITIZENS SHOULD BE INVOLVED EVERY STEP OF THE NATIONAL DIGITAL ID PROJECT

1. Include a citizen-centric vision in project governance (often represented by having UX designers in the team) to validate new integrations or services.
2. Change your perspective on citizens by interacting with them, during working groups but also directly on the field, in existing administrative contact points to better understand their customer journey, painpoints, needs, preferences, etc.
3. Implicate citizens in a true co-design process, from use case definition to the design of solution interface and choice of the digital ID form factor. This user-centric process will also help to define the relevant levels of security for each of the use case / service, ensure the solutions fits with local and cultural preferences and addresses all citizens.
4. Involve citizens in the implementation and roll-out, and have a clear and strong communication flow with them.

INSIGHT #5

FOSTER PUBLIC AND PRIVATE COLLABORATION FOR FINANCIAL STABILITY

> "It takes an average of 5 years to achieve market penetration and modify customer behavior, before something starts to crucially change. Then, it's easier to develop new business models because the players understand the service benefits and are ready to pay for them. "
>
> Jana Krimpe, Azerbaijan Public Private consortium representative

Digital Identity in many countries and cultures is considered as a state prerogative and many Digital Identities worlwide are still initiatied, financed and managed by governmental entities, as is the case in Austria, Singapore, Oman, etc. But understanding the added value of digital ID compared to the heavy investments that are required remains a challenge for many governments, especially in developing countries where these investments often represent trade-offs with other essential needs (infrastructure, health, education, etc.). The recent COVID-19 pandemic has helped to change perceptions by demonstrating "in situ" the benefits of digital identity to access often vital online services and benefits.

Bearing in mind that access to online public services should remain free and accessible to all, governments have started to engage in diverse forms of partnerships and revenue-sharing models with the private sector to finetune their business models and investment capacities. In countries such as Denmark, the financial sector has played an instrumental role in the success of Digital IDs. In developing countries, promising return and investment opportunities have started to attract identity and service providers, where business models can be based on considerable volumes of transactions.

Advantages to this public-private collaboration include reducing time of development and implementation, shared investment costs, providing private services that improve adoption through popular use cases such as online banking, but also sharing competencies between private and public, compliance support in remote client authentication, etc.

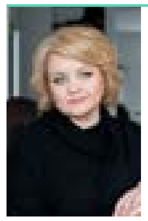
WHAT DO THEY THINK ABOUT PUBLIC AND PRIVATE SECTOR CO-FINANCING?

Mory Camara, President of IIC (Identity Council), ID4Africa

"Resources are always an issue. In countries like Guinea where everything is a priority - be it health, infrastructure, agriculture, housing - technology in general is not forgotten but just a priority among many others. There is a positioning problem and there must be political will for a real development of the digital sector in Africa."

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products GovTech Singapore

"For a digital platform to be sustainable, it is important to identify and clearly demonstrate the value first. From that value generated, we can then derive a commercial model. The challenge of any digital platforms is to have a critical mass adoption of consumers and producers to form a network effect, before the commercial model is able to kick in."



Jana Krimpe, Azerbaijan Public Private consortium representative

"For Africa and Asia, PPP will work perfectly because of the business model but also because of the complexity of infrastructure. With only the financial sector, services will be limited, but if you want to create a real service 24/7, you need to involve the whole country and motivate the government. It's better to start immediately to involve everyone by creating a PPP."

Eric A. Caprioli, Lawyer at the Court, France Representative UNCITRAL/CNUDCI

"You have to remember one thing: the state has no more money. If private actors were not capable of spending millions or even tens of millions in partnership with public actors, we would not have a digital identity. If the state had not opened up to the private sector, we would have stood idle. It's not a problem for state sovereignty because there will always be the state to control, audit and sanction if needed, and for European countries, compliance with the eIDAS regulation."

USE CASE #1

A PROGRESSIVELY PAYING MODEL IN INDIA

The creation of the Aadhaar scheme, the largest state biometric-based program worldwide, was entirely financed by the Indian government.

The UIDAI (Unique Identification Authority of India) in charge of the program, initially kept all authentication services free for all to lower the barrier to entry. It has only begun charging relying parties in 2019. Since then, private organizations are charged US$0.007 for Aadhaar authentication (for a yes/no challenge), and US$0.3 for e-KYC transactions.

USE CASE #2

FINANCIAL SECTOR CO-OWNS AND CO-FINANCES THE DENMARK DIGITAL ID

The third generation of the Danish digital ID, named MitID, is financed and co-owned by the government and the financial sector.

There will be a fee per transaction for service providers who will want to use it. This fee, calculated on the basis of running costs, is expected to be less expensive for most service providers than previous version NemID.

> "It's quite expensive for only 5 million people to build an infrastructure like this. So rather than building one for the public sector and one for the private and a third for the financial sector, it makes really good sense to build one that can be used across sectors. And I think that's also why it has been interesting for all parties to join."
>
> Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

USE CASE #3

9 PRIVATE IDPs FINANCE THE NATIONAL DIGITAL ID SCHEME IN ITALY

The Italian Public System of Digital Identity (SPID) is a public open ecosystem allowing private accredited IDPs to provide digital identity for citizens and businesses. The scheme is 100% financed by these private IDPs, who strongly believe in the profitability of SPID in the long-run.

This partnership provides a secure and reliable system to Italy's public administration, delegating heavy identity processes (issuing and maintaining credentials) and saving both humain and financial resources.

SPID is free for citizens and public service providers at all levels of security except for the highest level of assurance (used mainly by professionals) and private service providers follow a pay-per-use model.

FINETUNE THE BUSINESS MODEL DEPENDING ON DIGITIZATION MATURITY AND DATABASE OWNERSHIP

1 With a centralized government owned and funded Digital ID and optional online public services (vs. mandatory), privilege a free for all approach for the first years (5-6) to secure use and take up. Once adoption is more or less stable, new business models (freemium, pay-per-use, etc.) can be explored with private services and relying parties for long-term financial ROI.

2 A Digital ID scheme with a strong history of public digitization strategy and mandatory online public services securing high levels of adoption can opt for a pay-per-use model from the start. However, the quality and volume of services available must be high and provide real added value to users.

3 To help finance the initial Digital ID infrastructure and operational costs of the Digital ID, governments can partner with the financial sector from the very start of the project. Financial sector will also help secure use and adoption if digitization is not mandatory, by providing online banking access with high frequency of use.

4 If databases are not established or not government owned and centralized, governments can privilege federated models with private IDPs financing, as long as they are regulated by clear governement frameworks and governance mecanisms. Federated models are an alternative to governement funding, are flexible and user-friendly for customers and business who can select the IDP of their choice.

INSIGHT #6

SET UP INTERGOVERNMENT AND MULTIDISCIPLINARY TASK FORCE TO LEAD DIGITAL IDENTITY

Governments often have difficulties grasping the technical, security and privacy aspects of Digital Identity projects and are tempted to outsource the project to technical teams and experts. This leads to under staffed and under-represented projects teams that often lack strong political backing - vital for smooth and efficient project management. Because Digital Identity is at the intersection of legal identity and access to critical public services, it is a strategic national and political project, and should be staffed, represented and managed as such.

> Having the ressources to manage the digital ID project is both about having the rights ressources, as well as enough ressources. Teams are too often understaffed, and lack of key competencies such as communication, marketing, UX/UI.
> To gain in time and effiency, collaboration within the digital identity public (ministries, administrations, municipalities) and private ecosystem (identity providers, service providers, relying parties, solutions providers, etc.) from the beginning is key for successful design, management, implementation and adoption.

"To approach FranceConnect from a purely technical perspective is a mistake. The technical implementation is simple and well documented. FranceConnect is above all about business and functional choices, strategic positioning."

Lionel Fouillen, Partner Relations Manager, FranceConnect

THEIR CHALLENGES ON DIGITAL ID GOVERNANCE AND PROJECT MANAGEMENT?

Michiel Van der Veen, Director Innovation & Development at the National Office for Identity Data, The Netherlands

"This whole world of Digital Identity is very complex. You need to have the people who can understand this, develop policy and make design choices. You need to make sure that you have those people on board, or that you can access those people and make this knowledge available to you."

Herbert Leithold, Secretary-General Secure Information Technology Center, Austria

"All the stakeholders have been involved since the beginning : different ministries, the provinces, the representatives from the municipalities, as well as the private sector represented by the Chamber of Commerce. These collaborative working groups were probably one of the success factors for e-governement and e-ID. It takes longer, but once the standards are set, it avoids silos in the ID scheme and increases the probability of success."

Mory Camara, President of IIC (Identity Council), ID4Africa

"We have experts at doctorate level, high level international consultants and level 1 and 2 technicians but between the two, there is a gap - at the level of project management, supervisors, managers - which makes that project implementation, monitoring, maintenance always a problem."

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

"Our main everyday challenge is governance: how do we work in a collaborative way with all our stakeholders? How do we manage to not dilute what they are asking for, but still allow us to prioritize ideas and functionalities according to the funds we have?"

USE CASE #1

INTERGOVERNMENTAL COLLABORATION TO PROVIDE DIGITAL SERVICES IN COLOMBIA

The National Civil Registry of Colombia agency (RNEC) is mandated to issue and manage citizen identity and the Ministry of Technology and Telecommunications (MINTIC) to lead digital ID usages in the country through its National Digital Agency.

RNEC and MINTIC are leading an intergovernmental effort to provide the country with a digital Citizen Digital Folder including an authentication system, interoperable with the main public services. The Citizen Digital Folder is defined as a service for hosting documents online accessible to citizens as well as authorized legal persons thanks to their Digital ID. This tool will facilitate administrative documents exchange between public entities and other stakeholders. Digital services will also be extended to the financial sector and the elections electronic system.

This intergovernmental approach brings important benefits in terms of security, efficiency, transparency, and privacy.

USE CASE #2

AN INDEPENDANT TASK FORCE TO LEAD AND MANAGE THE DIGITAL ID IN NIGERIA

In many African countries, national identity registries are hosted in different ministries or public organizations. In Nigeria, however, the Government created the National Identity Management Commission (NIMC) to deal with the multiple stakeholders involved in the design of the digital identity scheme. NIMC is an independent and autonomous agency, governed by a board of 18 individuals, representing different government agencies as well as the private sector in the country.

Benefits of this organization include better stakeholder coordination, with more fluidity and fewer influence struggles. It also leverages the opportunity for private sector innovation thanks to public-private partnerships (PPPs), where private firms provide the funds in exchange for revenue streams in the future digital ID scheme.

USE CASE #3

MULTI-STAKEHOLDERS COLLABORATIVE DESIGN AND MANAGEMENT PROCESS IN FRANCE

When the FranceConnect Digital Identity Federator project started in 2015, the DINUM (Direction Interministérielle du Numérique) had 5 full time staff. 5 years later, approximitely 30 people work for FranceConnect, with a majority of developpers and 6 supports functions.

Managed by the DINUM, The Digital Identity was co-built with approximately fifteen public administrations for input on data mangement and day to day run.

SETTING UP THE RIGHT TASK FORCE FOR PROJECT MANAGEMENT

1 **Identify from the start the digital identity project as a political, legal, strategic and national priority - and not as a technical one only - to gain immediate legitimacy within different ministries and administrations and benefit from strong political portage.**

2 **Set-up a inter-government team with a certain degree of autonomy and independance for a transversal approach and avoid silos within different ministries. Be as present as possible in strategic interministerial governance bodies.**

3 **Build a strong multidisciplinary team with both strong project management skills as well as technical, architecture, regulation, UX, communication experts. In house expertise to learn from and work alonsgside external expertise is key for being agile.**

4 **Collaborate on a regular basis with public and private stakoholders. Include them in workshops to co-design with them, making sure the right use cases are prioritized and major interests represented. Collaborative methodologies and tools help stakeholders prioritize and converge efficiently, although it is an every-day challenge for many of the project teams interviewed.**

INSIGHT #7

GET INVOLVED IN INTERNATIONAL REGULATION & STANDARDIZATION BODIES

Governments planning to launch a new mobile ID scheme first have to establish a comprehensive legal framework for the digital ID to be recognized and endorsed by law and to safeguard data privacy, security and user rights.

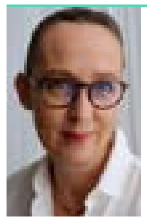
Building their identity scheme on existing international standards such as ISO, ICAO, OSIA, NIST or frameworks such as eIDAS is key for governments to ensure interoperability, provide a common language and understanding between policy makers and technicians, and enable comparability within countries at a national and local levels and with other countries at a regional/international level.

Standards ensure the implementation of universally understood protocols necessary for operation, compatibility, and interoperability, which are in turn necessary for product development and adoption. Taking part in the definition of new standards can also give governments early access to industry information, give them a voice in the development of standards and help keep market access open.

"When we drafted our decree in Vietnam, we learned from different schemes; first one of course is eIDAS. We also read the digital ID framework from Australia and also learned from the US. These three are our main sources of references."

Lã Hoàng Trung, Director of the National E-Authentication Centre, Ministry of Information and Communications, Vietnam

THEIR VISION ON INTERNATIONAL REGULATION AND STANDARDIZATION BODIES

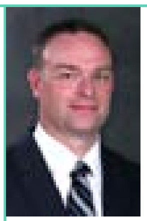


Valérie Péneau, Director of the interministerial program France Identité Numérique

"The issue of standardization is colossal in terms of digital identity. It is an issue for the industry, for the State, which must guarantee its long-term representation at the right level and in the right bodies, in order to anticipate the technological evolutions and disruptions expected in the coming years."

Lionel Fouillen, Partnership Relations Manager, FranceConnect

"For FranceConnect, eIDAS is very reassuring and allows two things: it clearly defines the levels of security, and sets up the modalities of European interoperability."



Eric Jorgensen, Motor Vehicle Division Director at Arizona Department of Transportation, USA

"Whether state to state or country to country, cooperation and standards such as ISO standard for Mobile Digital Licence are very helpful."

"We're now looking even beyond that and what other standards need to be in place, from not just a technology standpoint, but from a vetting standpoint, from an acceptance standpoint, from a policy standpoint. We are working with groups to understand what these standards would look like for us. International standards are important for the future of identity."

USE CASE #1

MOBILE DRIVER LICENCE (MDL) INTEROPERABILITY IN ARIZONA AND AUSTRALIA

ISO/IEC 18013-3 standard on mobile driver licence defines the communication protocols to enable authentication and validation of a mobile driver licence app. International recognition and interoperability are especially essential given the nature of drivers licence, used worlwide. MDL and ID verifier apps are often not provided by the same supplier, particularly at an international level of interaction. However, smooth engagement between these two devices must enable a frictionless experience.

Many public transport authorities were involved at a very early stage in the definition of the ISO standard, such as the Australia Queensland TMR department and US AMVA authorities. They were able to express their pain points to best address them, as well as gain visibility on the latest features and protocols to better anticipate and have a clear vision on next steps.

USE CASE #2

TOWARDS AN INTEROPERABLE FRAMEWORK IN LATIN AMERICA

CLARCIEV, the Latin American Council for Civil Registration, Identification, and Vital Statistics organization is working towards standardization and interoperability between national registries and identification solutions from each countries.

Their ultimate goal is to build a framework inspired by eIDAS in Latin America but based on biometrics, which is not currently the case in Europe. Indeed, Latin America countries such as Colombia, Argentina, Ecuador, Peru and Chile have started building their digital identity schemes around biometric databases.

USE CASE #3

OPEN STANDARDS IN NIGERIA TO CAPITALIZE ON EXISTING INFRASTRUCTURE

Nigeria is building its digital ID framework on open standards such as ISO/ICAO specifications for data layout, FIPS Level 2 and NIST specifications for PKI and Encryption, OSIA and GDPR for API compliance.

The Nigeria MobileID ecosystem will be based on a very robust backend system replete with tokenization, non-repudiation, biometric authentication via Face Recognition, blockchain-driven time stamping and auditing, and of course, OSIA-friendly REST API interfaces.

MAIN REASONS TO INTEGRATE INTERNATIONAL REGULATION & STANDARDIZATION BODIES

1 Ensure legal framework recognizes digital identity and regulates citizens data privacy.

2 Use open standards and ensure vendors and technology neutrality.

3 Get involved in international regulation and standardization bodies to have a voice in the definition of standards and stay one step ahead.

4 Look for inspiration thanks to successful identity frameworks.

INSIGHT #8

THINK MOBILE FIRST

> "We think that the future will be mobile. The main argument to support our choice to change to the mobile ID is the usability."

Sylvan Fux, Head of Business Consulting Finance/Justice and E-Government, Liechtenstein

> "Gradually, digital or mobile credentials will prevail when there will be more confidence in the security aspects."

Mory Camara, President of IIC (Identity Council), ID4Africa

Over the last decade, digital ID schemes have been gradually going from physical digital ID forms to 100% mobile ones, a trend reflected throughout all our interviews. Mobile identity can take several form factors, from 100% dematerialized solutions to simple SIM-based solution and mobile app, or digital ID wallet applications.

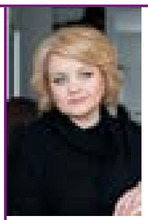
In their tenders, governments now require a strong mobile component from their solution provider to ensure better adoption, in sync with worldwide mobile and smartphones penetration, privacy for sharing of necessary attributes for user identification, user-friendliness for faster enrollment and credential issuance, and resilience throught the live update of identity attributes and easier, secure and cost effective replacement in case of credential loss. Mobile applications also leverage on the plethora of functionalities provided by mobile devices, such as contactless functionnalities with NFC, Bluetooth or biometric features. Digital IDs that began in the early 2000's with physical tokens are now all shifting towards mobile first strategies.

Mobile ID technology and devices are increasingly secure, using whitebox cryptography security mechanisms, Trusted Execution Environments or soon leveraging on eSIMs. For high level of assurance and sensitive use cases, physical smart alternatives remain necessary. In the future, mobile credentials and physical smart credentials should continue to coexist.

THEIR OPINION ABOUT MOBILE ID

Margus Arm, Deputy Director General, Estonian Information System Authority, Director of State Information System Branch

"I think that if I would start from scratch today, I would not do the ID card anymore. I think it should be something based on the mobile phone, it is not easy to distribute the card, all the updated software. It is impossible to cover all the citizens. I think all new schemes must be based on the mobile phone and biometrics because it is always with you."



Jana Krimpe, Co-Chair at GANMI - Global Alliance for Mobile National Identities.

"We see e-SIM [virtual SIM card] as a potential trusted alternative to cloud based solutions in terms of cryptography, when there are still a lot of concerns with the security and control of cloud signatures. e-SIM has the potential to be more secure with the possibility to implement a variety of cryptography and switch to another technology if one is compromised. The only challenge is standardization."

Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)

"In the coming years, citizens could have both a physical smartcard at home and a smart credential stored in their digital wallet, a network or a trusted agent."

Christopher Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland, Australia

"COVID showed the importance of our app, with a contactless validation of identity enabled by our digital licence, but also the possibility to easily register who was at a nightclub or a party in case of a contamination. It is better than a plastic ID card, or to share a pen and write down names on an attendance list. We are about to extend this service to restaurants."

USE CASE #1

MOBILE ID FOR MORE FLEXIBILITY IN LIECHTENSTEIN

Launched in April 2020, eID.li is the new smartphone app digital identity of the Principality of Liechtenstein with which Liechtenstein citizens and residents as well as foreign nationals can securely identify and log in to electronic government services and authenticate by using biometrics.

The Liechtenstein government is phasing out its inital smartcards and replacing these with Mobile ID for several reasons:
> more flexibility and reactivity in case of technical or security issues
> live-checking of attributes.

> "Mobile solutions also allow us to live-check the users attributes with our database. It is not based anymore on a signature on the smartcard, because the mobile ID does not store any data on the phone. It always retrieves the latest information on the database. If someone marries or moves to a new place, there is no need to reissue a new card."

Sylvan Fux, Head of Business Consulting Finance/Justice and E-Government, Liechtenstein

USE CASE #2

AZERBAIJAN OPTED FOR THE SIM-BASED SOLUTION

The Azerbaijani mobile ID, named Asan İmza, is a SIM card connected to 3 different certificates (citizen, businesses, civil servants) equal to a physical ID-card in the electronic environment.
The mobile ID can be used as a form of secure electronic ID to prove identity and digitally sign documents. The user has only one PIN code, no matter which certificate is used, for authentication and signing.

> "All people can use mobile phones, even if they have a low general literacy. A SIM card-based solution has the advantage of working in all types of network systems, starting from 2G. The penetration of smartphones is not going as rapidly as we want to admit. Internet is still quite expensive and the accessibility to a good high-speed internet is also a big question. An SMS based solution works much better, especially for developing markets."

Jana Krimpe, Azerbaijan Public Private consortium representative

USE CASE #3

A 100% DEVICE FREE STRATEGY FOR ITALY'S SPID

The Italian Public System of Digital Identity (SPID) is a digital identity scheme managed by the "Agenzia per l'Italia Digitale" (AgID) and financed by 9 private accredited identity providers.

SPID is the first digital ID to have passed the eIDAS notification procedure with no cards and no tokens. It has been designed to be 100% device free, with the exception of the smartphone. Some alternatives are possible for high levels of authentication, for which a HSM (Hardware Security Module) is required.

> "SPID is also compatible with smartcards such as the electronic identity card, to get a high level of assurance, but it is not used often because you need to buy a smartcard reader, or at least a smartphone with NFC technology, which is not easy for the older populations because they don't always have the skills."

Andrea Spallacci, Project Leader, Agenzia per l'Italia Digitale (AgID)

WHAT DOES THINK MOBILE FIRST MEAN?

1 Take advantage of mobile functionnalities and embarked latest technologies (NFC, Bluetooth, Biometrics) to offer enhanced user experience with advanced features such as remote enrollment, biometric authentication, privacy mechanisms, new IoT opportunities, etc.

2 Offer a smooth user experience with a mobile first approach and combine both physical smart credentials such as smartcards with mobile ones whenever needed to reach higher security when sensitive use cases requires it.

3 Software-based Mobile IDs are independant from Mobile Network Operators, which can be an important decision factor for some countries.

4 Benefit from high go-to market flexibility with mobile apps, by nature scalable, enabling governments to add more features as they go along (ex: covid features were integrated in Digital ID Wallets).

INSIGHT #9

IMPLEMENT AGILE AND ITERATIVE PROCESSES – AND BE EXPLICITE ABOUT IT

Development and processes for Digital Identity implementation worldwide are changing in a bid to keep up with fast evolving technology and uses. Agile is a new mindset and methodology that delivers value as fast as possible with incremental steps, each step delivering valuable improvements or additional features. Several governments have adopted this approach to develop their digital ID projects, releasing early versions of their digital ID (called MVP for Minimum Viable Products) to integrate user and stakeholder feedback.

Digital Identity project team members and government officials have identified having an agile mindset as a key success factor, for several reasons:

> Agile integrates user feedback and technical tests more frequently, avoiding a long development tunnel which could result in a solution encountering non-anticipated technical problems or risking being obsolete when it is released.

> Running pilotes and "minimum viable products" help identify not only technical problems but also legal, political and cultural painpoints.

> Pilots are powerful demonstrators, showcasing successful use cases and customer satisfaction to onboard future partners and stakeholders.

"One of the challenges will be to make people understand that we are in a digital application and that therefore, by definition, there will be upgrades, successive versions. This is not easy to understand, neither for the user, nor for public sponsors, who are used to declining an offer for a need in a more traditional and stable approach."

Valérie Péneau, Director of the interministerial program France Identité Numérique

THEIR CONVICTIONS ABOUT AGILE PROCESSES

Michiel Van der Veen, Director Innovation & Development at the National Office for Identity Data, The Netherlands

"In the Netherlands legislation is such that it's very difficult to experiment, and that hinders innovation. Digital identity is not something you can develop from an ivory tower and from a policy perspective, you also have to experiment and learn, hand-in-hand with the policy development."

Herbert Leithold, Secretary-General Secure Information Technology Center, Austria

"The main takeaway from the pilot we are doing on cross border services and digital ID is to know, more than the technical challenge, all the other issues we will face, like the legal, the data protection issues, etc. Then, we will know what to work on."

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products, GovTech Singapore

"Three years ago, I would not have been able to tell you exactly what trust services we would provide and who would use these services on our National Digital Identity platform. We had a broad vision, an idea, a gut feeling. We need to accept that it's impossible to predict the future and we don't have all the answers. So we had to be very agile - and that means being able to listen to and understand the gaps, problems and inefficiencies of the target market, being responsive to these needs and quickly capture those opportunities. It has been an exciting journey for us."

"It's not easy to be agile, it requires all our processes to be agile: from governance to procurement, to how we do funding, to product development. For example, about five years ago, GovTech Singapore started to rebuild its own engineering capabilities, instead of relying on outsourcing our projects. With our own engineering capabilities, we are now in better control of our product management and development processes, allowing us to be more responsive to the needs of our citizens and businesses."

USE CASE #1

QUEENSLAND GOES FOR AN AGILE APPROACH

In 2016, the Queensland Department of Transport and Main Roads (TMR) released its Digital Strategic Plan 2016-2020, with a clear priority given to connecting customers and powering delivery.

Queensland TMR is one of the very first public entity to implement Agile methodology and put it at the heart of its tendering process for digital ID. The Digital License App was developed by using a co-design process and a 4-week sprint with various technology vendors. The Agile-SCRUM methodology helped develop a complex wallet-style software, which hosts various digitalized documents in a user-friendly interface app, through an iterative approach based on regular customer feedback.

Tests with end user panels were performed at the end of each sprint and throughout the software development lifecycle to assess and increase desirability and use. Adapting tendering and procurement process towards more agility is key to delivering efficient, transparent, and cost-effective public services to citizens, and many governments are embracing these new methodologies.

USE CASE #2

ALICEM MOBILE APP IN FRANCE, AN IN-HOUSE EXPERIMENT

The Alicem Mobile application is an innovative experiment launched in 2019 with limited functionalities and scope. This experiment was instrumental in gathering feedback on technical bricks (under the CNIL[1] and ANSSI[2] control), user feedback and legal frameworks as well foster societal debates on biometric data, face recognition, discriminatory biases and inclusion.

Feedback was useful to adapt the tender specifications and confirmed the move towards a mobile application enabling secure identification and authentication, with a desktop version later.

"Choose an agile development mode, allowing us to gain in reactivity and to be in a perspective of constant improvement of the solution, in very close connection with user feedback and those of the community."

Valérie Péneau, Director of the interministerial program France Identité Numérique

[1] CNIL: French public authority responsible for the protection of personal data

[2] ANSSI: National Cybersecurity Agency of France

USE CASE #3

MYINFO PILOT, A SHARING DATA PLATFORME, IN SINGAPORE

The MyInfo pilot, a data sharing platform within the National Digital Identity (NDI) of Singapore, was launched in 2018 with several banks primarily for eKYC use cases. Within two years of the pilot's success, more than 300 private sector services are now relying on MyInfo to streamline their customer onboarding experience and build greater customer trust.

"These cross border pilots are not meant to focus on exploring technical implementation approaches - the technical part is usually quite straightforward. But through these pilots, we hope to start learning about differences in legislation, standards and other contexts, so that we can look at ways in which to bridge these differences to achieve mutual recognition."

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products, Singapore

BEING AGILE MEANS TESTING BUT ALSO CHANGING MINDSETS, STARTING IN-HOUSE

1 Revamp in-house engineering capabilites (product management, product development, architects, etc.) within the Digital Identity task force to be more responsive and agile, to complement external partners.

2 When working with external partners, have internal teams co-construct and mutually benefit and learn from respective competencies and skills.

3 Adopt an agile approach in procurements, processes and implementation by testing and doing pilots - and educate and communicate about it – not only to the public (citizens and businesses) but also to all stakeholders (administration, partners, relying parties, etc.). Agile is a new mindset and it takes considerable time to change habits.

4 Select technology based on standards to ensure interoperability and gain in flexibility and responsiveness.

INSIGHT #10

IMPLEMENT ADPATIVE & MODULAR INFRASTRUCTURE TO BRIDGE PAST AND FUTURE

Starting points and past IT legacy are different for every country, explaining the diversity of Digital Identity schemes, from centralized to federated. While some countries can rely on robust foundational identity systems, starting with a secure and digitized national register of their population, others that are just now enrolling their population are choosing to leapfrog directly to more decentralized models.
Regardless of these initial contexts, the endgoal for every country remains the same - creating robust and trusted digital identity ecosystems. This holistic approach to identity is challenging but necessary on a many accounts. The difficulty lies in evolving from a closed and secure database, to an open, flexible and scalable infrastructure, capable of easily integrating new private and public services, new credentials and new emerging models, such as Self Sovereign Identity.

Governments will have a pivotal role in enabling such an ecosystem by being a trusted credential and identity issuer, by creating the regulatory space for innovation, and by providing legal framworks and standards.

"We do have a legacy of systems that we have to work through, and we are not starting at the beginning. We have to do it in a way that works with the old, bridges to the new and makes room for what comes after, from a global digital economy perspective."

Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)

THEIR CONVICTIONS ABOUT DIGITAL ID INFRASTRUCTURES

Michiel Van der Veen, Director Innovation & Development at the National Office for Identity Data, The Netherlands

"The speed of innovation is so fast at the moment that the technology that you have today will be outdated in five years. Our view, as a government, is to develop not just a system but a digital identity ecosystem and the boundaries and conditions which are needed by this ecosystem."

"Our government acts as an authoritative source of trusted information, to bring trust in the digital economy. In the Netherlands, we introduced the notion of what we call a digital source identity: a legal piece of information, which makes secondary identification, applications and systems possible. It's a kind of building block in the digital economy."

Margus Arm, Deputy Director General, Estonian Information System Authority, Director of State Information System Branch

"What is important to see in our scheme is that we don't have a unique big centralized database, but thousands of them. If a relying party wants to join the ecosystem, they just purchase the X-Road platform, and they use the protocol, there is no need to replace their legacy IT system and databases."

"It over-killed startups to implement X-Road platform. We are looking for alternative solutions– startups need a secure and standard alternative to X-Road."

Eric Jorgensen, Motor Vehicle Division Director at Arizona Department of Transportation, USA

"Our architecture used to be based on a mainframe system, which has its benefits but was not flexible enough to adapt to changes and modern demands. We decided to change our technology with a modular architecture. When we built our system, we always thought about where we will be able to plug the next piece of technology even if we do not know what it is. It is a change in our philosophy."

USE CASE #1

A BROKERED HUB IN DENMARK FOR MORE MODULARITY

For its third generation of Digital Identity (MitID), Denmark co-financed with the financial sector security-enhanced infrastructure by limiting its access to certified brokers only. The brokers will manage the technical interface and sell their services to services providers.

This modular infrastructure is expected to solve integration and security issues thanks to its inherent modularity. Credentials can be plugged and unplugged according to user's needs and evolving technology, and small services providers will be able to integrate MitID without having in-house IT skills.

"It makes more sense to have a few number of brokers who have the capability to manage the technical infrastructure security and integration."

"We wanted to be able to constantly modernize and update the infrastructure: there will probably be quite a lot of technical changes over the years."

Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

USE CASE #2

DIGITAL ID AS A MODULAR TOOL FOR THE PRIVATE SECTOR TO BOOST THE DIGITAL ECONOMY IN INDIA

Aadhaar was designed from the beginning with open services and protocols that can extend to the private sector and boost the digital economy. Different functions are based on the scheme, with an open API that allows business to do eKYC check against the Aadhaar database, for proof of address or other biographic or biometric attributes. The data is always shared with the consent of the applicant.

Since March 2019, private organizations are charged US$0.007 for Aadhaar authentication (for a yes/no challenge), and US$0.3 for e-KYC transactions. In 2018, a total of 4.9 billion e-KYC transactions have been done through Aadhaar.

USE CASE #3

A MODEL AGNOSTIC FRAMEWORK TO SECURE DIGITAL TRUST IN CANADA

The Digital ID & Authentication Council of Canada (DIACC) is developing the Pan Canadian Trust Framework, with the collaboration of both public and private stakeholders.

The framework's goal is to map and identify where technologies and legal policies intersect. It is meant to be model agnostic and will be applicable for any existing (federation, brokered hub, etc.) or emerging models (distributed ledger blockchain, Self Sovereign Identity).

"Portability of the credential in different ecosystems will become essential as well as interoperability based on different technologies, but same standards such as W3C."

Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)

FACILITATE TECHNICAL INTEGRATION BY CREATING AN ENABLING ENVIRONMENT

1 Adopt a modular architecture to increase the flexibility of the ecosystem and make the technical integration easier for the service providers. For example, delegate the integration with a brokered-hub approach.

2 Obtain true interoperability that works around multiple technologies. For credentials and identity providers, adopt a plug-n-play approach to follow the users' needs and constantly modernize and update the infrastructure.

3 Be technology neutral and follow guidelines that define minimum requirements, as well as international and open standards.

4 Create an enabling environment in terms of innovation, policies and regulation to create an ecosystem: keep policy and regulatory scheme in pace with safe and pragmatic innovation.

INSIGHT #11

PROVIDE USEFUL & RECURRING SERVICES BY PIGGYBACKING ON PRIVATE SECTOR

Return of experience from national digital identities which have progressively opened their access to private service providers is unanimous: providing useful and recurring online services (2-3 times a month) for citizens is key to create an adoption momentum - and private sector services are a key accelerator.
Most digital identities, launched and financed by governments in the context of their e-government programs, had an initial focus on providing free online public services to citizens, such as online tax declaration, access to retirement rights, etc. Over the years and even more so during the COVID-19 pandemic, time-efficient and more recurrent public services were made available online, such as education portals on which parents can regularly connect to access their children's grades. Digital ID gradually opened access to private sector services.

Online banking services have proven very successful in creating traction, recurring visits and boosting adoption. Encouraged by these results, many digital IDs - Singapore, Australia, France – are integrating new private actors, at different levels (from national banks, insurance, MNO's to local restaurants, bars and nightclubs). This trend has taken so much momentum that international regulation bodies such as eIDAS in Europe are currently leading public consultations to extend interoperability to the private sector and improve the usability and adoption of eID solutions.

"If we hadn't had the dissemination that we got with working with the banks, we would never have dared to make digitization mandatory."

Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

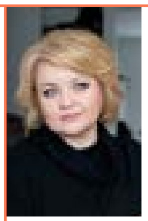
WHAT DO THEY THINK ABOUT OPENING TO PRIVATE SECTOR SERVICES?

Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products GovTech Singapore

"Issuing everyone a digital identity is not just a means to an end. Our focus is on the use cases – how can digital identity bring direct benefits to consumers and businesses. We work in close partnership with the industry to identify these use cases and making it a reality, I think that is what we are the most proud of."

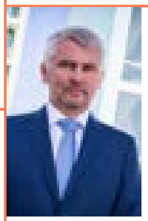
Andre Vasconcelos, eID Advisor to the Board of Directors, Administrative Modernization Agency, Portugal

"We had partnerships with associations and movements to push the digitalization of the society and present the Digital Mobile Key (CMD), which helped us build trust and connections with the private sector. However, the major driver to private sector adoption was not so much the promotion of the CMD, but the added value. That's why they decided to invest and change their systems, because they see a return on their investment."



Jana Krimpe, Azerbaijan Public Private consortium representative

"It is too difficult to create new user behaviors concerning digital services if the users access services only once a year. It is important that people access at least several times a month."



Margus Arm, Deputy Director General, Estonian Information System Authority, Director of State Information System Branch

"One of the best incentives we had for adoption of our digital ID is the fact that if people did their tax declaration on paper, they had to wait for their tax refund for three months. But with an online tax declaration using the ID-Card, the waiting time was reduced to 10 days. It was an easy decision for many users."

"It is essential to cooperate and involve the banks because people log in into their own online bank at least once a month or once a week to pay utility bills, ect. In Estonia, almost 75% of the transactions come from the financial sector: banks and insurance companies."

USE CASE #1

A WIN-WIN STRATEGY FOR PUBLIC AND PRIVATE SECTOR WITH THE CMD IN PORTUGAL

The Digital Mobile Key (CMD) launched in 2014 by the Portuguese Government was opened to the private sector from the date of launch. However, real interest really started once adoption reached around 1 million Portuguese - 10% of the population.

The main added value benefits of using the CMD for the private sector are authentication services and qualified electronic signatures, especially since these services are currently free for any relying party (except for costs of SMS for OTP). During the COVID-19 outbreaks, banks and telcos were able to identify and enroll new customers, as well as authenticate existing ones.

Used to secure authentication processes since the eID Citizen Card to access government e-services in 2007, citizens are now pushing for the private sector to provide same levels of security.

USE CASE #2

NEW SECTORS OF ACTIVITY AVAILABLE SOON THROUGH FRANCECONNECT

FranceConnect, a digital Identity federator, connects users to 800 public and private services, through the identity provider of their choice.

To boost adoption, services with more frequent use will be integrated in the FranceConnect ecosystem by 2021, such as housing subsidies (CAF), unemployment benefits (Pôle Emploi) or access to school report cards online. Integrating new private services with sector specific regulations such as medical e-consultations, car sharing platforms or real estate agencies is both a challenge to overcome and a priority for the future of FranceConnect.

"We are currently launching an experiment to bring in new sectors of activity that are not currently eligible in FranceConnect (passenger transport, medico-social, real estate rental, car rental, etc.)."

Lionel Fouillen, Partner Relations Manager, FranceConnect

USE CASE #3

PARTNERSHIP WITH BANKS FOR WIDESPREAD DISSEMINATION OF NEMID IN DENMARK

NemID, a code card or code application (soon to be MitID) was launched in 2010 by a unique cooperation between the Danish Agency of Digitization and Danish banking sector (Finans Denmark) to enable citizens to use their public e-ID for online banking. Providing these services were instrumental in creating dissemination and frequency of use for Danish citizens, and a necessary step before making NemID mandatory. Today, the adoption rate is close to 100%.

"The main value of joining up with the financial sector is certainly to have this dissemination and the frequency of use - without this frequency of use, digitization could not have been made mandatory."

Charlotte Jacoby, Head of Office for Division for Infrastructure Development, Denmark

PROVIDE RECURRENT AND USEFUL SERVICES TO BOOST ADOPTION

1 Provide useful online services for citizens that create a real difference in day to day use, efficiency, time and cost savings. On the other hand, avoid prioritizing intrusive and limitative use cases that concern a small category of the population.

2 Prioritize access to services that have a high frequency of use, such as online banking services, which are used several times a month or even week.

3 Work hand in hand with relying parties that know their customers and encourage them to come with their identified use cases.

INSIGHT #12

PROVIDE A SECURE, EASY AND MULTIPLE ENROLLMENT PROCEDURE

"Italian citizens are very happy about these remote procedures. There is no opposition. Due to the pandemic, there has been a strong increase in requests for authentication procedures. They don't want to go into a private company or a government office and stand in line to get an identity."

Andrea Spallacci, Project Leader, Agenzia per l'Italia Digitale (AgID)

The enrollment procedure involves capturing and recording key identity attributes from a person who claims a certain identity, which may include biographical data (ex: name, date of birth, gender, address, email), biometrics (ex: fingerprints, iris scan) and an increasing number of other attributes (*"Technical Standards for Digital Identity", ID4D, 2017*). Enrollment is key to the creation of a trusted digital identity

A secure, convenient and quick enrollment process is key for digital identity go-to market and wide spread adoption both for citizens and for businesses, especially in a context where online services are not mandatory. It is a decisive moment where trust is established between the user, the solution provider and the government.

Today, most enrollment procedures require physical presence for enhanced security reasons but some countries such as Italy, the United States or the Netherlands provide options for remote processes and more and more countries are testing remote face verification technologies.
To authorize remote identification and counter attacks and fraud by presenting fake subjects, counterfeit or fake documents, video manipulation and lack of user identity verification by an agent, eIDAS is currently working onproviding better guidance, standardisation and conformity assessment practices for the use of these technologies (*"eIDAS COMPLIANT eID SOLUTIONS, Security Considerations and the Role of ENISA"*, March 2020).

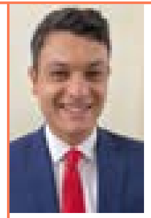
THEIR CONVICTIONS ABOUT ENROLLMENT PROCESS

Margus Arm Deputy Director General, Estonian Information System Authority, Director of State Information System Branch

"Our security is based on a secure enrollment process. A lot of the trust is based on our secure face-to-face enrollment process. In the future, maybe there will be a possibility to enrol people remotely. However, we currently require a face to face enrollment because we think that it is the only way to guarantee the highest level of security required for use cases such as i-voting."

Jana Krimpe, Azerbaijan Public Private consortium representative

"During the COVID crisis, we increased the number of physical enrollment points - banks can now issue mobile ID in Azerbaijan - so that people get their SIM card and certificates in one single place. We redesigned the whole process to simplify it with only one page agreement to avoid bureaucracy features from the past. In the near-future, we will be implementing the full remote online enrollment process."



Andrea Spallacci, Project Leader, Agenzia per l'Italia Digitale (AgID)

"SPID was the first notified scheme in Europe to have remote onboarding process. Our point of view was different from other member states. eIDAS initially required the physical presence of the citizen during the onboarding/registration. We stronly believe that the physical presence is guaranteed even if it is through a display, because physical presence does not mean the possibility to touch the applicant."

Aziz Aliyu, Head of the National Identity Management Commission (NIMC), Nigeria

"We hope that we will have more than 90% of the population enrolled by 2023. To reach this ambitious objective, we developed a legal framework for the registration process in 2017, with several guidelines that will allow many private companies to be certified to become enrollment centers and reach the whole population."

USE CASE #1

ALICEM, A SECURE ENROLLMENT BASED ON FACE-RECOGNITION

In 2019, the French government launched the test phase of the Alicem app, a new authentication method for FranceConnect, the French Digital Identity scheme.

The Alicem experiment tested a deviced-based face recognition technology to facilitate enrollment. Users could utilize their NFC (Near-field Communication) enabled mobile devices to read their biometric passport or a resident permit. Alicem compares the picture stored in the chip with a "challenge" video, shot by the user. The video is immediately deleted after the process and the comparison is done on the users' device. No user data is sent on the internet.

Once enrollment is complete, Alicem will provide a secure and simple access to the FranceConnect ecosystem, using a mobile device with associated security codes to authenticate. For certain sensitive use cases, an NFC reading of the biometric passport might also be required. In 2021, the new mobile application will also be able to rely on NFC reading of the new national e-ID card (CNIe) for authentication.

USE CASE #2

ITALY SET UP A UNIQUE REMOTE VIDEO & AUDIO ONBOARDING PROCESS

SPID was the first eIDAS notified scheme to have an audio and video remote process for citizen enrollment (vs. physical presence) with a live validation by an operator, which takes around 20 minutes. Satisfaction rates concerning remote onboarding are extremely high among Italians, with a sharp increase in requests for authentication procedures during COVID-19 outbreak.

An update of the enrollment process is currently being redesigned, improving enrollment time and process (10 seconds for audio and video recording without a live operator). Citizens will perform random actions requested by the app and the operator will decide later to validate or not the enrollment process.

USE CASE #3

MULTIPLE ENROLLMENT CHANNELS CREATE LEAP IN ADOPTION IN PORTUGAL

Enrollment for the Digital Mobile Key (CMD) launched in 2014 by the Portuguese government made an impressive leap in 2018 when the Administrative Modernization Agency of Portugal (AMA) decided to create multiple enrollment channels. In addition to traditional face to face or by using the eID citizen card with a smartcard reader (mandatory since 2007 for all Portuguese citizens), two new channels are now available:
> Enroll for CMD when renewing the Citizen Card.
> Enroll for CMD when using the tax department password. Codes are sent by physical mail thanks to the address that is linked to the citizen.
> The AMA is also thinking of enabling users to enroll for the CMD through ATM's or by using biometrics with mobile apps.

"In the last two years, we changed levels. We moved from 1,000 new enrollments per month to having 4,000 per day. We did some investment on communication, but It made little difference. Clearly, the biggest difference we noticed is when we provided these three different enrollment channels."

Andre Vasconcelos, eID Advisor to the Board of Directors, Administrative Modernization Agency, Portugal

ENROLLMENT PROCESS AS A KEY ELEMENT TO DIGITAL IDENTIFICATION UPTAKE

1 Rely on the existing public and private ecosystem (public administration, bank or mobile operator agencies, etc.) and provide certification to increase the number of enrollment centers and register a large part of population. If properly organized and regulated with a legal framework and clear technical mandatory guidelines, it can dramatically increase the enrollment procedure efficiency and reduce its costs.

2 Think about online simple and fast pre-enrollment and/or enrollment procedure using audio and video to accelerate the whole process and offer a better user experience to citizen. Keep in mind that some sensitive use cases such as i-voting may require higher level of assurances.

INSIGHT #13

DESIGN A CUSTOMIZED STAKEHOLDER CAMPAIGN TO BOOST ADOPTION

The adoption rate is the most followed key indicator, revealing the accessibility, inclusivity and success - or lack of - of a digital ID in a country. Adoption can of course be nuanced by other indicators, such as active users, number of transactions, customer satisfaction, etc.

Starting points for adoption are very different for countries: some have made their digital ID mandatory, reaching close to 100% adoption, while others face additional challenges because possessing a national form of identification is not part of their country culture, or because national databases are not yet even consolidated.

Adoption comes into play long before digital ID roll-out and go-to-market. The design of the user interface and experience, the choice of the credentials, the relevance of the use cases, the simplicity of registration and authentication process - all these choices will have an impact on the adoption level and have to be thoroughly analysed before hand. Once the digital ID is designed and ready for roll-out, successful go-to-market strategies define different target groups of consumers and key stakeholders, and adapt the communication and adoption strategy accordingly.

> **"Marketing initiatives for the digital ID, with TV spots and newspapers, creates a continuous adoption but no measurable impact."**
>
> **Herbert Leithold, Secretary-General Secure Information Technology Center, Austria**

THEIR CONVICTIONS ABOUT COMMUNICATION AND ADOPTION STRATEGIES

Margus Arm, Deputy Director General, Estonian Information System Authority, Director of State Information System Branch

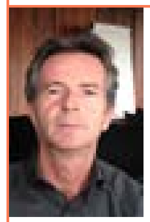
"Almost 70% of the population is using e-Id and I think it is the maximum we can reach because there are always some people who will not have access and who do not want to use it. It is impossible to reach 100%."

Sarah Kirk-Douglas, Vice President, Global Marketing & Communications, SecureKey Technologies Inc. (Candada)

"We had a marketing working group with all of the seven different financial institutions that developed Verified.Me in cooperation with us. Working with brands of trust participating in the network we were able to deliver focused marketing campaigns to educate, drive awareness and consumer adoption. We had a multiple phased approached leveraging different participants of the network with a variety of tactics. (events, PR, social media, videos, advertising, etc.)."

Andre Boysen, Chief Identity Officer, SecureKey Technologies Inc. (Canada)

"The Verified.Me go-to market strategy is based on the successful credit card model, with an issuing side (banks, government, telcos, etc.) and a acquiring side (the relying parties) for which we had a concerted effort to go out and enable partners to sign up new services and join the network. It allowed us to scale faster, and now we're building business relationships where partners can go out and sign up relying parties for us."



Lionel Fouillen, Partnership Relations Manager, FranceConnect

"There is a real communication job to be done to help the general public in their understanding of the concepts of GDPR, identity provider, data transit, security, privacy, etc."

USE CASE #1

REACHING OUT TO PROVINCES TO BOOST ADOPTION IN THE NETHERLANDS

In the Netherlands, the authentication service DigID enables Dutch citizens to securely log in the public government portal.

To ensure adoption, the Dutch Government started with a phased approach by limiting the number of service providers and waiting for a critical mass of active users before opening it to a wider range of public e-services.

In addition, a partnership program of the Dutch Ministry of the Interior and Kingdom Relations, the Association of Netherlands Municipalities, the professional associations, and the lobby organizations, was put in place to reach citizens in different provinces and boost adoption. To help citizens in their DigID application and usage, online and face to face courses (4 sessions of 2 hours each) are taught by specially trained teachers in libraries in each province to facilitate local access for every citizen.

USE CASE #2

POPULAR PETITIONS TO INCREASE UPTAKE IN AUSTRIA

The first eID program was launched in 2003, with 3 main milestones for takeup:

> e-government portals started introducing user friendly registration process.
> digital by default strategy to access pension records and social security. The government sent a letter to Austrian households and urged citizens to create their e-ID to access their pension records online even though the offline alternative was still active.
> using eID for signing popular petitions (to ban smoking and increase womens rights). Daily activation increased from 2000 per day to 10 000 per day.

USE CASE #3

A TWO-SIDED GO TO MARKET STRATEGY IN SINGAPORE

To drive adoption of the national digital Identity (NDI), the Government Technology Agency of Singapore GovTech (GovTech) have to consider a two-sided adoption strategy:

> the citizen adoption strategy was to be as inclusive as possible to drive adoption and collaborate with multiple agencies, media and carry out roadshows to increase digital skills of the elderly and lower income families.

> the business adoption strategy is to first make onboarding as simple and developer-friendly as possible, and also to celebrate the successful use cases so as to demonstrate the value and possibilities to other businesses.

ADOPTION AND COMMUNICATION STRATEGIES TO ADOPT

1 Progressively roll-out Digital ID by starting with a priority target group (citizens, big business, small and medium business, civil servants, etc.), show positive results and continue roll-out.

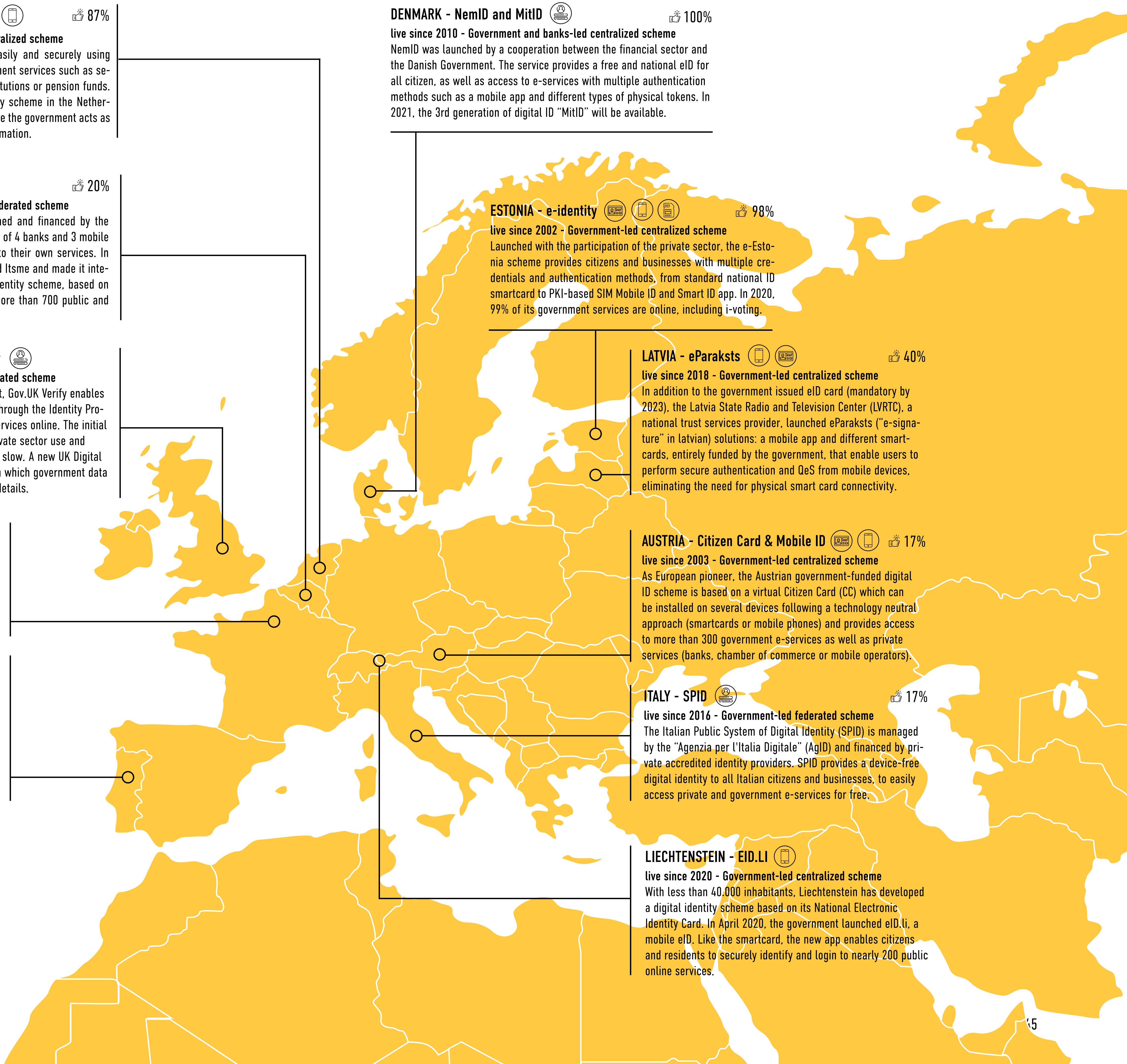
2 Target strategies and campaign according to key stakeholders - not only consumer targets but also key political, legal, compliance stakeholders and key industries.

3 Introduce "digital by default" strategies on popular services (petitions, pensions, taxes, etc.) once online services are up and running.

4 Carefully select the communication elements and angles: a high security and privacy angle may not be the most efficient, communicate rather on utility and user benefits.

COUNTRIES DIGITAL ID SCHEMES

STUDIED COUNTRIES IN EUROPE



THE NETHERLANDS - DigID 👤 📱 👍 87%

live since 2003 - Government-led centralized scheme

Citizens and residents can identify easily and securely using the DigID app to access online government services such as secondary education and healthcare institutions or pension funds. DigID is part of a larger Digital Identity scheme in the Netherlands, an open market ecosystem, where the government acts as an authoritative source of trusted information.

BELGIUM - itsme® 📱 👍 20%

live since 2017 - Cross-industry-led federated scheme

The Mobile ID solution itsme® is owned and financed by the private consortium "Belgium Mobile ID" of 4 banks and 3 mobile operators, providing a secure access to their own services. In 2018, the Belgium Government certified Itsme and made it interoperable with the regalian national identity scheme, based on the e-ID. Itsme now gives access to more than 700 public and private e-services.

UNITED KINGDOM - Gov.UK Verify 👤

live since 2017 - Government-led federated scheme

Initially launched by the UK government, Gov.UK Verify enables citizens and residents to authenticate through the Identity Provider of their choice when accessing services online. The initial government contract did not enable private sector use and adoption for the public sector was very slow. A new UK Digital ID scheme is currently being defined, in which government data sources can be used to check identity details.

FRANCE - FranceConnect 👤

live since 2016 - Government-led federated scheme

Launched by the government, FranceConnect is a digital identity federator that maintains and regulates an ecosystem for users, identity providers and service providers. Users can select their preferred IdP when accessing one of the 800 public and private services available.

PORTUGAL - Chave Móvel Digital 📱 👍 14,5%

live since 2014 - Government-led centralized scheme

Seven years after the launch of its eID card, the Portuguese government released the Digital mobile key or "Chave Móvel Digital" (CMD), a user centric mobile ID scheme providing simplicity and convenience to citizens and residents. It enables secure authentication on various public and private websites, requiring only a mobile phone, a 4-digit PIN code and an OTP or biometric recognition.

DENMARK - NemID and MitID 👤 👍 100%

live since 2010 - Government and banks-led centralized scheme

NemID was launched by a cooperation between the financial sector and the Danish Government. The service provides a free and national eID for all citizen, as well as access to e-services with multiple authentication methods such as a mobile app and different types of physical tokens. In 2021, the 3rd generation of digital ID "MitID" will be available.

ESTONIA - e-identity 💳 📱 ▦ 👍 98%

live since 2002 - Government-led centralized scheme

Launched with the participation of the private sector, the e-Estonia scheme provides citizens and businesses with multiple credentials and authentication methods, from standard national ID smartcard to PKI-based SIM Mobile ID and Smart ID app. In 2020, 99% of its government services are online, including i-voting.

LATVIA - eParaksts 📱 💳 👍 40%

live since 2018 - Government-led centralized scheme

In addition to the government issued eID card (mandatory by 2023), the Latvia State Radio and Television Center (LVRTC), a national trust services provider, launched eParaksts ("e-signature" in latvian) solutions: a mobile app and different smartcards, entirely funded by the government, that enable users to perform secure authentication and QeS from mobile devices, eliminating the need for physical smart card connectivity.

AUSTRIA - Citizen Card & Mobile ID 💳 📱 👍 17%

live since 2003 - Government-led centralized scheme

As European pioneer, the Austrian government-funded digital ID scheme is based on a virtual Citizen Card (CC) which can be installed on several devices following a technology neutral approach (smartcards or mobile phones) and provides access to more than 300 government e-services as well as private services (banks, chamber of commerce or mobile operators).

ITALY - SPID 👤 👍 17%

live since 2016 - Government-led federated scheme

The Italian Public System of Digital Identity (SPID) is managed by the "Agenzia per l'Italia Digitale" (AgID) and financed by private accredited identity providers. SPID provides a device-free digital identity to all Italian citizens and businesses, to easily access private and government e-services for free.

LIECHTENSTEIN - EID.LI 📱

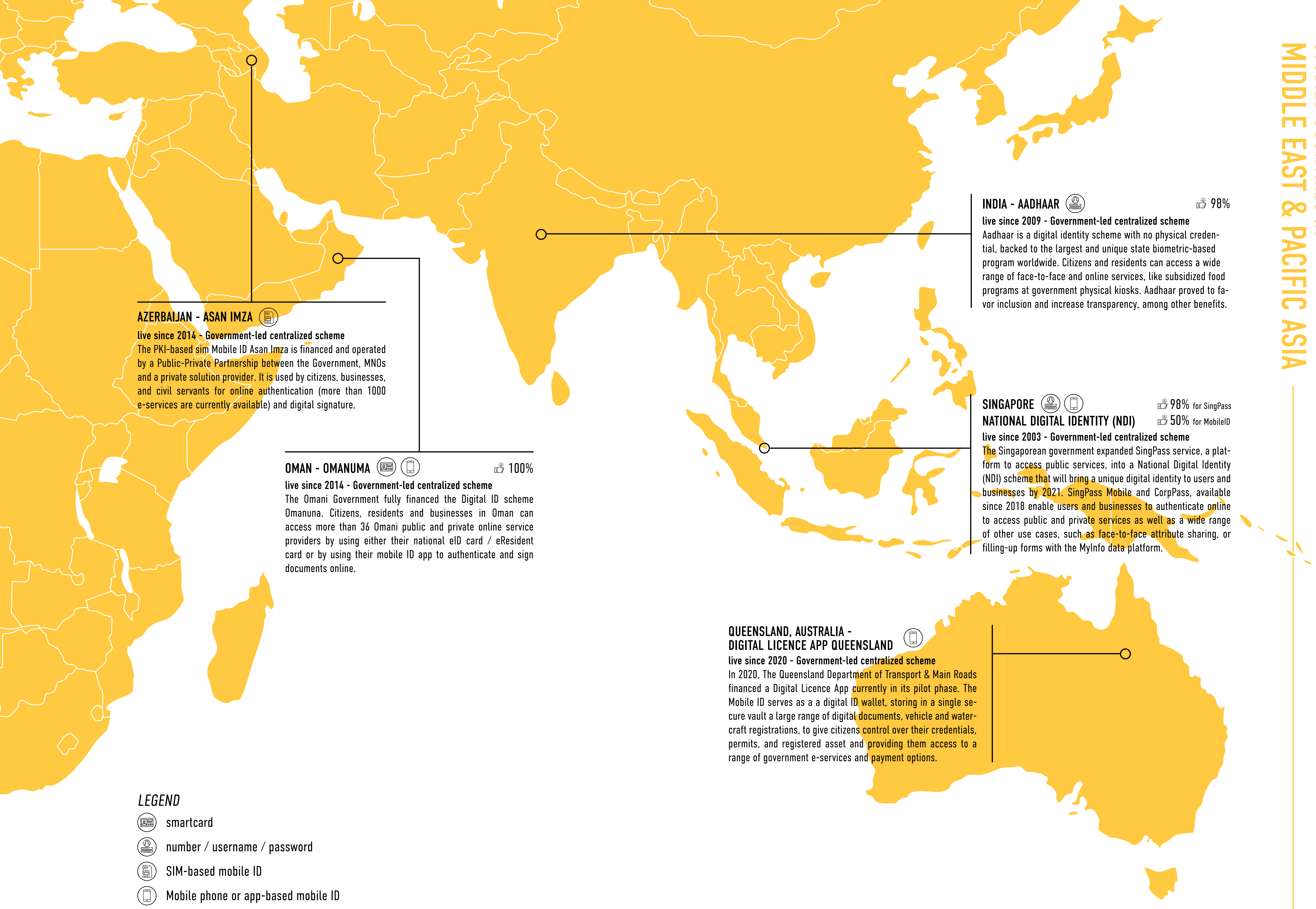
live since 2020 - Government-led centralized scheme

With less than 40.000 inhabitants, Liechtenstein has developed a digital identity scheme based on its National Electronic Identity Card. In April 2020, the government launched eID.li, a mobile eID. Like the smartcard, the new app enables citizens and residents to securely identify and login to nearly 200 public online services.

LEGEND

💳	smartcard
👤	number / username / password
▦	SIM-based mobile ID
📱	Mobile phone or app-based mobile ID

STUDIED COUNTRIES IN MIDDLE EAST & PACIFIC ASIA



AZERBAIJAN - ASAN IMZA

live since 2014 - Government-led centralized scheme

The PKI-based sim Mobile ID Asan Imza is financed and operated by a Public-Private Partnership between the Government, MNOs and a private solution provider. It is used by citizens, businesses, and civil servants for online authentication (more than 1000 e-services are currently available) and digital signature.

OMAN - OMANUMA

👍 100%

live since 2014 - Government-led centralized scheme

The Omani Government fully financed the Digital ID scheme Omanuna. Citizens, residents and businesses in Oman can access more than 36 Omani public and private online service providers by using either their national eID card / eResident card or by using their mobile ID app to authenticate and sign documents online.

INDIA - AADHAAR

👍 98%

live since 2009 - Government-led centralized scheme

Aadhaar is a digital identity scheme with no physical credential, backed to the largest and unique state biometric-based program worldwide. Citizens and residents can access a wide range of face-to-face and online services, like subsidized food programs at government physical kiosks. Aadhaar proved to favor inclusion and increase transparency, among other benefits.

SINGAPORE NATIONAL DIGITAL IDENTITY (NDI)

👍 98% for SingPass

👍 50% for MobileID

live since 2003 - Government-led centralized scheme

The Singaporean government expanded SingPass service, a platform to access public services, into a National Digital Identity (NDI) scheme that will bring a unique digital identity to users and businesses by 2021. SingPass Mobile and CorpPass, available since 2018 enable users and businesses to authenticate online to access public and private services as well as a wide range of other use cases, such as face-to-face attribute sharing, or filling-up forms with the MyInfo data platform.

QUEENSLAND, AUSTRALIA - DIGITAL LICENCE APP QUEENSLAND

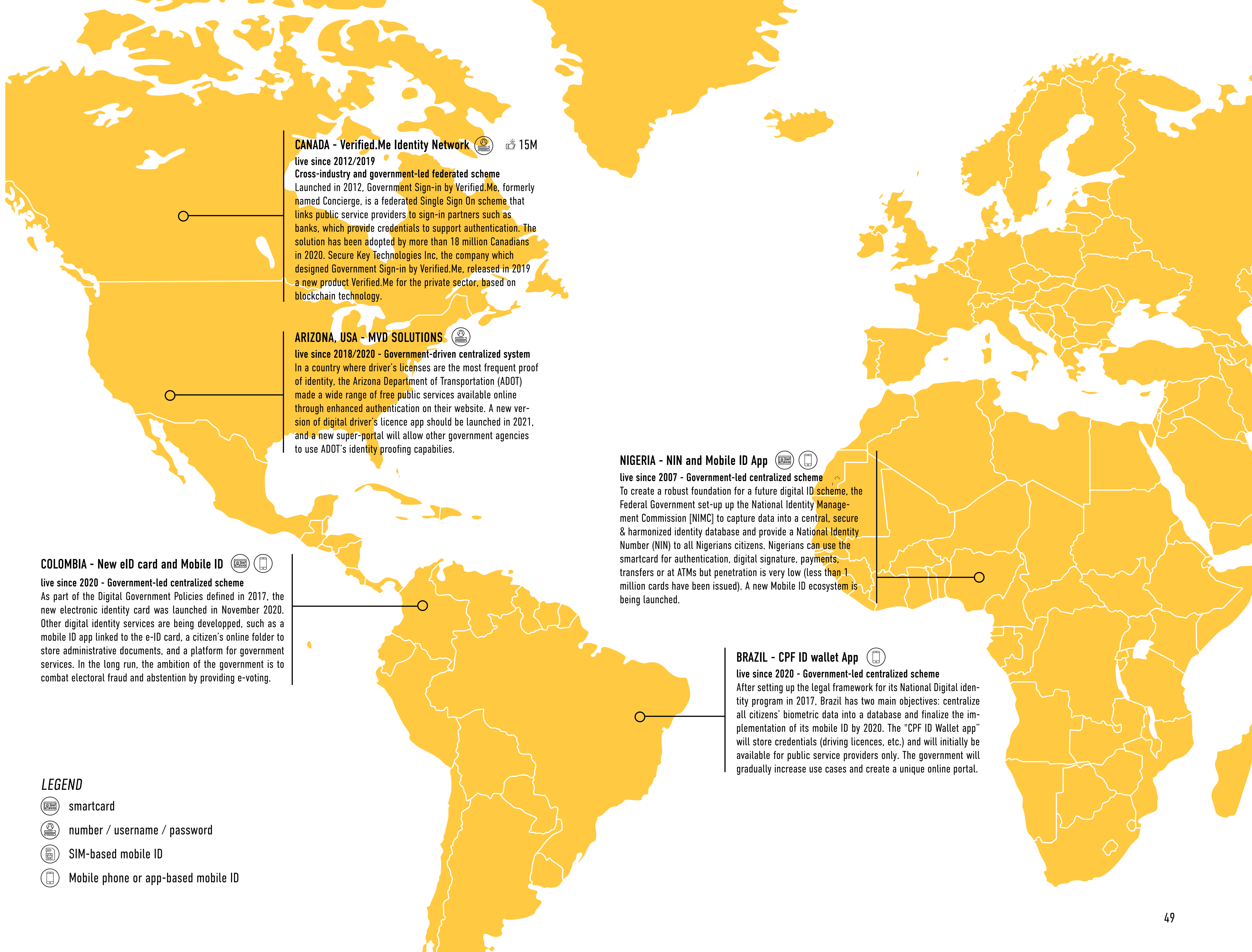
live since 2020 - Government-led centralized scheme

In 2020, The Queensland Department of Transport & Main Roads financed a Digital Licence App currently in its pilot phase. The Mobile ID serves as a a digital ID wallet, storing in a single secure vault a large range of digital documents, vehicle and watercraft registrations, to give citizens control over their credentials, permits, and registered asset and providing them access to a range of government e-services and payment options.

LEGEND

- smartcard
- number / username / password
- SIM-based mobile ID
- Mobile phone or app-based mobile ID

STUDIED COUNTIRES IN AMERICA & AFRICA



CANADA - Verified.Me Identity Network 15M

live since 2012/2019
Cross-industry and government-led federated scheme
Launched in 2012, Government Sign-in by Verified.Me, formerly named Concierge, is a federated Single Sign On scheme that links public service providers to sign-in partners such as banks, which provide credentials to support authentication. The solution has been adopted by more than 18 million Canadians in 2020. Secure Key Technologies Inc, the company which designed Government Sign-in by Verified.Me, released in 2019 a new product Verified.Me for the private sector, based on blockchain technology.

ARIZONA, USA - MVD SOLUTIONS

live since 2018/2020 - Government-driven centralized system
In a country where driver's licenses are the most frequent proof of identity, the Arizona Department of Transportation (ADOT) made a wide range of free public services available online through enhanced authentication on their website. A new version of digital driver's licence app should be launched in 2021, and a new super-portal will allow other government agencies to use ADOT's identity proofing capabilies.

COLOMBIA - New eID card and Mobile ID

live since 2020 - Government-led centralized scheme
As part of the Digital Government Policies defined in 2017, the new electronic identity card was launched in November 2020. Other digital identity services are being developped, such as a mobile ID app linked to the e-ID card, a citizen's online folder to store administrative documents, and a platform for government services. In the long run, the ambition of the government is to combat electoral fraud and abstention by providing e-voting.

NIGERIA - NIN and Mobile ID App

live since 2007 - Government-led centralized scheme
To create a robust foundation for a future digital ID scheme, the Federal Government set-up up the National Identity Management Commission [NIMC] to capture data into a central, secure & harmonized identity database and provide a National Identity Number (NIN) to all Nigerians citizens. Nigerians can use the smartcard for authentication, digital signature, payments, transfers or at ATMs but penetration is very low (less than 1 million cards have been issued). A new Mobile ID ecosystem is being launched.

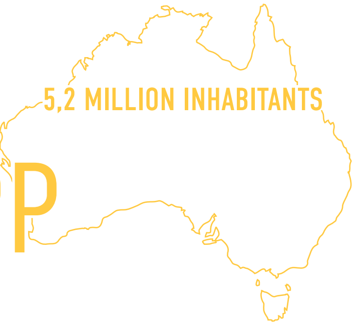
BRAZIL - CPF ID wallet App

live since 2020 - Government-led centralized scheme
After setting up the legal framework for its National Digital identity program in 2017, Brazil has two main objectives: centralize all citizens' biometric data into a database and finalize the implementation of its mobile ID by 2020. The "CPF ID Wallet app" will store credentials (driving licences, etc.) and will initially be available for public service providers only. The government will gradually increase use cases and create a unique online portal.

LEGEND

- smartcard
- number / username / password
- SIM-based mobile ID
- Mobile phone or app-based mobile ID

FOCUS ON
AUSTRALIA, QUEENSLAND


5,2 MILLION INHABITANTS

DIGITAL LICENCE APP

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

MOBILE APP (WALLET) *including driver licences, photo identification cards and recreational marine licences*

IN PILOT PHASE, WITH LAUNCH PLANNED IN 2021

✓ IDENTIFICATION *online & offline*

✓ ID ATTRIBUTES SHARING

> Face-to-face identification for over the counter Identity verification through device-to-device engagement via a QR code scan and data sharing via Bluetooth Low Energy at pharmacist, alcohol consumption, rental cars, etc.) in non connected mode (locally from phone to phone) and in connected mode (with a verification on server).
> Over the counter proof of age
> Reverse QR code for phone / skype secure access (POC phase)

✓ AUTHENTICATION

Online authentication of users to access public and private services expected in second phase

✓ ELECTRONIC SIGNATURE

The app offers a digitally signed PDF that can be sent via Text, Email or Airdrop.

✓ CROSS-BORDER RECOGNITION

Based on ISO 18013-5 standards for interoperability and cross border usage.

CONTEXT & OBJECTIVES

The Queensland Department of Transport and Main Roads launched a new Digital Licence App currently in trial in the Fraser Coast region before launch in 2021.

The main initial driver was to modernize the Queensland driver licence scheme by adding a mobile companion to the card to cope with fraud and loss of physical documents. Beyond being an entitlement to drive, a licence is also a key ID component widely used by the private industry. The project was also motivated by the ambition to provide a trusted digital ID to Queenslanders as a mean to preserve individuals' dignity, enabling access to everyday essential services and much more.

VALUE PROPOSITION

The Digital Licence App Queensland is a mobile application which also serves as a digital ID wallet storing a large range of digital documents, vehicle and watercraft registrations in a single secure vault. It is intended to give all Queensland citizens, from all background and communities, control over their stored credentials, permits and registered asset and providing access to a range of government eServices and payment options.

OTHER SPECIFIC SERVICES & USE CASES:
> Confirm eligibility to disaster relief (bushfire, floods) and payment
> COVID compliance in nightclubs, restaurants
> Payment functions are expected soon (especially for business)
> Registrations will be available for a large range of vehicles and watercraft

BUSINESS MODEL: GOVERNMENT FUNDED

> Government funded digital ID seen as the most efficient model to avoid a 30% premium on the cost if outsourced by private sector and there would be regulatory and privacy barriers to overcome.
> Only public agencies can add credentials and digitalized documents to the wallet app
> The private sector can become relying parties and use the app as a validation tool for their own services
> ROI of the project is measured in terms of cost efficiency, fraud avoidance, once a number of government credentials are integrated into a single platform

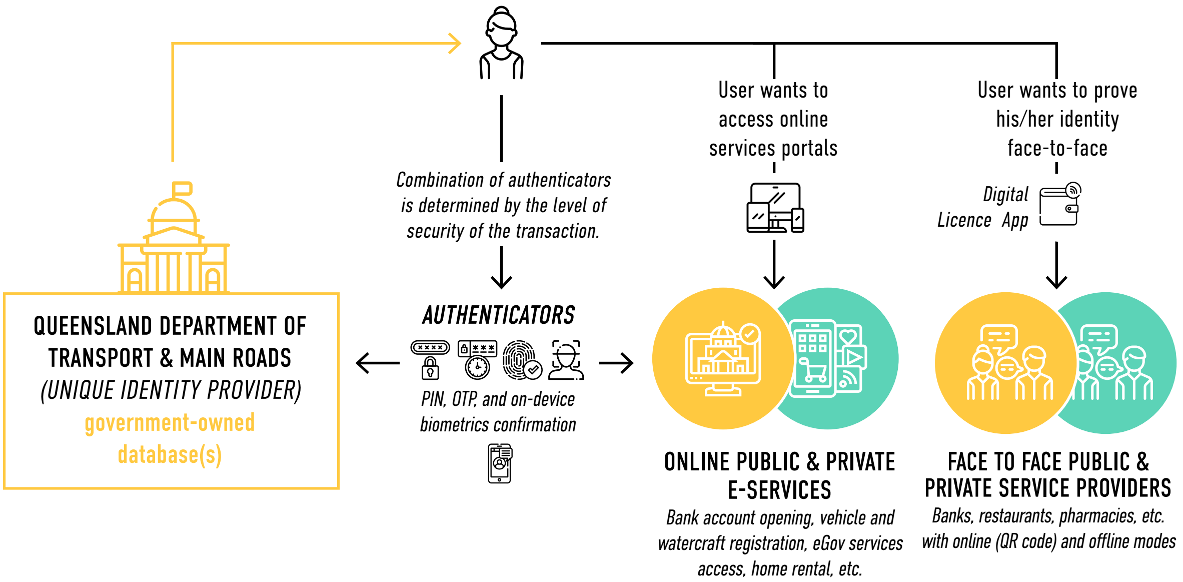
SECURITY & PRIVACY CHOICES

> The Digital Licence App and Reader App are both compliant with the Information Privacy ACT and specific confidentiality provisions in transport legislation.
> The model is based on consent based data sharing
> The app is based on multi layered security mechanisms and went through security pen-testing.

PROJECT MILESTONES

Nov. 2018	Summer 2019	2020	2021
Start of prototyping & codesign	Pre-pilot with intensive community engagement, digital ambassador program, roadshow, etc.	Pilot launch Accepted as a legal form of ID	Launch of Queensland Digital ID Wallet

DIGITAL LICENCE APP QUEENSLAND ECOSYSTEM


User wants to access online services portals

User wants to prove his/her identity face-to-face

Combination of authenticators is determined by the level of security of the transaction.

Digital Licence App

QUEENSLAND DEPARTMENT OF TRANSPORT & MAIN ROADS *(UNIQUE IDENTITY PROVIDER)* government-owned database(s)

AUTHENTICATORS
PIN, OTP, and on-device biometrics confirmation

ONLINE PUBLIC & PRIVATE E-SERVICES
Bank account opening, vehicle and watercraft registration, eGov services access, home rental, etc.

FACE TO FACE PUBLIC & PRIVATE SERVICE PROVIDERS
Banks, restaurants, pharmacies, etc. with online (QR code) and offline modes

LEGAL FRAMEWORK

> A Privacy Impact Assessment (PIA) was independently validated
> The IP Act requires Queensland Government agencies to comply with the IPPs. The IPPs deal with the collection, storage, use and disclosure of personal information.

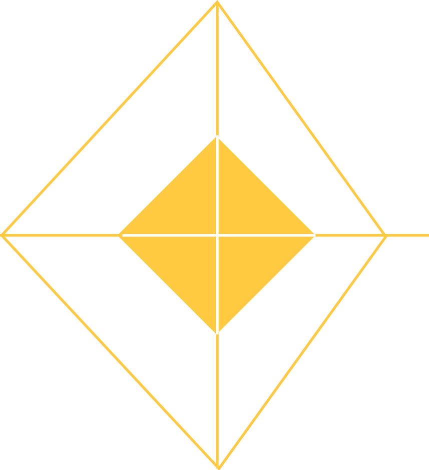
OTHER DIGITAL ID INITIATIVES IN THE COUNTRY

> Mobile driver licence initiatives in South Australia and in New South Wales
> Australia Post Office launched a mobile ID to provide its customers with online authentication services

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

A governance board with 3 reference groups (Customer Experience, Architectural, Policy & Legislative) governed by an inter-department task force to validate any new bespoke integration to the app.

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

> A unique digital ID wallet that host various ID documents (driver licences, photo identification cards and recreational marine licences, etc.) and enable online and offline identity proofing as well as attribute sharing.

> A true codesign and user-centric process involving a panel of 120 end-users who weighted on the selection of the final vendor.

TECHNOLOGY IMPLEMENTATION

A data privacy based on consent model, where citizens are in control, know exactly what data they are releasing and can customize it.

GO TO MARKET & PROMOTION

> A 4 stakeholder approach for adoption: standard media campaign for cities, a specific approach for industries (pharmacists, tobacconist, etc.) and communities such as carers, and specific campaigns to hire long time unemployed and turn them into active ambassadors.
> A gamification strategy bound to the young generation: the Digital Ambassadors program holds regional competitions where high school students submit promotional videos of the App that celebrates their region and the Digital Licence.

8,8 MILLION INHABITANTS
18% ADOPTION RATE

CITIZEN CARD AND MOBILE ID

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

SMARTCARD (HEALTH INSURANCE CARD) + MOBILE ID (SMARTPHONE & WEB BASED)

LIVE SINCE 2003

✓ IDENTIFICATION
online and offline
Use of unlinkable sector specific identifiers.

✓ ID ATTRIBUTES SHARING
For public authorites if a legal basis exists

✓ AUTHENTICATION
Technology-neutral framework which defines minimum requirements for credential to enable online and offline authentication.

✓ ELECTRONIC SIGNATURE

✓ CROSS-BORDER RECOGNITION
Pilots with other European countries on cross border services for businesses

300 PUBLIC E-SERVICES
including tax portal, social and health security portal, pensions and several private services.

EIDAS NOTIFICATION PLANNED FOR 2021

CONTEXT & OBJECTIVES

Austria was one of the first European country to implement a national ID system based on an electronic ID, strongly embedded in the e-government initiative.

While registration into the Central Register of Residents (CRR) is mandatory for all citizens and residents, there is no requirement to get a physical identity card. Instead, Austria has a virtual Citizen Card (CC), which can be installed on several devices based on a technology neutral approach: smartcards or mobile phones.
The main objective is to reduce costs and efforts for the government, as well as save time and money for citizens and businesses.

VALUE PROPOSITION

Currently, the virtual Citizen Card provides access to the Austrian e-government as well as to several private services (banks, chamber of commerce or mobile operators).

The e-ID is accessible for all Austrians, residents and some foreigners such as cross border commuters and expatriates.

OTHER SPECIFIC SERVICES & USE CASES:
> Electronic representation: the holder can carry out legal transactions on another person's behalf.
> Business use cases are being considered: the digital ID scheme is linked to the business-related databases (ie. Business Service Portal) for use cases like digital signatures, tax payment or representation.

A GOVERNMENT FUNDED BUSINESS MODEL

> Mobile ID is free for citizens and for public & private service providers (integration of e-ID in the service) to encourage take-up and use.
> Some services such as the tax portal are mandatory for business, but never for citizens.

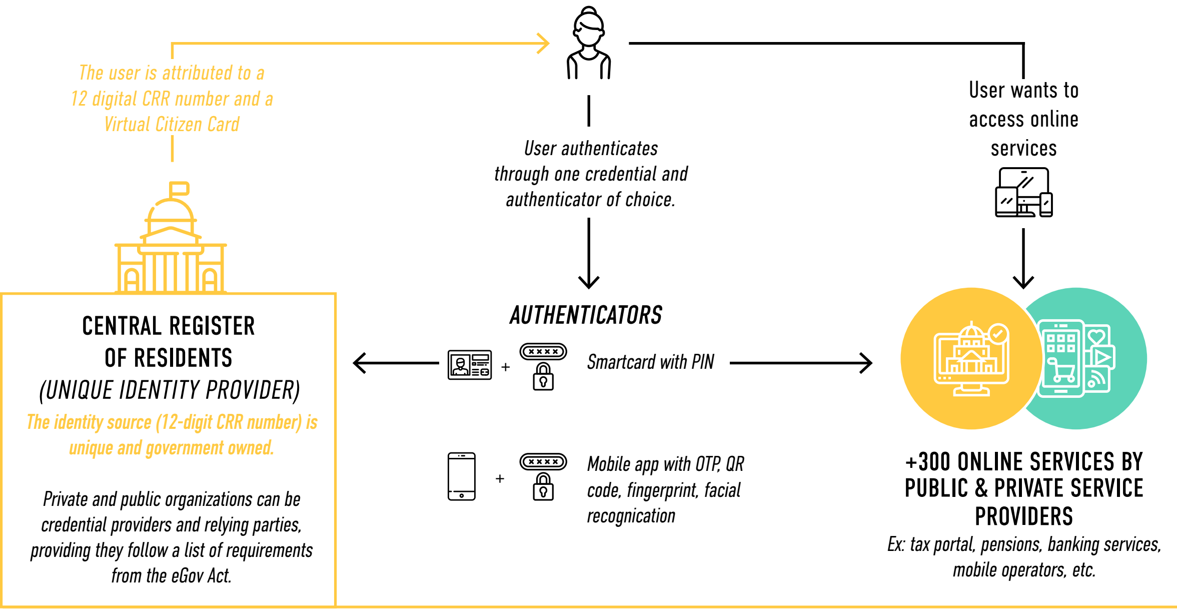
SECURITY & PRIVACY CHOICES

> Strong security requirements through e-IDAS certification requirements for qualified electronic signatures
> Sector specific identifiers derived from CRR number as a general rule: for the same individual, each government sector or private service provider uses a different identifier cryptographically derived from the CRR number. It prevents the matching of individuals across their use of services.
> The Austrian GovCERT, operated by the department for Federal ICT Strategy of the Federal Chancellery, manages security breaches of the infrastructure.

PROJECT MILESTONES

2003	2005	2008	2009	June 2021	2021
Launch of the eID program	Smartcards & Mobile ID launch	Foreign eID recognized	Mobile ID signature	1,5 Million Mobile e-IDs active users	Shift towards mobile first strategy New standard interface for service provider integration. eIDAS notification objective.

AUSTRIAN DIGITAL ID ECOSYSTEM



The user is attributed to a 12 digital CRR number and a Virtual Citizen Card

CENTRAL REGISTER OF RESIDENTS
(UNIQUE IDENTITY PROVIDER)
The identity source (12-digit CRR number) is unique and government owned.

Private and public organizations can be credential providers and relying parties, providing they follow a list of requirements from the eGov Act.

User authenticates through one credential and authenticator of choice.

AUTHENTICATORS
Smartcard with PIN
Mobile app with OTP, QR code, fingerprint, facial recognication

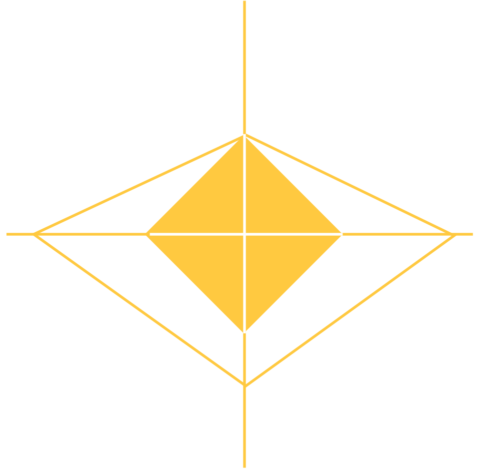
User wants to access online services

+300 ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
Ex: tax portal, pensions, banking services, mobile operators, etc.

LEGAL FRAMEWORK
> Austrian Data Protection Act (Datenschutzgesetz, DSG) (2000)
> eGovernment Act (2004) established a general framework, defined the e-ID and sets high level requirements: Unique ID, electronic qualified signatures & "on behalf" representation.
> Independent Source PIN Register Authority operates the processing of person identifiers (PINs)
> Unilateral acceptance of countries' e-ID since 2008 and e-IDAS notification planned for 2021

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

A new zero footprint approach where citizens just need a browser and a smartphone

TECHNOLOGY IMPLEMENTATION

> An interoperable by design system to integrate other countries if the requirements are met. Pilots are taking place with other European countries on semantics of cross border electronic representation and electronic mandate (SEMPER project with the Netherlands, Slovenia and Spain)
> Sector specific identifiers for privacy and data sharing if legitimate

GO TO MARKET & PROMOTION

> Main milestones in adoption when portals introduced user-friendly registration processes.
> A social security letter campaign announced digital by default for pension record access in 2008/2009
> The use of e-ID for signing popular petitions in 2018 (smoking ban, women rights)

FOCUS ON AZERBAIJAN

ASAN IMZA

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

MOBILE ID (SIM-BASED PKI) ON FEATURE & SMARTPHONES

LIVE SINCE 2014

✓ IDENTIFICATION *online & offline*

○ ID ATTRIBUTES SHARING

✓ AUTHENTICATION

✓ ELECTRONIC SIGNATURE

Legally binding digital signature. Possibility to e-sign without internet connection and on a feature phone.

✓ CROSS-BORDER RECOGNITION

Ratified in 2020 the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific adopted UN ESCAP.

1000+ public and financial e-services

CONTEXT & OBJECTIVES

The development of its ICT sector has been a strong focus for Azerbaijan since 2003. Digital maturity in the country is very high for businesses (around 100%) but far lower for citizens, although the COVID crisis has increased citizen penetration, especially due to the use of online financial services.

The initial objectives of the government for digital ID were to provide an easier access to services, add transparency in the processes by solving root-based bureaucracy and corruption issues and increase global population digital education by making services only accessible online. Today, most of the digitized services concern businesses.

VALUE PROPOSITION

The mobile ID Asan İmza is a SIM-card connected to 3 different certificates (citizen, businesses, civil servants) equal to a physical ID-card in the electronic environment and equal to handwritten ones. Every single SIM card is connected with a citizen unique personal code from the population registry. The mobile ID can be used as a form of secure electronic ID to prove identity and digitally sign documents. All e-services are mandatory when possible. For more user convenience, the user has only two PIN codes, no matter which certificate is used, for authentication PIN1 and signing PIN2.

After getting a SIM card from MNOs, citizens can activate their certificates face-to-face in Tax-payers service agencies, ASAN service centers and banks or remotely (since 2020 because of the COVID outbreak) through Asan Imza' service portal, using biometric data (face-recognition).

OTHER SPECIFIC SERVICES & USE CASES:

> 9 services based on a verbal solution, currently powered by a human, but Artificial Intelligence is explored for the future. Services are popular in rural area for tax declaration.

> E-Residency and M-Residency programs provided by the Digital Trade Hub for foreign and local entrepreneurs around the world to set up and run a location-independent business in Azerbaijan thanks to their government issued Digital Identity.

A BUSINESS MODEL BASED ON A PPP

The technology and service is provided by a private solution provider, while the Tax Authority under the Ministry of Economy ensures the trusted services provision (key storage, certificate delivery and activation, etc.). The SIM card issuing process and cost is decided by MNOs, according to their regulation and business model.

> Certficates are free for citizens, businesses pay a service fee (approx. 9€ for a 3-year certificate.

> Citizens and businesses pay a monthly fee (1€) per SIM card, regardless the number of certificates. The benefits are divided between MNOs and the provider of the solution.

> Because of service efficiency issues, the fee evolved from an SMS transaction-based fee to unlimited SMS transactions for all.

SECURITY & PRIVACY CHOICES

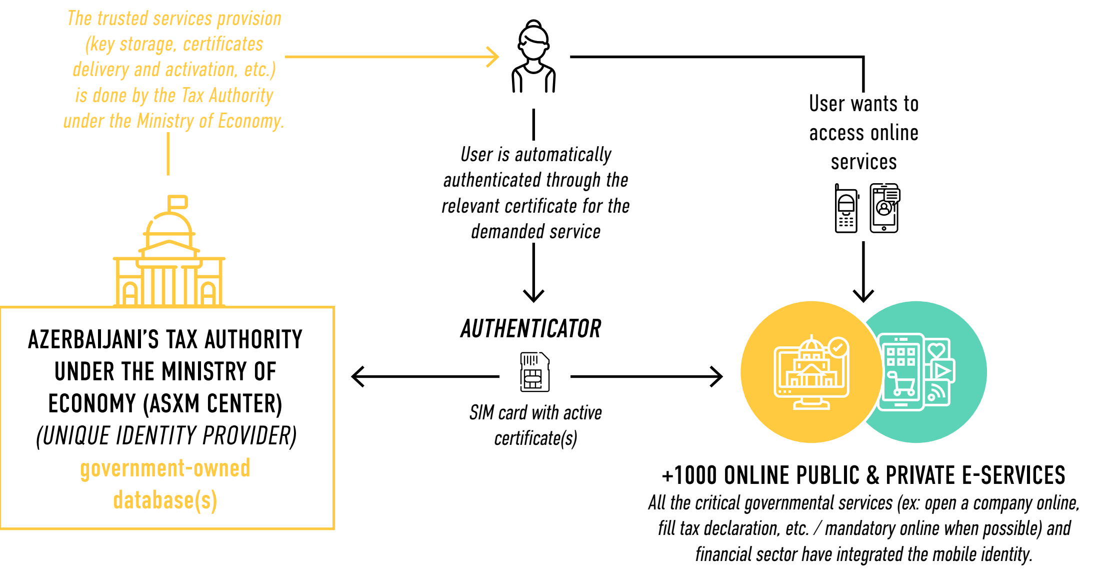
> The mobile ID follows international regulations such as GDPR and is eIDAS compliant thanks to its PKI based solution (the private key is stored on the hardware which belongs to the customer).

> Follows US NIST standards and e-IDAS High (EU): currently, all levels of assurance are supported by the Azerbaijani digital identity scheme.

PROJECT MILESTONES

2014	2016	2017	2018	2019	2020	2021/2022
Launch of Asan Imza	More than 650 e-services and 25 banks connected	Launch of the Digital Trade Hub of Azerbaijan for validation of cross-border e-Signatures and e-Services	The worlds first m-Residency program was launched. Available in 79 embassies around the world.	NIST award for Asan Imza SIM card technology. OECD recognized Asan Imza as an outstanding innovation example.	More than 90 million transactions made and more than 1000 e-services available	New generation of Mobile ID: working offline with Mobile Drivers licence support and passport, blockchain authentication, e-SIM with quantum proof cryptography. Achieving mutual two-way recognition with the EU for e-signatures.

ASAN IMZA DIGITAL ID ECOSYSTEM


The trusted services provision (key storage, certificates delivery and activation, etc.) is done by the Tax Authority under the Ministry of Economy.
User is automatically authenticated through the relevant certificate for the demanded service
User wants to access online services
AZERBAIJANI'S TAX AUTHORITY UNDER THE MINISTRY OF ECONOMY (ASXM CENTER) (UNIQUE IDENTITY PROVIDER) government-owned database(s)
AUTHENTICATOR
SIM card with active certificate(s)
+1000 ONLINE PUBLIC & PRIVATE E-SERVICES
All the critical governmental services (ex: open a company online, fill tax declaration, etc. / mandatory online when possible) and financial sector have integrated the mobile identity.

LEGAL FRAMEWORK

> Fundamental laws regulate the digital environment in Azerbaijan on electronic signature, electronic document and data protection.

OTHER DIGITAL ID INITIATIVES IN THE COUNTRY

> Physical ID Card with signature

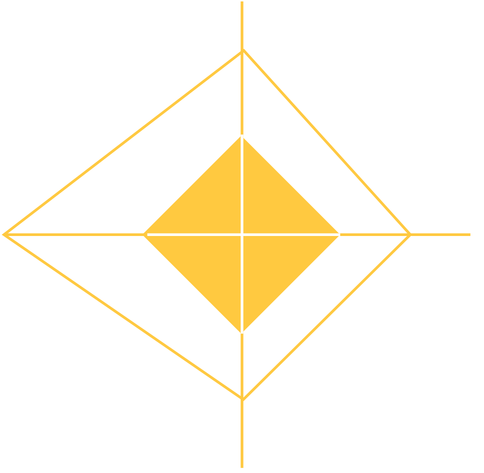
> E-signature with tokens

> New type of ID cards with picture including storage of electronic signature

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

A public private partnership model between the government, a private solution provider and the MNOs, built the Azerbaijanese ecosystem in 6 months (compared to traditional government managed procedure - in average 2 years). The PPP scheme provided self-explanatory, quick and concrete results convincing key decision makers and stakeholders - especially government).

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

> The SIM card-based solution is convenient for all types of networks (2G) and for any type of mobile phone, making it a relevant choice for developing markets.

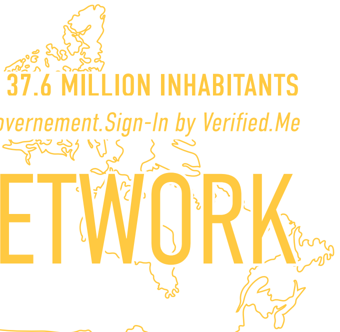
> Free accessibility to digital services for citizens during the COVID-19 outbreak, to reach a critical mass of users and accelerate the citizens digital education.

TECHNOLOGY IMPLEMENTATION

The solution provider benchmarked international standards and regulation to provide the highest LoA. This approach was necessary to establish the trust required to succeed internally and to expand into cross-border transactions and eTrade with other countries worldwide.

GO TO MARKET & PROMOTION

A close collaboration and partnership between government and private sector including banks and MNO's to increase uptake and promote Asan Imza to private citizens and businesses. Activities include advertisement campaigns or on the spot consultations.



37.6 MILLION INHABITANTS

+18M USERS *for Governement.Sign-In by Verified.Me*

VERIFIED.ME IDENTITY NETWORK

GOVERNMENT-DRIVEN for Governement Sign-In by Verified.Me
CROSS-INDUSTRY DRIVEN for Verified.Me

LIVE SINCE **2012** *for Government Sign-In by Verified.Me*
2019 *for Verified.Me*

269 FEDERAL GOVERNMENT SERVICES *available on Governement.Sign In by Verified.Me*

FEDERATED SCHEME

SIGN-IN WITH BANK CREDENTIALS + **VALIDATION ON AN APP AND WEB BROWSER**

✓ **IDENTIFICATION**
online only

✓ **AUTHENTICATION**

✓ **CROSS-BORDER RECOGNITION**

Verified.Me is designed to be exportable to other countries and compatible with other ecosystems: it is developed around the EMC Check for identity model, as well as using W3C open standards and meant to be technology agnostic, in accordance to the DIACC framework.

✓ **ID ATTRIBUTES SHARING**

Consent-based and explicit attribute sharing at each connection to a service provider thanks to the Verified.Me network on mobile or web browser.

✓ **ELECTRONIC SIGNATURE**

Enhanced verification of the document signer

CONTEXT & OBJECTIVES

In 2012, the Canadian federal government issued an RFP to develop an authentication service for canadian citizens to access public services online. SecureKey Technologies Inc. developed Government Sign-in by Verified.Me (formely Concierge) a federated SSO service that acts as a trusted network operator, linking services providers to a credential provider, and uses existing financial credentials (card numbers, usernames and passwords) to authenticate users online.

In 2019, SecureKey Technologies Inc. released Verified.Me for the private sector in collaboration with a consortium of seven of Canada's major financial institutions.

VALUE PROPOSITION

Verified.Me simplifies identity verification processes by enabling users to share their identity and attribute information from trusted sources (financial institutions, mobile operators, credit bureau, or government) with the services that they wish to access.

To enroll, users are required to connect an active and existing account from at least one of the participating financial institutions on the Verified.Me platform (web and mobile). Between 85-90% of adults in Canada have such an account.

Today, dozens of Canadian government services, but also services in the financial, healthcare, or telecommunication sectors, are integrated to the ecosystem.

PRIVATE SECTOR FUNDED BUSINESS MODEL

> Initially funded by the members of the consortium.
> Free for the end-users
> Pay-per-use model for the service providers.

> Important costs saving for service providers regarding their on-boarding process[1] with a 50% reduction
> From 2012 to 2018, Government Sign-in by Verified.Me took the governmental authentication costs down to $200 million (comparing to the $970 million spent from 2004 to 2012)[2].

SECURITY & PRIVACY CHOICES

Data protection is at the core of the design of Verified.Me. The service embraces the "privacy by design" approach and is intended to exceed data protection requirements.

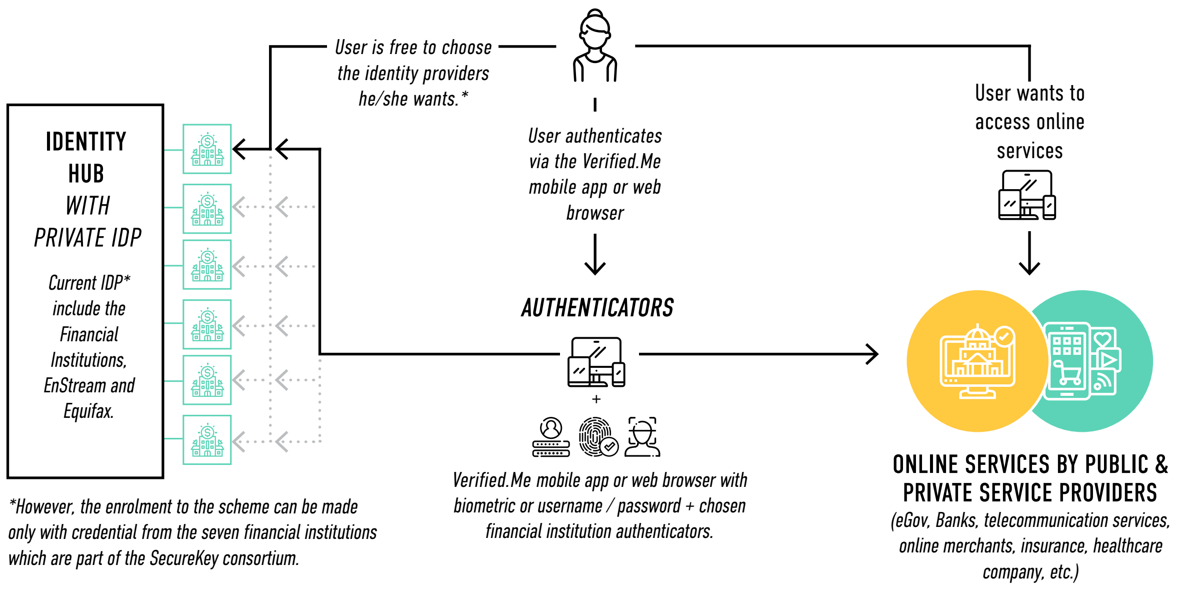
> In the system, no explicit attribute data is collected or shared by Verified.Me between the identity or service providers: the credentials (containing attributes) are encrypted end-to-end with dynamically generated cryptographic keys, which are communicated independently of the credential transmission. Blockchain is also a key factor in providing trust, privacy and security.
> The architecture ensures that subjects have full control over which credentials are shared while maintaining the principle of Triple Blind®, meaning that non of the network participant, including the operator, can have a complete view of the users' transactions.

PROJECT MILESTONES

2012	2014	2019	2020
Launch of Concierge	+1M transactions per month	Launch of Verified.Me	Massive rise from 100 to 800 transactions per second during pandemic: 18 million users on Government Sign-In by Verified.Me

[1] How to Make Digital Identity a Success: Insights and Learnings from Seven Digital ID Schemes, Mobey Forum's Digital ID Expert Group, 2020
[2] Andre Boysen, SecureKey Technologies Inc. Chief Identity Officer, 2020

VERIFIED.ME DIGITAL ID ECOSYSTEM


User is free to choose the identity providers he/she wants.*
User authenticates via the Verified.Me mobile app or web browser
User wants to access online services
IDENTITY HUB WITH PRIVATE IDP
Current IDP* include the Financial Institutions, EnStream and Equifax.
AUTHENTICATORS
+
Verified.Me mobile app or web browser with biometric or username / password + chosen financial institution authenticators.
ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
(eGov, Banks, telecommunication services, online merchants, insurance, healthcare company, etc.)

*However, the enrolment to the scheme can be made only with credential from the seven financial institutions which are part of the SecureKey consortium.

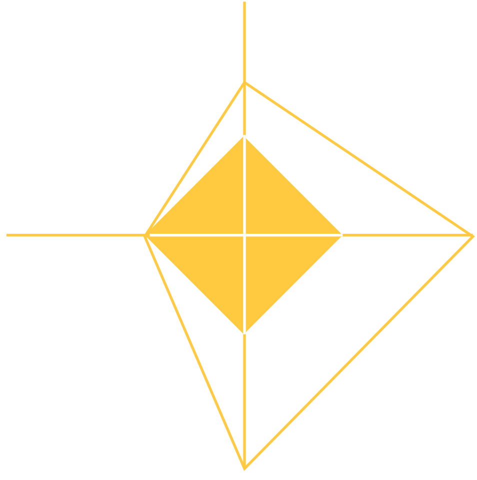
LEGAL FRAMEWORK

> Independent data protection authority: The Office of the Privacy Commissioner Canada.
> Several province and sector-specific privacy laws, as well as several federal regulations: The Privacy Act (1983), or the Personal Information Protection and Electronic Documents Act (2000) for the private sector, amended by the Digital Privacy Act (2015).
> The Digital ID & Authentication Council of Canada (DIACC) developed the Pan Canadian Trust Framework with both public and private stakeholders. The framework's goal is to map & identify where technologies & legal policies intersect. It Is meant to be model agnostic and will be applicable for any model (federation, brokered hub, etc.).

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

A public and private consortium approach with a distributed consent-based ecosystem with a structured and documented liability.

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

TECHNOLOGY IMPLEMENTATION

Use of blockain for Verified.Me to implement the Triple Blind protocol. The Verified.Me trusted network and encrypted hash guarantees that the data comes from a trusted source, that it has not been altered and that the data is being presented by the person it belongs to.

GO TO MARKET & PROMOTION

An adoption strategy inspired by the credit cards model, by separating the issuing side from the acquiring side. On the first side, focus on making partnerships with banks that issue credit cards, and on the other side, sign up partners to accept credit cards and create universal acceptance. Verified.Me is built on the same example. On the issuing side, Verified.Me relies on posts, banks, credit scoring agencies, government, telcos to participate. On the acquiring side (merchant side), a concerted effort to enable partners to sign up new services. This strategy helped to scale faster by building business relationships where partners can go out and sign up relying parties for Verified.Me.

49,65 MILLION INHABITANTS

NEW EID CARD AND MOBILE ID

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

SMARTCARD (DEPLOYMENT IN 2021) + MOBILE ID (DEPLOYMENT IN 2021)

LIVE SINCE 2020

✓ IDENTIFICATION
online and offline

Offline identification with the new eID card enables access to various data such as medical history or civil registry.

○ ID ATTRIBUTES SHARING

✓ AUTHENTICATION

○ ELECTRONIC SIGNATURE

○ CROSS-BORDER RECOGNITION

Discussion are ongoing about standardization and interoperability in latin America: thanks to ICAO standard, the new eID could be accepted as a travel document by other countries.

191 public entities services will be connected
thanks to citizen portal GOV.CO by 2022.

CONTEXT & OBJECTIVES

Since 2015, the National Civil Registry of Colombia (RNEC) - constitutionally in charge of the Colombian citizens identification - enables public and private organizations to use its biometric citizen database to provide identification and authentication services through interoperability mechanisms, mitigating identity fraud.
By working closely with the government, the digital identity provided by the RNEC will be the key access to different services (health, public services, social services and financial services). This unique digital identification model will be based on biographic and biometric data, as well as a unique identification number,

Apart from RNEC, other initiatives are currently happening in Colombia around three axes: the Electronic Citizen Folder and the interoperability platform, and the Electronic Authentication, lead by the government.

VALUE PROPOSITION

The new national identity will take two forms: a traditional physical eID card (launched in December 2020) and a mobile digital ID, which is a dematerialization of the eID card. The mobile digital ID will be legally recognized as an equivalent of the physical document and as the natural identification for in person and remote transactions.

The new services brought by digital identity tools will allow citizens to access public services easily, avoiding cumbersome forms and multiple passwords. It will also bring important benefits in terms of security, interoperability, efficiency, transparency and privacy.

The authentication process for the mobile app uses biometrics including facial recognition with a liveness detection. The level of assurance (e.g. strong authentication), will be adapted to the service.

Digital identity paves the way to analyze new opportunities such as the electronic vote to fight against electoral abstention, to optimize the process and ensure transparency. This objective is openly designated as the long-term goal by Colombian politics. The National Registry of Civil Status and the National Electoral Council (CNE) are already setting up a framework for the new voting system, with four voting modalities: manual, mixed electronic, remote electronic and anticipated.

A GOVERNMENT FUNDED BUSINESS MODEL

> The government financed the implementation of the infrastructure to provide the digital identity, as well as a percentage of the cost of the digital document.
> For Colombians who do not have any previous ID, the new smartcard and the associated mobile ID is free. For those who already had one and want the new one, they have to pay $US 12-13 (same as the current National ID).
> Free for public services to use the digital ID to identify and authenticate citizens identities.
> Fixed cost per transaction for private service providers. This fee will be reinvested in the infrastructure and security tools to improve the digital identity system.

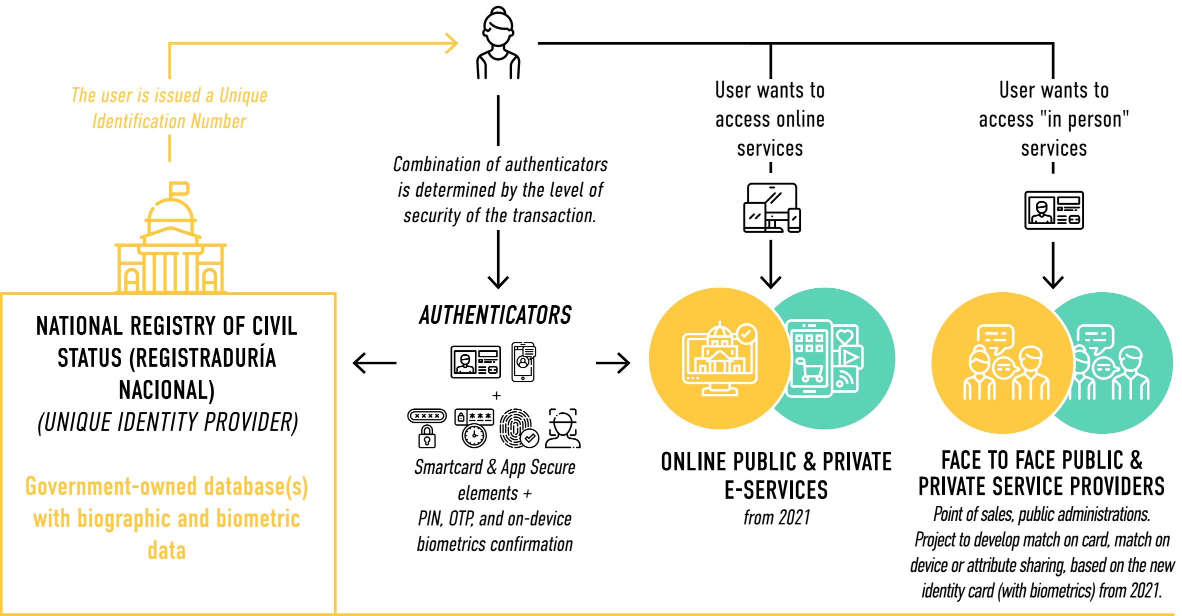
SECURITY & PRIVACY CHOICES

> Unique randomly issued identification number for all citizens of Colombia.
> Biometrics allows identification and authentication with a high level of trust.
> All the scheme is based on PKI-CSC. Blockchain should be used for the electronic voting.

PROJECT MILESTONES

1948	2012	2017	2020
Creation of the National Registry of Civil Status	The RNEC allows public institutions to verify information against its database.	A law defines the 3 axes of the digital identity: the Electronic Citizen Folder, the Electronic Authentication and the Interoperability platform.	99,98% of Colombian citizens are registered within the database. 50 000 eID cards are issued. In Dec. 2020, legislation by the Congress of the use of the Digital ID as a mean of authentication for the election electronic system.

COLOMBIAN DIGITAL ID ECOSYSTEM ⟶ OPERATIONAL IN 2021



The user is issued a Unique Identification Number

NATIONAL REGISTRY OF CIVIL STATUS (REGISTRADURÍA NACIONAL)
(UNIQUE IDENTITY PROVIDER)

Government-owned database(s) with biographic and biometric data

Combination of authenticators is determined by the level of security of the transaction.

AUTHENTICATORS

Smartcard & App Secure elements +
PIN, OTP, and on-device biometrics confirmation

User wants to access online services

ONLINE PUBLIC & PRIVATE E-SERVICES
from 2021

User wants to access "in person" services

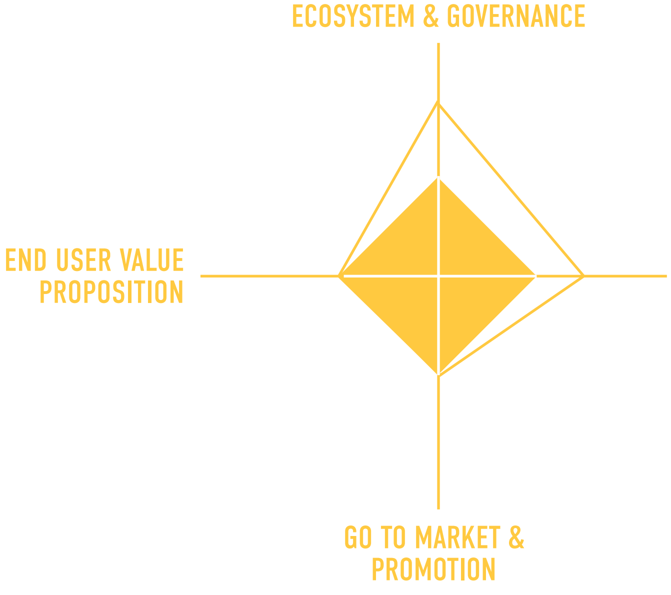
FACE TO FACE PUBLIC & PRIVATE SERVICE PROVIDERS
Point of sales, public administrations.
Project to develop match on card, match on device or attribute sharing, based on the new identity card (with biometrics) from 2021.

LEGAL FRAMEWORK

There have been many decrees related to digital government, transparency, privacy or identity over the last two decades. Some of the most important and recent ones are:
2017: Decree 1413 includes the digital identity guidelines of the three projects: authentication, citizen folder and interoperability.
2018: Digital Government Act encourages the use of digital tools to boost economy and innovations thanks to digital trust.
2020: Decree 620, mainly based on eIDAS regulation, defines the transversal aspects of Digital Government Policy: definition, cost, security, privacy, accessibility and others.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

> Independant and collaborative governance: The National Registry of Civil Status (RNEC) in charge of Identity management and elections closely collaborates with the Ministry of ICT to get access to the Digital Citizen Folder.

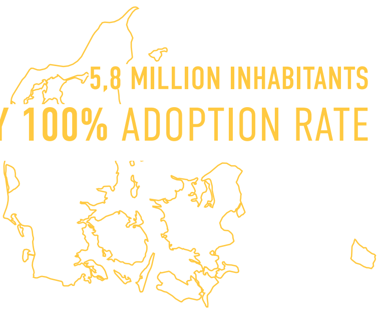


TECHNOLOGY IMPLEMENTATION

> Assumed choice of using facial recognition for the future: the RNEC agency is trying to open their facial biometric database and implement facial recognition as a complement to the fingerprint database that is already used in several sectors in Colombia (Financial, telecommunication or notary sector).

FOCUS ON DENMARK

NEMID & MITID


5,8 MILLION INHABITANTS

NEARLY 100% ADOPTION RATE

GOVERNMENT AND BANKS-DRIVEN CENTRALIZED SYSTEM

FOR NEMID: USERNAME AND PASSWORD with a keycard or an app used as second factor (PKI technology)
FOR MITID: EID STANDARD WITH DIGITAL SIGNATURE SOLUTION BASED ON PKI (with NEM login) on a wide range of credentials.

✓ IDENTIFICATION *online*

LIVE SINCE 2010

✓ ID ATTRIBUTES SHARING

NemLogin solution provides administration of users rights for public services.

+800 public & private connected services

✓ AUTHENTICATION

***Multiple authentication solutions:** a mobile application, a key token, the MitID chip (FIDO token, a chip token used for high insurance levels) specific accessible tokens for elderly, visually impaired persons, etc.*

✓ ELECTRONIC SIGNATURE

✓ CROSS-BORDER RECOGNITION

EIDAS NOTIFICATION (SUBSTANTIAL) FOR NEMID

CONTEXT & OBJECTIVES

Denmark has a long tradition of e-ID and is currently transitioning to its third generation (MitID), co-owned with the financial sector.

In 2003, the main priority was to enable access to e-government services by providing a secure online identification for citizens. In 2010, in cooperation with the financial sector, citizens could use their public e-ID for online banking. Now very largely disseminated throughout the Danish population, NemID provides a free and a national eID for all citizens.

For the new MitID solution, the government engaged a Public Private Partnership with the financial sector, who will be the co-owner of the solution.

VALUE PROPOSITION

NemID is a common secure login on the internet usable for online banking, finding out information from the public authorities or engaging with one of the many businesses that use NemID.

From a user point of view, there will be no difference between NemID and MitID, except offering a better user experience especially in the Nemlogin solution for employee identities administration.

The main difference lies at the infrastructural level: it will offer more reliability, security and flexibility. With MItID, only certified MitID brokers will be allowed to engage directly with the MitID core system. The role of the brokers will be to join the MitID infrastructure, do the technical interfaces and then sell their services to service providers who want to use MitID for their services.

BUSINESS MODEL

NEMID

> The public sector has a contract with the e-ID supplier and provides free NemID for all citizens and 3 free employee certificates for all companies.

> Private companies pay for validating the NemIDs received.

MITID

> The new model is financed and co-owned by the government and the financial sector. It is still free for citizens, with 3 employee certificates for all companies.

> There will be a fee per transaction for service providers who will want to use MitID. The transaction fee, calculated on the basis of the running costs, is expected to be less expensive for most service providers.

SECURITY & PRIVACY CHOICES

MitID is based on a broker infrastructure. It will reduce the level of risk to which the system is exposed. Service providers will access the infrastructure through a broker and each sector (public, financial, private) will have its own brokers:

> The public sector will have only one broker: NemLogin

> The financial sector will have several of brokers

> Private brokers will be able to join the infrastructure so that they can make it accessible for private services providers.

PROJECT MILESTONES

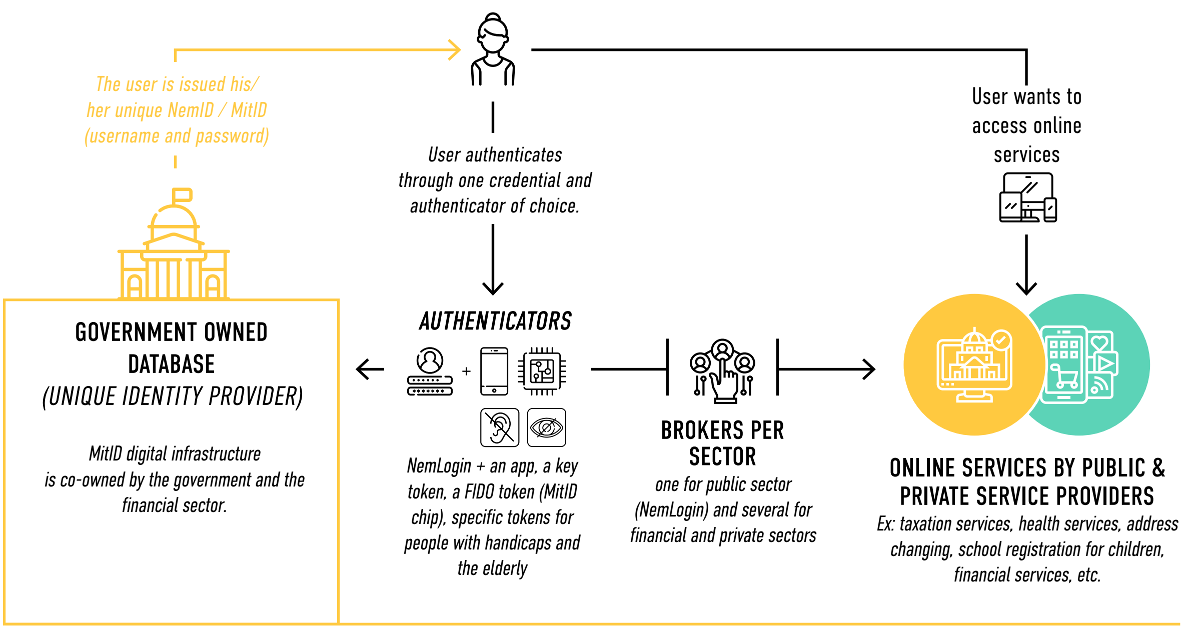
2003
First national public online services infrastructure

2010
Launch of national NemID solution

2020
5.6 million NemIDs issued to Danish citizens and residents from 15 years old or up.
1.5M companies are using NemID infrastructure.

Q2 2021
MitID launch

MITID DIGITAL ID ECOSYSTEM


The user is issued his/her unique NemID / MitID (username and password)

User authenticates through one credential and authenticator of choice.

User wants to access online services

GOVERNMENT OWNED DATABASE
(UNIQUE IDENTITY PROVIDER)

MitID digital infrastructure is co-owned by the government and the financial sector.

AUTHENTICATORS

NemLogin + an app, a key token, a FIDO token (MitID chip), specific tokens for people with handicaps and the elderly

BROKERS PER SECTOR
one for public sector (NemLogin) and several for financial and private sectors

ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
Ex: taxation services, health services, address changing, school registration for children, financial services, etc.

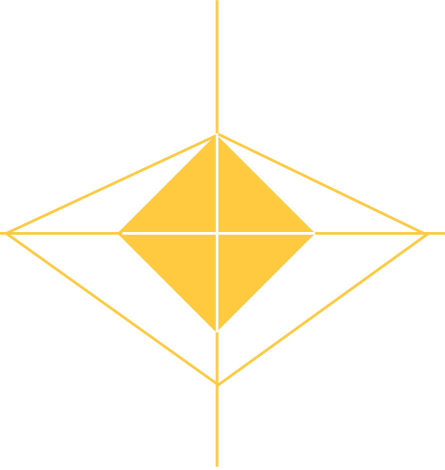
LEGAL FRAMEWORK

> National standards

> A law on the infrastructure of MitID and NEM login, which regulate the access to the infrastructure and user compliance is in process.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

A wide variety of credentials to adapt to all types of population (with specific ones for people with handicaps and the elderly).

TECHNOLOGY IMPLEMENTATION

> A broker-based infrastructure to increase the security level by limiting the access of the infrastructure to brokers only.

> A modular infrastructure to follow the technology evolution and plug / unplug credentials to fit with user's needs.

> An inclusive and easy access for small service providers without advanced IT competencies to use MitID - integration is taken in charge by brokers.

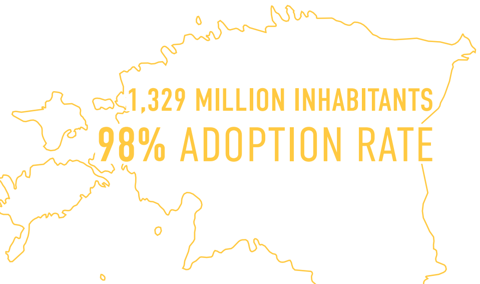
GO TO MARKET & PROMOTION

> A partnership with the financial sector since the launch of NemID to increase the frequency of use and the adoption of the ID solution.

> A strong implication and test process with all stakeholders, including companies & different industries, associations representing the elderly, people with handicaps, etc.

> A strong teachers network to rely on to help the elderly use digital ID & access public online services

E-IDENTITY



GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

600+ government e-services for citizens

2400+ government eservices for businesses

99% banking services apply digital ID.

4 AVAILABLE CREDENTIALS

- **ID-CARD: A STANDARD NATIONAL ID SMARTCARD**
- **DIGI-ID: A COMPLEMENTARY SMARTCARD** (which provides the same functionalities as the ID-card but with no picture - no physical identification)
- **MOBIIL-ID: A PKI-BASED SIM SOLUTION**
- **SMART-ID APP: A PKI-BASED SOLUTION** using iOS and Android secure elements and shared keys method

LIVE SINCE 2002

EIDAS NOTIFIED FOR SEVERAL LEVELS OF ASSURANCE (INCLUDING HIGH) DEPENDING ON THE CHOSEN SOLUTION.

✓ **IDENTIFICATION**
online & offline

✓ **ID ATTRIBUTES SHARING**

✓ **AUTHENTICATION**
The credential will always have two digital certificates: one for user authentication and one for digitally signing documents. Access to these certificates is secured by a PIN.

✓ **ELECTRONIC SIGNATURE**
All three solutions are eIDAS notified for qualified electronic signature.

✓ **CROSS-BORDER RECOGNITION**
X-Road is the first data exchange platform - data exchange layers like X-Road habe been implemented in Finland, Azerbaijan, Namibia and the Faroe Island.
For cross-border interoperability within the EU, two central eIDAS-Node services:
> the service node, for authentication with notified Estonian eID in another EU Member State e-service.
> the connector node, for authentication in Estonian public sector e-services with EU notified eID schemes.

CONTEXT & OBJECTIVES

Estonia is one of the most digitally integrated societies in the world. People can access digital services thanks to three interoperable digital identity solutions:
> An ID card (ID-Kaart) based on smartcards (National Identity card and Resident ID card). The main government agency involved is the Ministry of Interior, which oversees the population registry. It is mandatory for every Estonian citizen above 15 to obtain the identity card.
> Mobiil-ID, provided by the Estonian mobile operators and the government. This system allows online transactions without the need for a computer or a card reader.
> Smart-ID, provided by the private sector, is also a mobile based eID on an app linked to the smartphones secure elements.

Historically, the ID-Kaart was the most popular but the trend has recently stopped, giving the advantage to Smart ID (500 000 users).

VALUE PROPOSITION

99% of public services are available online in Estonia (including I-voting with 44% of users in the last elections). Only a few acts that require a physical presence cannot be performed via the Internet, such as getting married or buying a house.
New services are available like parking, e-banking and public transportation, social security services (including medical e-prescriptions), loyalty program integrating by merchants.

BUSINESS MODEL

> The eID Card is mandatory and financed by government and provided by the private sector, folllwing a Public Private Partnership. Citizens pay an initial 25€ to obtain a new ID card valid for 5 years.
> Mobile ID is optional and co-financed by government and the private sector. Citizens pay ~1€ / month to Mobile Network Operators for the new sim card, SMS, etc.
> Smart ID is optional, financed and provided by the private sector and completely free of charge for citizens. However, e-services providers have to pay twice as much for digital signature & authentication services compared to the Mobile ID.

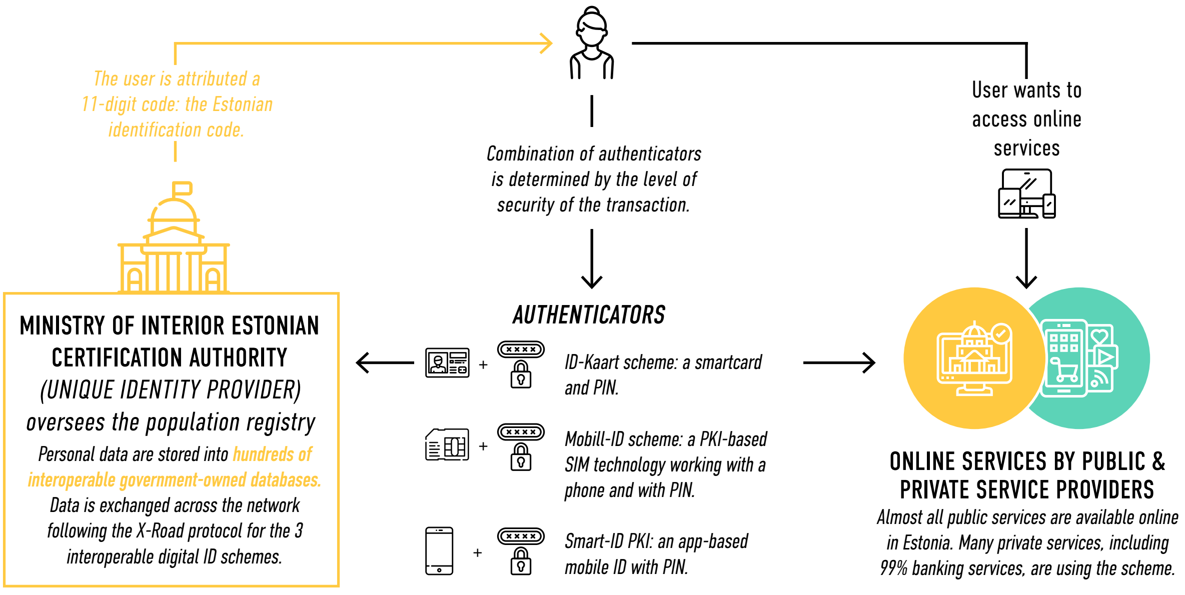
SECURITY & PRIVACY CHOICES

> The data is exchanged across a system of joined-up databases following a protocol called X-Road.
> The Estonian Data Protection Inspectorate, a supervisory authority founded in 1999, protect the rights of the Estonian citizens (use of personal data, right to get information, right to access data...).
> Minimal data is shared, and Estonia follows the "once only principle", which stipulates that citizens share the same data only once with identity and service providers.
> Estonia's citizen portal provides users with tools to oversee and control who has access to their data.
> In 2017, Estonia had to reprogram thousands of smartcards because they had a security issue related to the PKI private keys stored on the chip. Known as "ROCA vulnerability", the card were exposed to identity theft.

PROJECT MILESTONES

2002	2005	2006	2007	2011	2017	2020
First eID card issued and digital signature used.	First internet vote for the local elections. 2% of voters voted on internet.	90% of the population has an ID-kaart	Launch of mobile ID services with PKI-enabled SIM cards.	integration of mobile-ID scheme into e-government services.	Release of Smart-ID service based on SplitKey digital ID platform. ROCA crisis (identity theft)	98% of citizens have a national eID card 67% of them actively use it. 250.000 users for the Mobiil-ID 500,000 smart-ID users. 900,000 active ID-kaart users.

ESTONIAN DIGITAL ID ECOSYSTEM

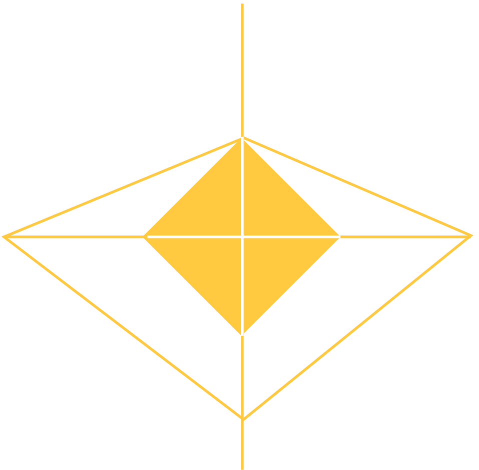

The user is attributed a 11-digit code: the Estonian identification code.
Combination of authenticators is determined by the level of security of the transaction.
User wants to access online services
MINISTRY OF INTERIOR ESTONIAN CERTIFICATION AUTHORITY (UNIQUE IDENTITY PROVIDER) oversees the population registry
Personal data are stored into hundreds of interoperable government-owned databases. Data is exchanged across the network following the X-Road protocol for the 3 interoperable digital ID schemes.
AUTHENTICATORS
+
ID-Kaart scheme: a smartcard and PIN.
+
Mobill-ID scheme: a PKI-based SIM technology working with a phone and with PIN.
+
Smart-ID PKI: an app-based mobile ID with PIN.
ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
Almost all public services are available online in Estonia. Many private services, including 99% banking services, are using the scheme.

LEGAL FRAMEWORK

> The Estonian Data Protection Inspectorate, founded in 1999, is a supervisory authority with the objective is to protect the rights of the Estonian citizens (use of personal data, right to get information, right to access your data...).
> The Estonia Information System Authority (RIA), defines the regulatory frameworks for the different stakeholders.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

> Time saving use cases for citizens: i-voting reduced the need to travel, a real benefit for people living in rural areas. In 2017, it saved 11,000 working days for the election.
> An increased efficiency and accuracy of the country's health system, with reduced bureaucracy and implementation of new services: 99% of medical prescriptions are transacted electronically.
> An e-residency program which places Estonia as a pioneer in the "country-as-a-service" model. It enables non-citizens and non-residents to get an Estonian virtual residency card, with a limited number of actions such as opening a bank account of registering a business in the country.

TECHNOLOGY IMPLEMENTATION

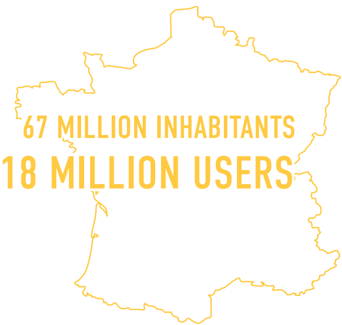
> X-Road open source platform, a pioneering example of domestic and international interoperability, enabling the "only once" principle for e-government service delivery and data collection.
> Smart-ID onboarding process innovative technology such as facial authentication comparing with the photograph in the passport.

GO TO MARKET & PROMOTION

> A training and support approach for adoption: specific training for the population and support phone line are always available for users in case of a problem.
> Incentives to use of digital services: Ticketless public transport, faster tax refunds, higher limits on bank transfers.

FOCUS ON FRANCE

FRANCE CONNECT


67 MILLION INHABITANTS
18 MILLION USERS

GOVERNMENT-DRIVEN | FEDERATED SCHEME | *Credentials and authentication processes depend on the identity provider: username, password + PIN, Mobile app, etc.*

✓ IDENTIFICATION *online only*
✓ ID ATTRIBUTES SHARING
✓ AUTHENTICATION
○ ELECTRONIC SIGNATURE
○ CROSS-BORDER RECOGNITION

LIVE SINCE 2016 | 800 public and private e-services connected to FranceConnect (with 50 private) | AMBITION TO OBTAIN EIDAS NOTIFICATION IN 2021

CONTEXT & OBJECTIVES

Over the past 15 years, there have been several government-led attempts to develop a digital identity ecosystem in France before France.Connect. Unlike other European countries, none of the major French financial institutions or mobile operators have opted to invest in the development of a a digital identity service.

The initial objective of FranceConnect was to guarantee a secure access to a maximum number of online services without having to multiply passwords. Thanks to a strong political support, the service has now the objective to become a fully functional digital ID scheme, compatible with the highest level of insurance defined by eIDAS.

VALUE PROPOSITION

FranceConnect is a digital identity federator that maintains and regulates an ecosystem for identity providers, service providers and users. The particularity of FranceConnect is that the user can select the IdP of his or her choice when accessing a service.

To boost penetration, new daily services will be integrated in the ecosystem by 2021, such as housing subsidies (CAF), unemployment benefits (Pôle Emploi) or education (access to report cards online).

By 2021, a Smartcard (Carte Nationale d'Identité Électronique - CNIE) will be linked to a government-owned Mobile App.

OTHER SPECIFIC SERVICES & USE CASES:

> Receipt of electronic registered letters for the national post (La Poste).

> Three planned innovative extensions of the FranceConnect service:
- One dedicated to businesses: Pro Connect
- One dedicated to people with disabilities/with no access to digital tools and will provide electronic representation: Aidants Connect
- One for civil servants: AgentConnect.

A GOVERNMENT FUNDED BUSINESS MODEL

> FranceConnect services are entirely funded by the government.
> The service is free for users, service providers and public / private identity providers.
> Private identity providers can make private service providers pay for their authentication services but must provide it for free for public services.

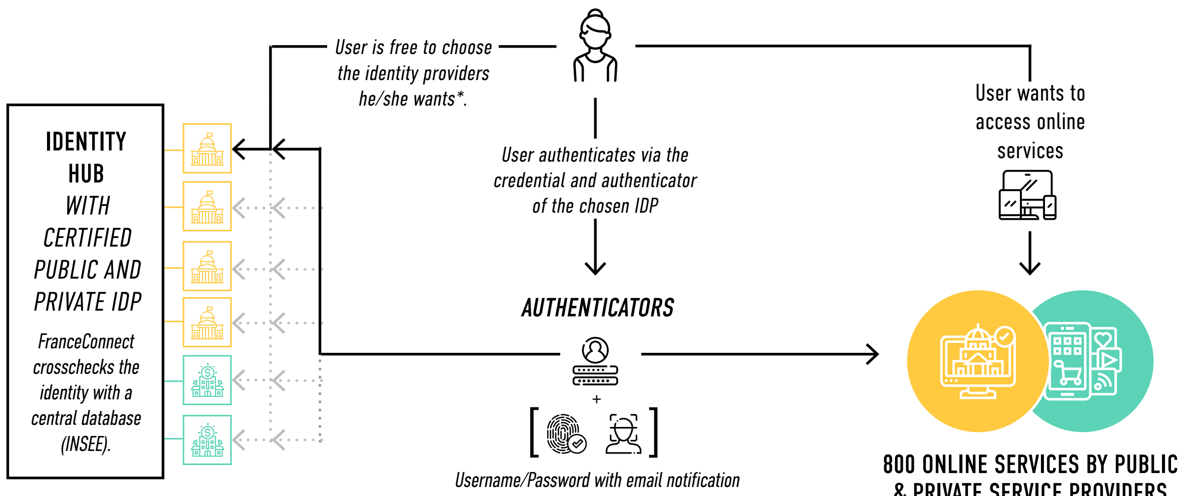
SECURITY & PRIVACY CHOICES

> FranceConnect does not store any information retrieved from the IDP's, a unique hash key guarantees the uniqueness of the identity.
> The majority of FranceConnect IdP's require a username and password for authentication. One IdP, La Poste, provides was approved for the substantial eIDAS level.
> FranceConnect ensures a strong confidentiality provision for users: services providers do not know which IDP the users has chosen and vice versa.
> In accordance with the requirements of the CNIL, there is no centralization of data within the FranceConnect ecosystem and ownership of all identities is shared between identity providers. This choice was made early on and has been confirmed over the years.

PROJECT MILESTONES

2015	2016	Sept. Oct. 2020	June 2021	2021	2022
FranceConnect Proof of Concept (POC)	Launch of FranceConnect	18M users in France and around 30 people in the FranceConnect team.	Target for eIDAS notification	Adding of new frequently used services. Launch of the CNIE smartcard.	Target of 30M users. Opening to new private services.

FRANCECONNECT DIGITAL ID ECOSYSTEM


IDENTITY HUB WITH CERTIFIED PUBLIC AND PRIVATE IDP
FranceConnect crosschecks the identity with a central database (INSEE).
User is free to choose the identity providers he/she wants*.
User authenticates via the credential and authenticator of the chosen IDP
AUTHENTICATORS
User wants to access online services

Majority of public identity providers. Two private identity providers: La Poste (French Post Office) and a startup: AriadNext.

Username/Password with email notification + Strong authentication available for one IdP with Biometrics / push validation

800 ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
most of them are public services (federated services and single sign-on), and around 50 private services (banks, online gaming, insurance, EDF, etc.).

**depending on compatibility of the IdP with the level of assurance required by the service provider for the online transaction*

LEGAL FRAMEWORK

> Strict regulations and control by the CNIL (Commission nationale de l'informatique et des libertés), an independent French organization in charge of protecting the privacy of French citizens.
> Legislative blind spot when adding new online private services such as real-estate agencies: future regulation should adapt to integrate these new services.

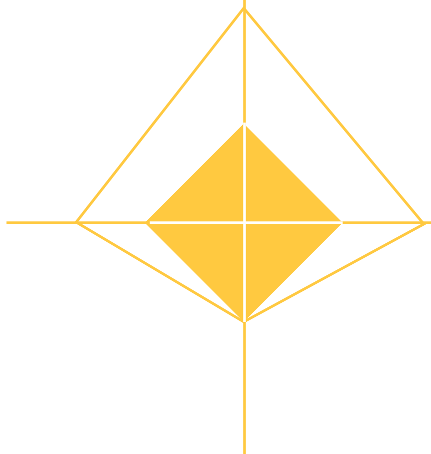
OTHER DIGITAL ID INITIATIVES IN THE COUNTRY

> ALICEM: Government owned Mobile ID was piloted and should be launched in 2021
> In parallel, the French government is developing the next generation of eID card (CNIE), which will be linked to a government-owned Mobile App. The service should be integrated to FranceConnect.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

> An inter-ministerial governance - - one of the key success factor of FranceConnect - with committees representing stakeholders (Ministry of the Interior, Finance, National Education, Health, etc.) and the French National Cyberprotection Agency
> A government-led scheme: Unlike other semi-centralized scheme, FranceConnect does not depend on private actors like banks or mobile operators.

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

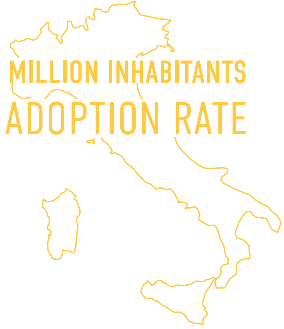
Choice of identity provider by the user: the user can choose to authenticate with the identity provider of his choice, among several widely used public and private organizations. Only one credential is needed to access the ecosystem.

TECHNOLOGY IMPLEMENTATION

> An interoperable by design system with the use of standards such as OAuth 2 and Open ID Connect.
> A technologically agnostic solution: identity providers are free to use any technology if they respect the regulatory framework.

GO TO MARKET & PROMOTION

SPID


60 MILLION INHABITANTS
26% ADOPTION RATE

GOVERNMENT-DRIVEN	FEDERATED SCHEME	USERNAME & PASSWORD + OTP code or App according to LoA	LIVE SINCE 2016

✓ IDENTIFICATION *online & in presence*	✓ ID ATTRIBUTES SHARING	✓ AUTHENTICATION	✓ ELECTRONIC SIGNATURE	✓ CROSS-BORDER RECOGNITION
100% **Italian public services are connected to SPID by law.** Many private services are already connected or are planning to connect.	*SPID federation foresees another entity, called Attribute Authority which provides certified attributes based on the authenticated user. No attributes are shared between identity providers.*	*Single Sign-On only for some services with low LoA*	*Process varies depending on the chosen identity provider. Since March 2020, SPID may also be used to sign documents and contracts electronically, with the same effects as handwritten signatures.*	**EIDAS NOTIFIED SINCE 2018** FOR SEVERAL LEVELS OF ASSURANCE (INCLUDING HIGH) DEPENDING ON THE CHOSEN SOLUTION.

CONTEXT & OBJECTIVES

The Italian Public System of Digital Identity (SPID) is a digital identity scheme managed by the "Agenzia per l'Italia Digitale" (AgID) and financed by private accredited identity providers.

SPID's main objective is to provide a device-free (with the exception of the smartphone) digital identity to all Italian citizens and companies, and to allow them to easily access public administration services for free. With more than 10 million identities issued, the scheme is considered a success in Italy. More and more private service providers are willing to join the ecosystem and are being accredited progressively by AgID.

VALUE PROPOSITION

SPID is a public open ecosystem allowing private accredited identity providers to provide digital identity for citizens and businesses. Currently, every citizen can choose up to nine free identity providers, although most users have one. Professionals and companies can also subscribe to a special type of identity made especially for businesses, for a fee.

SPID allows citizen to access public and private services with a single credential, safe, easy to remember and usable on computers, tablets and smartphones. To access services that require a higher degree of security, the user chooses a username and password and a temporary access code (one-time password) is generated. The use of an app available of any device (smartphone) or biometrics can also be additional authentication factors.

SPID also provides a secure and reliable system to Italy's public administration that now delegates heavy identity processes (issuing and maintaining credentials, etc.) and saves resources in terms of workload and costs.

BUSINESS MODEL: PRIVATE SECTOR FUNDED

> The federated scheme is financed by private identity providers who expect an important return on investment in the coming years (some services providers havec paid over1M € a year for OTP SMS.)
> SPID is free for citizens and public service providers for all level of security except for the highest level of assurance, used mainly by professionals and linked to a qualified electronic certificate.
> Private service providers follow a pay-per-use model and pay a fee per unique user per year to the identity providers (0.40€ to 7€ depending both on the amount of attributes and the LoA requested)
> SPID will also provide new types of digital identities to professionals and companies for a fee, which will be a component of the business model.

SECURITY & PRIVACY CHOICES

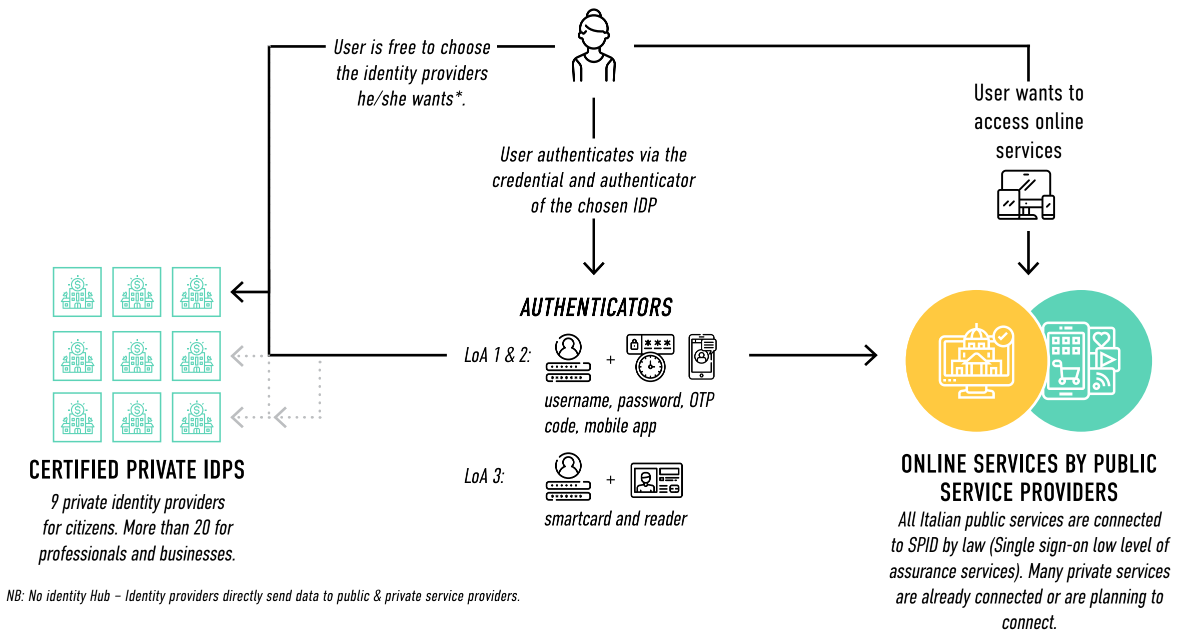
> AgID acts as a supervisor for data protection and management. The conformity and security assessment bodies assess the candidate provider before the accreditation by the AgID.
> SPID loA are consistent with standard ISO-IEC 29115 as well as eIDAS. Unlike other eID schemes with national gateway between IdPs and SPs, SPID enables direct data sharing (only the personal data that required to perform a service) from IDPs to SPs after citizen consent. Although it may seem a non-optimal choice in terms of privacy, other technical and organisational strategies make SPID fully compliant with the "privacy by design" principle[1].

PROJECT MILESTONES

2016	End of 2017	2018	2019	2020	2021
Launch of SPID with 3 identity providers.	All 600 public services are accessible by 2018.	2.5M SPID digital identities issued. eIDAS notification of SPID	5.5M SPID digital identities issued.	15M SPID digital identities issued.	Objective of 20M SPID identities issued and number of private service providers x2

[1] privacy by design" principle set out in Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.

SPID DIGITAL ID ECOSYSTEM


User is free to choose the identity providers he/she wants*.
User authenticates via the credential and authenticator of the chosen IDP
User wants to access online services
AUTHENTICATORS
LoA 1 & 2:
+
username, password, OTP code, mobile app
LoA 3:
+
smartcard and reader
CERTIFIED PRIVATE IDPS
9 private identity providers for citizens. More than 20 for professionals and businesses.
ONLINE SERVICES BY PUBLIC SERVICE PROVIDERS
All Italian public services are connected to SPID by law (Single sign-on low level of assurance services). Many private services are already connected or are planning to connect.

NB: No identity Hub – Identity providers directly send data to public & private service providers.

LEGAL FRAMEWORK

> National Legal framework stipulates that the acceptance of SPID is mandatory for the public sector.
> SPID is regulated by the Digital Administration Code via an implementing legislative decree (commonly known as the CAD) and by several guidelines and technical rules issued by the Italian Digital Agency (AgID).

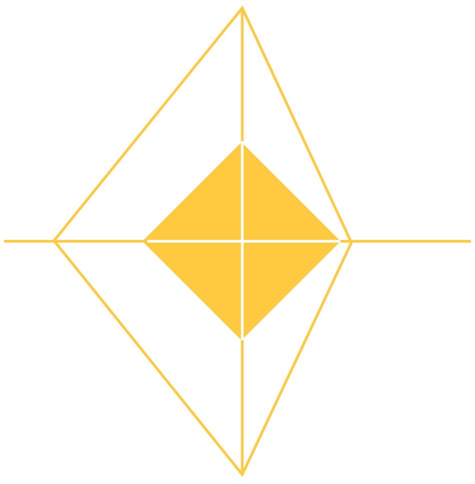
OTHER DIGITAL ID INITIATIVES IN THE COUNTRY

> The national ID card (CIE) was eIDAS notified in its last version (Carta d'identità elettronica (CIE 3.0) launched in 2016) in 2019. This scheme, highly adopted (in 2020, 13,6M new ID cards have been delivered so far), is mainly based on the physical electronic ID card, released in 2001.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

A private and public governance and busines model with a scheme managed by the government, but entirely financed by the private IDPs.

ECOSYSTEM & GOVERNANCE



END USER VALUE PROPOSITION

A 100% mobile-based strategy with a diversity of choice to access substantial LoA services: users can choose between the national eID card (CIE), a qualified electronic signature, or a more user friendly remote qualified signature where the HSM is often hosted by the identity provider.

TECHNOLOGY IMPLEMENTATION

OpenID connect standard choice for SPID, instead of SAML (used by most of the EU notified schemes). This solution allows, among other features, a better UX when using mobile device.

GO TO MARKET & PROMOTION

A unique audio and video remote process for citizen enrolment (vs. physical presence) with a live validation by an operator, which takes around 20 minutes. SPID was the first scheme to be notified with a remote enrollment process. Satisfaction rates concerning remote onboarding are extremely high, proving useful during COVID-19 outbreak. Recently, AgID has authorized a new procedure to improve enrollment time and process (10 seconds for audio and video recording without a live operator): citizens perform random actions requested by the app and the operator decides later to validate or not the enrolment process.

EID.LI

38,7 THOUSANDS OF INHABITANTS
5% ADOPTION RATE

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

MOBILE ID SMARTPHONE APP (EID.LI APP) WITH A PIN AND BIOMETRIC AUTHENTICATION

LIVE SINCE 2020

✓ IDENTIFICATION *online and offline*

✓ ID ATTRIBUTES SHARING

✓ AUTHENTICATION *Old Smartcard and mobileID provides advanced electronic functions facilitating secure authentication (FIDO protocol).*

✓ ELECTRONIC SIGNATURE

○ CROSS-BORDER RECOGNITION

nearly 200 governmental e-services *available including tax declarations, forms with an auto-filling feature. e-post, car registration, etc.*

EIDAS NOTIFICATION PLANNED FOR 2021

CONTEXT & OBJECTIVES

With a population of less that 40,000 people, Liechtenstein is a small European country which has developed a strategy and a digital agenda for the development of digital services.

In 2008, Liechtenstein developed a digital identity scheme relying on their National Electronic ID-card. Based on an embedded PKI certificate, the smartcard is used by citizens, residents and businesses to access governmental online services.

The card was issued by the National Immigration and Passport Office of Liechtenstein, the governmental agency in charge of developing the digital identity scheme is the Office of Information Technology.

In April 2020, the Principality of Liechtenstein launched a new mobile-based eID named eID.li and is planning to phase-out its smartcard in the coming months.

The eID.li app is tied to the mobile device that was used for registration through cryptographic measures. Users can then utilize their eID.li app to log in to a service and authenticate by using biometrics.

The current ambition of the Office of Information Technology of Liechtenstein is to expand the digital identity scheme to the private sector and become eIDAS notified in the coming years. A project to develop mobile eID for businesses is also in progress: employees would be able to represent their business / company using the digital identity scheme and upload tax declarations.

VALUE PROPOSITION

eID.li is the new digital identity with which citizens and residents of Liechtenstein as well as foreign nationals can securely identify and log in to electronic services. It comes with many benefits: easier enrollment and updates, strong user experience (ex: forms are automatically filled out with the registered personal attributes and sent easily to the government).

A GOVERNMENT FUNDED BUSINESS MODEL

> The government is financing 100% the digital identity scheme.
> The access to eID is free for citizens, residents and businesses.
> The project to expand the ecosystem to private service providers includes introducing pay per use modalities.

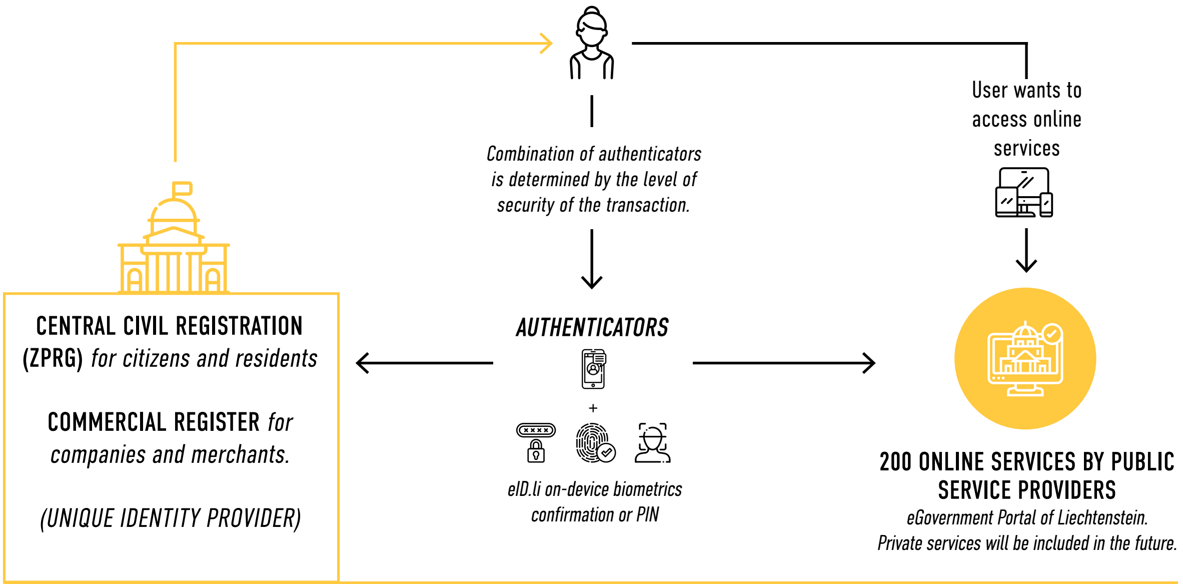
SECURITY & PRIVACY CHOICES

> Regular penetration tests and audit of the systems.
> For data protection, the Office of Information Technology of Liechtenstein follows general data protection regulation from the EU and Liechtenstein.
> The Office of Information Technology will go forward with the eIDAS notification for the levels substantial and high.

PROJECT MILESTONES

2008	2018	2020	2021	2023/2027+
Launch of the digital identity project	Issuance of a total of 5000 smartcard-based eID.	Launch of a new mobile-based eID in April. 500 mobile-ID are issued in October.	Objective to get eIDAS-notified for LoA high and substantial, to open to the private sector and implement remote video onboarding process	Objective to digitize all businesses processes and to adopt a digital-only policy for all citizens and residents according to the eGov roadmap.

LIECHTENSTEIN DIGITAL ID ECOSYSTEM



CENTRAL CIVIL REGISTRATION (ZPRG) *for citizens and residents*

COMMERCIAL REGISTER *for companies and merchants.*

(UNIQUE IDENTITY PROVIDER)

Combination of authenticators is determined by the level of security of the transaction.

AUTHENTICATORS

eID.li on-device biometrics confirmation or PIN

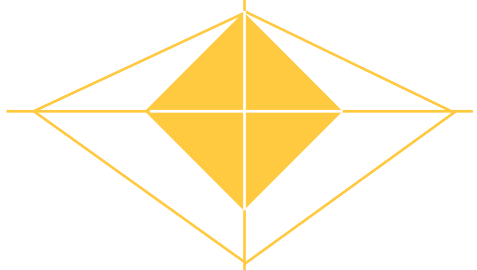
User wants to access online services

200 ONLINE SERVICES BY PUBLIC SERVICE PROVIDERS
eGovernment Portal of Liechtenstein.
Private services will be included in the future.

LEGAL FRAMEWORK

The Government adopted the Consultation Report on the adoption of a law implementing eIDAS Regulation, about electronic signatures and trust services in July 2019.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...



ECOSYSTEM & GOVERNANCE

END USER VALUE PROPOSITION

TECHNOLOGY IMPLEMENTATION

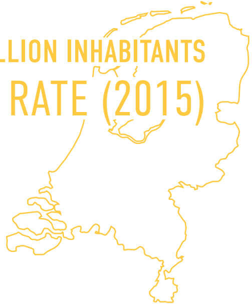
> Ambition to be 100% mobile by replacement of the smartcard and its services by the new mobile ID scheme to bring more flexibility. The systems uses the latest technology and security mechanisms to secure their citizens identity: the eID.li App is strongly bound to the users mobile device.

GO TO MARKET & PROMOTION

> A very quick enrollment process for the new mobile ID to boost users adoption: the enrollment process for eID.li takes place at the immigration and passport office and lasts between 2 to 5 minutes. The handling of eID.li App is very user friendly. Moreover, Liechtenstein performs regular events and webinars to promote the new eID solution.

FOCUS ON NETHERLANDS

DIGID


17,4 MILLION INHABITANTS

87% ADOPTION RATE (2015)

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM	USERNAME & PASSWORD WITH SMS VERIFICATION AND MOBILE ID (APP), NFC CHECK	LIVE SINCE 2003

✓ IDENTIFICATION *online*	○ ID ATTRIBUTES SHARING	✓ AUTHENTICATION	○ ELECTRONIC SIGNATURE	✓ CROSS-BORDER RECOGNITION

615 connected public and semi-public organizations	EIDAS NOTIFIED SINCE 2020 WITH SUBSTANTIAL AND HIGH LEVELS OF ASSURANCE

CONTEXT & OBJECTIVES

Netherlands benefits from a very solid foundational identity system, with a digital centralized population register since 1994, which attributes a unique identity number (BSN) to each citizen.
The ID card, the passport and the driver's licence are the legalized documents, which are used to verify the identity of a person.
In 2003, the DigID was set up by the ICT Unit, which was established in 2001 by the Ministry of the Interior and the Association of Dutch Municipalities, to access government services.

Rather than developing its own identity system, Netherlands is creating an open market ecosystem, in which private parties can also provide digital identities services, thanks to a new legislation (Digital Government Act – February 2020). The objective is three-fold: benefit from the innovations in the marketplace, build competitiveness in terms of prices, and remain resilient by having several reliable identity services in case of failure. The government will act as an authoritative source of trusted information.

In addition, the government will release its new smartcard on the 1st of January 2021. They are also working on a mobile version of the ID card and passport.

VALUE PROPOSITION

When citizens or residents apply for a DigiD, they enter a username and password they will then use to identify. Authentication procedures will often require the use of the DigID app or SMS verification. For particularly privacy-sensitive transactions (ex: health information check or update), a once-only ID check of ID physical documents can be required (performed with the DigiD app on smartphones with an NFC reader). DigiD is linked to the citizen service number (BNS).

DigID enables citizens and residents to identify easily and securely to access digitized public services (government, educational institutes, healthcare institutions or pension funds). It became mandatory in 2006 for everyone who submits electronic tax returns in the Netherlands.

eHerkenning, that replaced DigID for business, built with a public-private network of organizations, provides authentication services for organizations.

A GOVERNMENT FUNDED BUSINESS MODEL

> The government is financing 100% the digital identity scheme.
> Free for citizens and public service providers.
> New open market ecosystem with private identity providers, defined by the new legislation Digital Government Act in february 2020.

The main pillars of the Act are:
- Mandatory for public service providers to request LoA substantial or high.
- Open up to multiple IDP's (next to DigID) – Public Service providers have to accept these newly entered authentication solutions.
- Potentially opening up to private sector service providers.
- Lawful processing of BSN (Unique Identity Number) organized in the law.

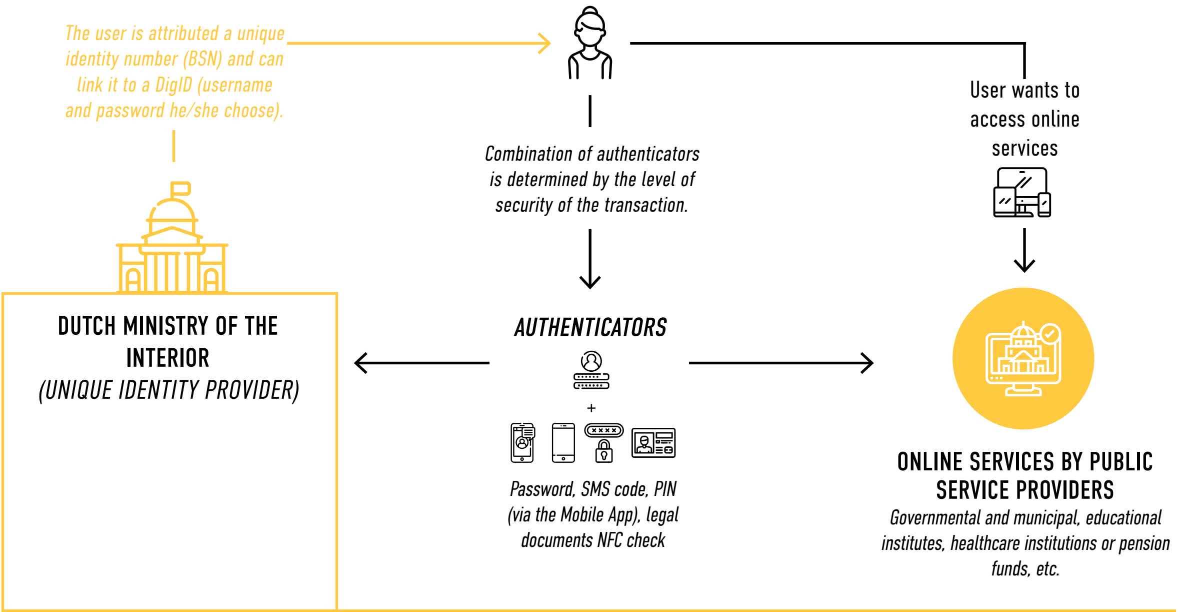
SECURITY & PRIVACY CHOICES

> Follow GPDR regulation.
> A unique identity number called BSN is used to establish uniqueness of the identity. It used to be printed on the ID card, but it will be removed to enhance privacy.
> Looking to adopt tokenization to anonymize the number for the different service providers. It will also be included in the eID card.

PROJECT MILESTONES

2003	2005	2011	2015	2020	2021
DigID launch	Launch of DigID for Business All public services are connected to DigID	Replacement of DigID for business by the eHerkenning	87% of the Dutch citizens over 16 years old are using DigID	eIDAS notification for DigID	1st of January, new eID card

DIGID ECOSYSTEM


The user is attributed a unique identity number (BSN) and can link it to a DigID (username and password he/she choose).
Combination of authenticators is determined by the level of security of the transaction.
User wants to access online services
DUTCH MINISTRY OF THE INTERIOR
(UNIQUE IDENTITY PROVIDER)
AUTHENTICATORS
+
Password, SMS code, PIN (via the Mobile App), legal documents NFC check
ONLINE SERVICES BY PUBLIC SERVICE PROVIDERS
Governmental and municipal, educational institutes, healthcare institutions or pension funds, etc.

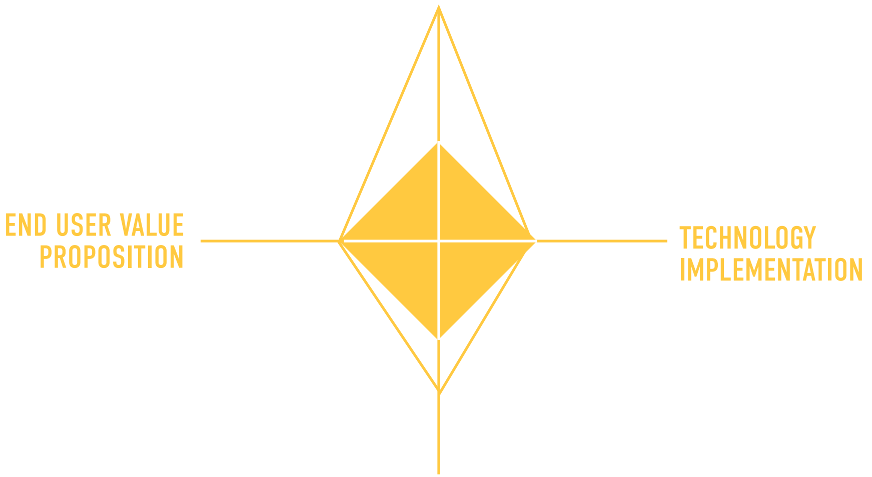
LEGAL FRAMEWORK

ICAO guidelines for credentials

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

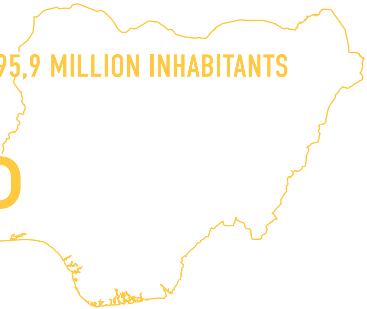
> A governmental position as an ecosystem builder rather than an identity system provider. with the government acting as an authoritative source of trusted information. Its objective is to bring trust in the digital economy. It issues the source identity and stamps it as a trusted digital identity issued by the government. Other service providers and identity providers can then make use of this to support other identification means.
> An open task force: the Dutch government works closely with the private sector but also with universities and knowledge institutes on digital identity matters.

ECOSYSTEM & GOVERNANCE



GO TO MARKET & PROMOTION

> A remote enrolment process: DigID is one of the rare digital identity scheme that is eIDAS notified with a remote enrolment procedure. The enrolment process takes several days to be completed: users have to fill an application form and they will receive a letter with an activation code within three working days. They can then activate their DigiD with their username, password and this code. After activation they are able to log in.



NIN & MOBILE ID APP

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

SMARTCARD (OR PRINTABLE NIN SLIP) + MOBILE ID (APP-BASED - CURRENTLY IN TRIAL)

LIVE SINCE 2014

✓ IDENTIFICATION *online & offline*

○ ID ATTRIBUTES SHARING

✓ AUTHENTICATION

> Smartcard can be used for authentication in combination with biometrics or a PIN (but lack of connected offline point-of-sales (POS))
> The mobile app will use Google Authenticator, among other credentials, for online authentication

✓ ELECTRONIC SIGNATURE

> Function with the Smartcard
> Digital ID Application will also feature the ability to digitally sign documents. Certificates and private keys will be stored in the Secure Element of smartphones, with backups stored securely on HSMs.

○ CROSS-BORDER RECOGNITION

In June 2021, bilateral discussions with ECOWAS and EAC countries for Cross-border recognition

CONTEXT & OBJECTIVES

Historically, the majority of Nigerians does not have any form of legal identification and the most populated country in Africa has a very fragmented identity landscape. Multiple non-interoperable private and public databases coexist (driver's licence, mobile operators, banks, voters' databases) requiring each different attributes.

To create a robust foundation for a future digital ID scheme, the Government set-up up the National Identity Management Commission (NIMC). It's main objective for the coming years is to capture data into a central, secure & harmonized identity database to provide a National Identity Number (NIN) to all Nigerians citizens, as well as refugees and Internally Displaced People (IDP).

The Digital ID scheme should improve financial inclusion - unbanked adult population in Nigeria is estimated between 40 and 60 million people - increase security and transparency, boost the economic development as well as reduce governance costs.

VALUE PROPOSITION

The National Identification Number (NIN) consists of 11 non- intelligible numbers randomly chosen and assigned to Nigerian citizens upon enrolment, during which demographic data, biometrics (10 fingerprints), head-to-shoulder facial picture and digital signature are captured.

Nigerians can use the national ID card for authentication and digital signature and it can also be used by banks for customer onboarding procedures (KYC). The card can also be used for payments, transfers or at ATMs. New services will be made available subsequently such as voting, pensions, health benefits, drivers licence, taxes, etc.

To date, smartcard penetration is low - only 1 million ID cards have been issued so far - due to a lack of available services. A new mobile ID ecosystem is ready for launch.

BUSINESS MODEL

> The federal government has the support of loans from the World Bank, the French Development Agency (AFD) and the European Union (UE) to finance the Digital ID scheme.
> Smartcard registration is free for citizens and residents, although there is a fee for card replacement (10$US).
> The Mobile ID app will be free for all NIN holders. Revenue will be generated by pre-purchasing credits, for anyone who wishes to pay any ID verification to access a service.

SECURITY & PRIVACY CHOICES

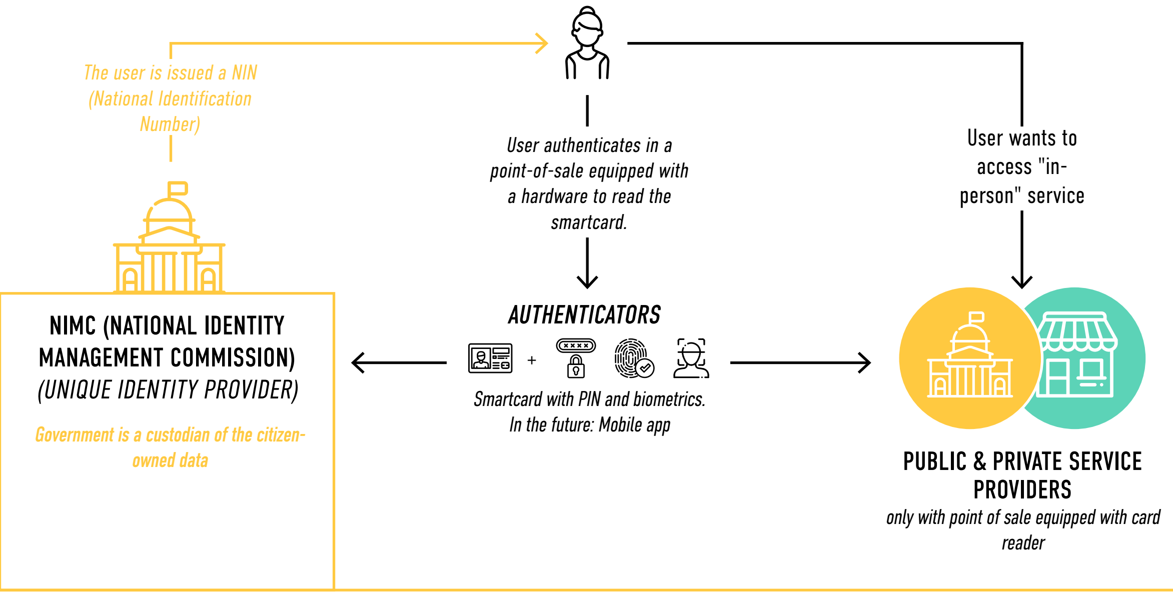
> NIMC issue a randomly generated number (National Identification Number, NIN) to all citizens.
> NIMC has a strong focus on security: encryption, backup servers, diesel generators. NIMC received ISO certification for its data storage and disaster recovery facilities and procedure.
> The Federal Government intends to actively pursue protecting Personal Identity by issuing secure, virtual credentials which will be time bound and issued by the Identity holder, for a specific merchant or verifier.
> No organization is mandated to protect the personal data and privacy of citizens.

PROJECT MILESTONES

2007	2014	2015	2016	2017	2020	2021
Creation of NIMC by the NIMC Act.	Smartcard launch	7M Nigerian registered in the database	14M Nigerians registered	28M Nigerians registered	Launch of the mobile app. 41M Nigerians registered.	Target of 90% Nigerians enrolled with a NIN number

NIGERIAN DIGITAL ID ECOSYSTEM

→ New services (including online ones) will be made available in the coming years.


The user is issued a NIN (National Identification Number)
User authenticates in a point-of-sale equipped with a hardware to read the smartcard.
User wants to access "in-person" service
NIMC (NATIONAL IDENTITY MANAGEMENT COMMISSION)
(UNIQUE IDENTITY PROVIDER)
Government is a custodian of the citizen-owned data
AUTHENTICATORS
+
Smartcard with PIN and biometrics.
In the future: Mobile app
PUBLIC & PRIVATE SERVICE PROVIDERS
only with point of sale equipped with card reader

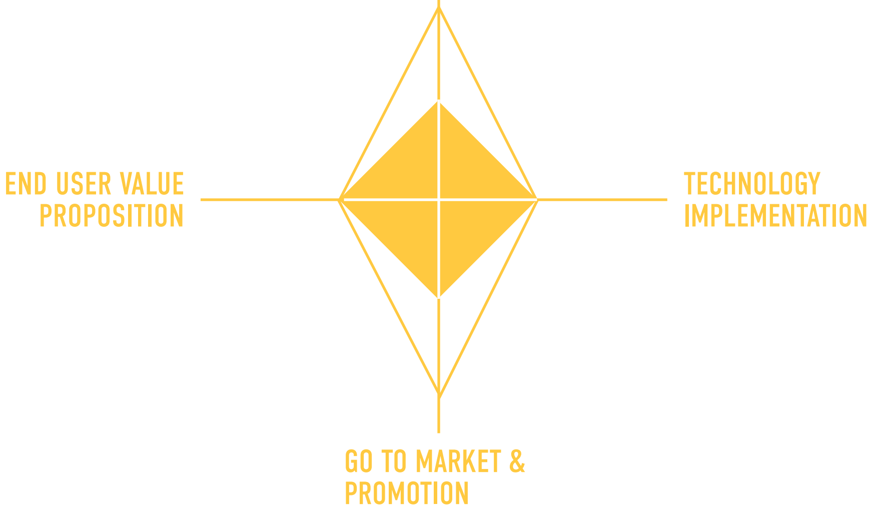
LEGAL FRAMEWORK

> Personal Data protection Act (2010)
> "Draft Guidelines on Data Protection" (2013): Private assessment and definition of policies on privacy that have been adopted by the government
> New data protection law (2019) inspired by European conventions. The law was ratified by both parliaments but was not signed by the president in time before the government change.

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

An independent and autonomous agency (NIMC) governed by a board of 18 individuals representing different government agencies and stakeholders. Some of the benefits of this organization include multi-stakeholder coordination and leverage private sector innovation thanks to Public-Private Partnerships: private firms provides the funds in exchange for a revenue streams in the future digital ID scheme.

ECOSYSTEM & GOVERNANCE



Enrollment of public and private partners to reinforce and accelerate the registration rate (banks, mobile operators and government agencies).

10,3 MILLION INHABITANTS
1.5M ACTIVE USERS

CHAVE MÓVEL DIGITAL AND CITIZEN CARD

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

CITIZEN CARD (SMARTCARD) + MOBILE PHONE + PIN + OTP (SMS OR EMAIL) OR MOBILE APP

LIVE SINCE 2014 (2007 FOR THE CITIZEN CARD)

✓ IDENTIFICATION
online and offline
Users can identify offline using their citizen card but also a Digital ID wallet app since 2019.

✓ ID ATTRIBUTES SHARING
Users can decide to select some or all attributes to share for each authentication.

✓ AUTHENTICATION
Citizen Card and Digital Mobile Key provide advanced electronic functions facilitating secure authentication (FIDO protocol).

✓ ELECTRONIC SIGNATURE
QeS based on HSM

✓ CROSS-BORDER RECOGNITION

EIDAS NOTIFICATION (HIGH) FOR BOTH THE CITIZEN CARD AND THE DIGITAL MOBILE KEY

+200 online services accessible from the eGovernment portal

CONTEXT & OBJECTIVES

Portugal was one of the pioneering countries to implement digital certificates with its eID Citizen Card, launched in 2007. The mandatory smartcard contains 5 differents cards (Civil identification card, Taxation card, Voting card Social security card, Healthcare card) in one, and includes a qualified electronic signature for secure authentication, enabling citizens to complete electronic transactions and to sign electronic documents.

The Citizen Card was seldom used by citizens to access online services, leading the AMA (Administrative Modernization Agency of Portugal) to create a more practical and user-friendly mobile ID, the Digital mobile key or "Chave Móvel Digital" (CMD) in 2014. Today, the Citizen Card is mainly used by specific audiences, mostly business or medical prescriptions, for its electronic signature service.

Contrary to the Citizen Card, the Digital Mobile Key is not mandatory but its activation is important, since practically all websites that provide public services - including ePortugal - have adopted this authentication system.

Since 2019, citizens can also upload their driver's licence, their Citizen Card, as well as other cards on a Digital ID wallet app (ID.gov.pt) avalailable on their mobile phone.

A GOVERNMENT FUNDED BUSINESS MODEL

> The government finances 100% of the digital identity scheme.
> The authentication and digital signature processes are free for citizens, residents and businesses.
> No fees for the public and private sectors providers, except for the costs of the OTP SMS sent.

VALUE PROPOSITION

Digital Mobile Key enables secure authentication on various public and private websites, requiring only a mobile phone, a 4 to 8 digit PIN code and an OTP (temporary code sent by SMS or e-mail). Since 2020, a biometric recognition system using the mobile phone can also be used to replace second factor authenticators such as OTP.

For Portuguese citizens, their Digital Mobile Key links their civil identification number to their mobile phone number, and the passport or title / residence card number for a foreign citizens

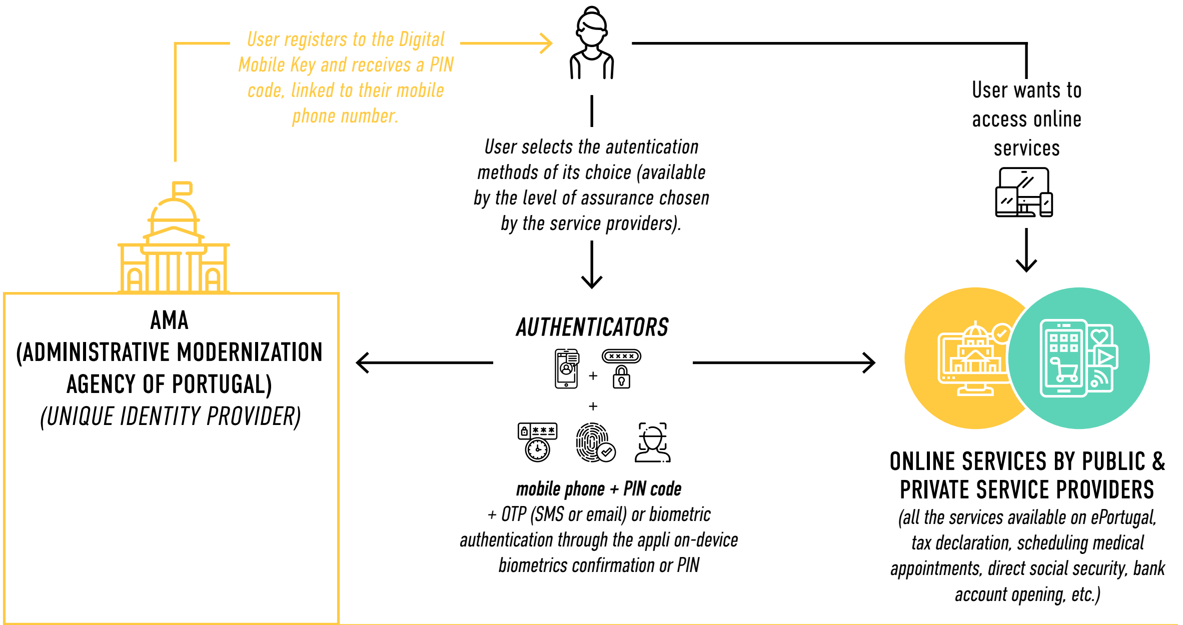
SECURITY & PRIVACY CHOICES

> Same security requirements for the Citizen Card and the Digital Mobile Key.
> Both the Citizen Card and the Digital Mobile Key are eIDAS notified with a High level of assurance. The service providers defines the level of assurance in each specific applications.
> Yearly audits for the eID platforms to maintain the qualification for providing digital signature and issuing qualified certificates.
> Privacy by design principles are applied. Users can check their authentications and signatures trackrecord on the Authenticao.gov website.

PROJECT MILESTONES

2007	2014	2018	2019	2020
Launch of the Citizen Card	Launch of the Digital Mobile Key (CMD)	160,000 CMD active users. QeS can be done with CMD	Law allowing for the digitization of driver's licence, citizen card, and other cards on a Digital ID wallet mobile app	1.5M active users (2M created accounts) Around 4,000 CMD enrollment per day

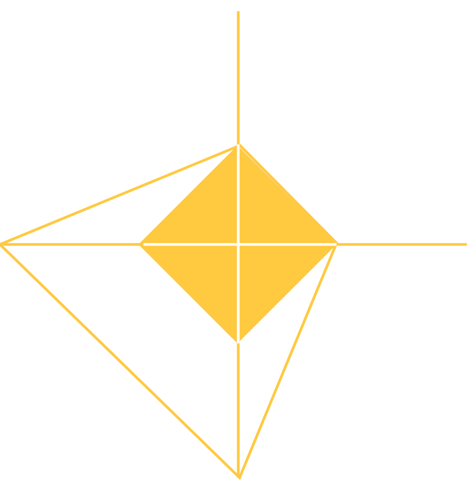
DIGITAL MOBILE KEY ECOSYSTEM


User registers to the Digital Mobile Key and receives a PIN code, linked to their mobile phone number.
User selects the autentication methods of its choice (available by the level of assurance chosen by the service providers).
User wants to access online services
AMA
(ADMINISTRATIVE MODERNIZATION AGENCY OF PORTUGAL)
(UNIQUE IDENTITY PROVIDER)
AUTHENTICATORS
+
+
mobile phone + PIN code
+ OTP (SMS or email) or biometric authentication through the appli on-device biometrics confirmation or PIN
ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
(all the services available on ePortugal, tax declaration, scheduling medical appointments, direct social security, bank account opening, etc.)

LEGAL FRAMEWORK

> The GNS (Gabinete Nacional de Segurança) public authority is responsible for the security.
> There is two national security organizations (GNS and CNCS (Centro Nacional de Cibersegurança - National Security Office - National Cybersecurity Centre))
> For the privacy, the CNPD authority (National Commission of Data Protection) reports to the Parliament

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...



ECOSYSTEM & GOVERNANCE

TECHNOLOGY IMPLEMENTATION

END USER VALUE PROPOSITION

> A very user centric and inclusive mobile ID scheme which offers simplicity and convenience for all citizens and residents (not only smartphones - the CMD is linked to a phone number) without compromising the level of security. The option of biometrics as an authentication factor to replace the OTP also increases the usability of the solution. User centricity continues to be a priority for the Portuguese government, which had already stood out with its 600 citizen shops (physical counters with the assistance of a trained mediator) and its recent chatbot SIGMA to provide citizens with online assistance.

GO TO MARKET & PROMOTION

Multiple enrollment channels for the Digital Mobile Key (CMD): an impressive leap was made when the AMA decided to create multiple enrollment channels. In addition to traditional face to face or by using the eID citizen card with a smartcard reader, two new channels are now available:
> Enroll for CMD when renewing the Citizen Card
> Enroll for CMD when using the tax department password. Codes are sent by physical mail thanks to the address that is linked to the citizen.
> The AMA is also thinking of enabling users to enroll for the CMD through ATMs or biometrics available through the mobile phone.

5,6 MILLION INHABITANTS

95-50% ADOPTION RATE (SINGPASS / MOBILE ID)

NATIONAL DIGITAL IDENTITY

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

MULTIPLE AUTHENTICATION FACTORS including cryptographic Mobile ID based on an app, cloud-based face recognition (physical and remote), PIN and passwords

LIVE SINCE 2003

✓ IDENTIFICATION *online & offline*

The "Verify with SingPass" feature enables users to perform secure face-to-face identity verification and data transfer through scanning of QR codes or NFC.

✓ ID ATTRIBUTES SHARING

Adoption of privacy principles, including specificity of purpose, consent driven access and data sharing and data minimalization.

✓ AUTHENTICATION

SingPass and SingPass mobile are using secure single sign-on for government services.

✓ ELECTRONIC SIGNATURE

Digital signature through the scanning of QR codes launched in October 2020.

○ CROSS-BORDER RECOGNITION

Discussions are engaged with several countries to look at bilateral pilots.

+1000 governmental services *are connected to SingPass* +300 services *are connected to CorpPass* +100 e-services *relies on MyInfo Business*

CONTEXT & OBJECTIVES

Since 2003, Singaporeans have been using SingPass to access online government services. With more transactions going online, Singapore's Government Technology Agency (GovTech) is now expanding SingPass into a National Digital Identity (NDI) scheme. The objective is to provide a government-as-a-platform service for users and businesses, with a universal digital identity scheme to transact with both the Government and private sector more securely and seamlessly.

The National Digital Identity (NDI) platform has been progressively introduced since 2017, enabling the private and public sectors to develop more value-added services on this common and universal trust platform.

VALUE PROPOSITION

The project brings various digital tools together to provide greater online convenience and transactional security for citizens and businesses. The primary product available on the consumer side is SingPass Mobile. On the business side, the main products are:

> Login with SingPass, an authentication-as-a-service that business can subscribe to.

> MyInfo / MyInfo Business, a data platform where citizens/businesses can give consent to businesses to retrieve data from government sources upon consent.

> Verify with SingPass, an in-person ID verification service.

> SingPass Face Verification, an ID verification as-a-service via face biometrics.

> Sign with SingPass, enables secure crypto digital signing.

There are several benefits of the NDI ecosystem: for citizens and residents, the NDI scheme provides a single digital identity, with a better security, user experience and efficiency.

For businesses, the NDI platform offers numerous benefits, with stronger security and user experience for customers and employees. Businesses are also encouraged to leverage the NDI platform to use features like digital signing to build value-added services.

A GOVERNMENT FUNDED BUSINESS MODEL

> NDI is government-owned and fully financed.

> Free for citizens and for businesses during the initial adoption period. Freemium models are being explored for the future.

> Businesses have reported savings of over $50 per transaction, and an 80% reduction in transaction time when their customers use MyInfo to prefill forms with information from government sources. Businesses also report up to 15 per cent higher approval rate for transactions due to better data quality input with MyInfo.

SECURITY & PRIVACY CHOICES

> Cybersecurity governance led by Cybersecurity Agency of Singapore (CSA).

> Adoption of Security-by-Design approach to ensure security design, assurance and testing at every stage of the product development and operations stage.

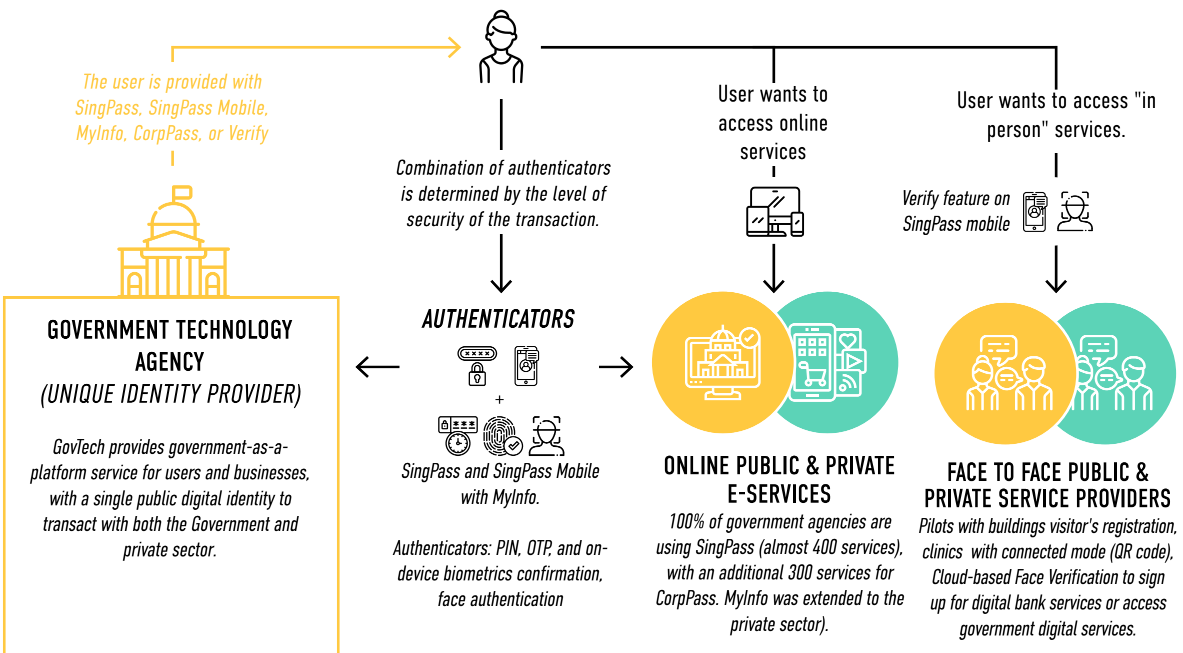
> Availability of multi factor authentication for step up authentication for more sensitive transactions.

> For Face Verification, no personal data is shared with relying parties; only a matching score will be returned after face matching is done. This service removes the burden of collecting, storing and securing data for businesses.

PROJECT MILESTONES

2003	2015	2016	2017	2018	2019	2020
Launch of SingPass	Launch of the new version SingPass with multi factor authentication, UX improvements	3,3M of users (equal to 66% population) 57M transactions 350 e-services and 64 GovAgencies connected	Launch of NDI program Pilot launch of MyInfo with the banking sector	Launch of SingPass Mobile app. 100% of gov agencies are using SingPass.	Launch of pilots for Verify with SingPass and Notify	4M citizens use SingPass (95% of eligible users). 2.2M users for SingPass Mobile. Launch of pilot for SingPass Face verification and Sign with SingPass

NDI DIGITAL ID ECOSYSTEM



The user is provided with SingPass, SingPass Mobile, MyInfo, CorpPass, or Verify

Combination of authenticators is determined by the level of security of the transaction.

User wants to access online services

User wants to access "in person" services.

Verify feature on SingPass mobile

GOVERNMENT TECHNOLOGY AGENCY

(UNIQUE IDENTITY PROVIDER)

GovTech provides government-as-a-platform service for users and businesses, with a single public digital identity to transact with both the Government and private sector.

AUTHENTICATORS

SingPass and SingPass Mobile with MyInfo.

Authenticators: PIN, OTP, and on-device biometrics confirmation, face authentication

ONLINE PUBLIC & PRIVATE E-SERVICES

100% of government agencies are using SingPass (almost 400 services), with an additional 300 services for CorpPass. MyInfo was extended to the private sector).

FACE TO FACE PUBLIC & PRIVATE SERVICE PROVIDERS

Pilots with buildings visitor's registration, clinics with connected mode (QR code), Cloud-based Face Verification to sign up for digital bank services or access government digital services.

LEGAL FRAMEWORK

> Personal Data Protection Act

> Public Sector Governance Act

> Electronics Transaction Act

> National Registration Act

> Computer Misuse Act

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

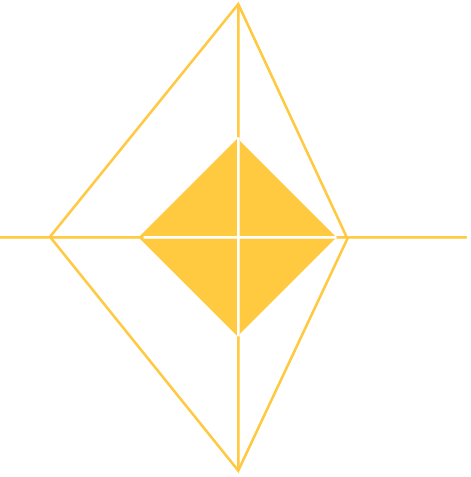
ECOSYSTEM & GOVERNANCE

> An in-house engineering team to enable faster response and innovation, especially during a crisis like the COVID-19.

END USER VALUE PROPOSITION

> Secure and convenient access to government and private sector services

> Accessing personal data and having the control to consent to sharing data when transacting on digital services, on both online and physical setting, for greater transparency, saving time and money.



TECHNOLOGY IMPLEMENTATION

Face verification matching with an image stored in an existing government-owned database to establish their identity. Face recognition service will be available as-a-service to government agencies and businesses. They will have to meet the governance requirements such as the obligation to ask for consent of the individual before face verification is conducted.

GO TO MARKET & PROMOTION

> A holistic communications strategy deployed to drive adoption among citizens with varying levels of tech-savviness.

> Leverage various Industry engagement platforms, both online and physical, to drive adoption of businesses.

> Developers and partners portal for businesses to easily integrate with the national identity platform.

> Pre-integrate with existing private sector solutions and platforms such as Adobe Sign, DocuSign and others.

FOCUS ON
UNITED STATES, ARIZONA

MVD SOLUTIONS

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM	MOBILE APP, COMPUTER WEB BROWSER *WITH FACIAL RECOGNITION, VOICE OTP, KBA*	LIVE SINCE 2020 *for the online portal*

☑ IDENTIFICATION *online & offline*	☑ ID ATTRIBUTES SHARING	☑ AUTHENTICATION	☑ ELECTRONIC SIGNATURE	○ CROSS-BORDER RECOGNITION
Face to face identification available in the beginning of 2020 with the digital driving licence mobile app.	*Digital driving licences enables sharing of required attributes to access a service.*	*Authentication on the website of the ADOT to access a wide range of online services. Opening of the platform to other public and private services planned in the roadmap.*	*The MDV accepts electronic signatures on all documents if they are authenticated by login into the portal and signing them on the portal.*	40 MVD services *are available through the portal*

CONTEXT & OBJECTIVES

In a country where driver's licences are the most used proof of identity, the Department of Transportation of Arizona (ADOT) was a pioneer in providing innovative online services to its customers. Currently, 65% of the registration renewals in the state are done through their website, a much higher rate than in most other states.

In 2018, the agency launched a new consumer portal, AZ MVD Now, with innovative multifactor authentication features, including a mobile app for authentication.
The next steps for the MVD (Motor Vehicle Division) is to transition to a fully deployed mobile digital licence app in 2021. It will securely store public credentials (Driver Licence, Photo ID Card) in a digital format. Following which, the MVD's objective is to expand the eAZ Identity Superportal, that will enable Arizona citizens to find and obtain online services from other participating Arizona public agencies.

VALUE PROPOSITION

The AZ MVD Now portal enables Arizona citizens to obtain most MVD services (Driver's licence renewal, vehicle registration, etc.) on a self-serve basis, without having to visit a MVD field agency.

In the coming years, the MVD strategy is to expand the identity capabilities of the Driver Licence beyond the simple right to drive with the eAZ Identity Super portal. The initial pilots included several public agencies for use cases such as pet registration, hazardous waste disposal permits, or campaign finance reporting system.

The democratization of identity proofing in the state of Arizona will pave the way to the widespread use of digital identity. In particular for business registrations, that are complex in Arizona. Applicants must go through a long process and fill-up forms for up to 7 state agencies. The eAZ Identity Super portal should ease the process and boost the dynamism of the economy.

A GOVERNMENT FUNDED BUSINESS MODEL

> Currently free for citizens.
> In the future, tools will be available for free to relying parties such as businesses.
> In total, $US60m investment from the ADOT since 2015 for their IT system reengineering, including the online portal and delivering mobile ID.

SECURITY & PRIVACY CHOICES

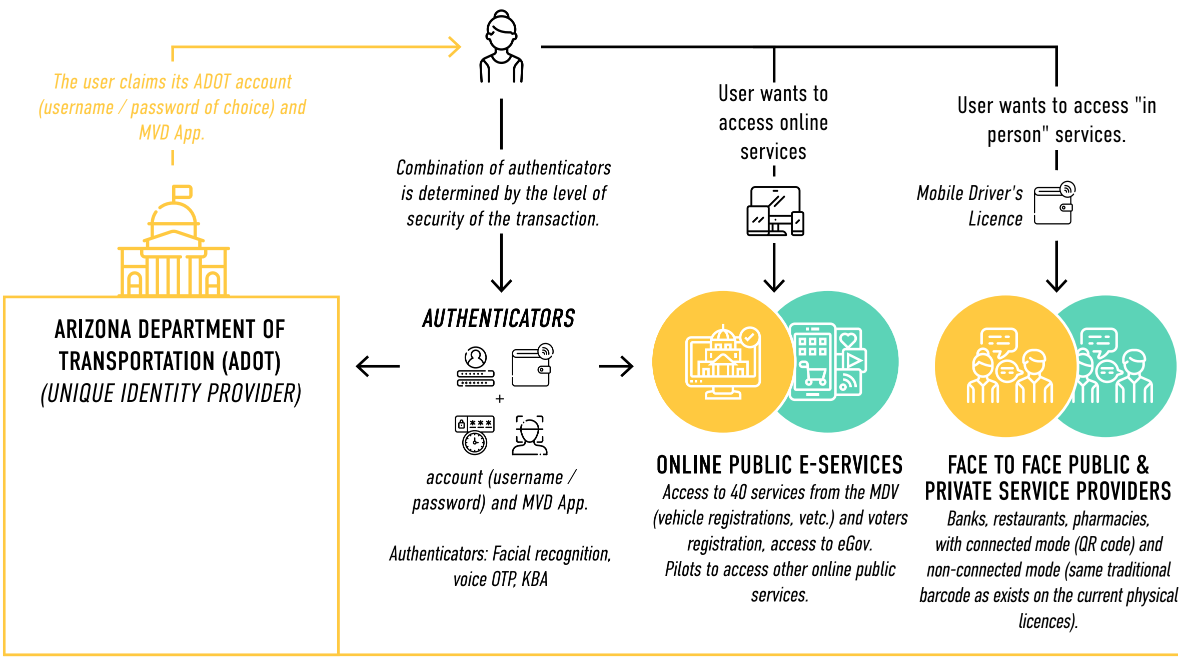
> To ensure an optimal level of security without down grading the user experience, the Department of Transportation implemented a simple and adaptative registration process. The agency requires only basic information, and asks simple questions to its users, They then run real-time checks on the device and the connection, among other factors. After attributing a score to users, they decide which authenticators will be required to access the service, with, for example, a mobile app or a computer web-based facial recognition.

While every login is assessed, the initial account creation (enrollment) and certain other specific, sensative transactions, including the reimbursement of funds and transfer of ownership, are more guarded than others and may require additional authentication actions by the customer.

PROJECT MILESTONES

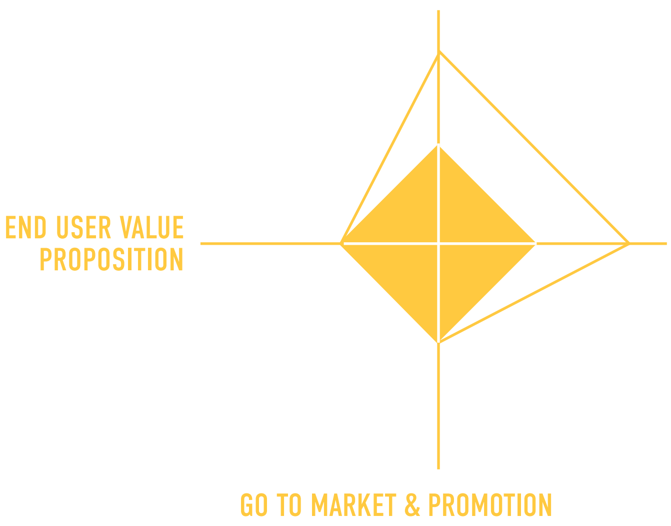
2018	April 2020	November 2020	2021
Launch of the AZ MVD Now online portal.	Launch of the platform. 200.000 accounts registered on the AZ MVD Now portal.	1.5m accounts are created, not all have the app.	New version of the Mobile Driver Licence

ADOT DIGITAL ID ECOSYSTEM


The user claims its ADOT account (username / password of choice) and MVD App.
Combination of authenticators is determined by the level of security of the transaction.
User wants to access online services
User wants to access "in person" services.
Mobile Driver's Licence
ARIZONA DEPARTMENT OF TRANSPORTATION (ADOT)
(UNIQUE IDENTITY PROVIDER)
AUTHENTICATORS
+
account (username / password) and MVD App.
Authenticators: Facial recognition, voice OTP, KBA
ONLINE PUBLIC E-SERVICES
Access to 40 services from the MDV (vehicle registrations, vetc.) and voters registration, access to eGov.
Pilots to access other online public services.
FACE TO FACE PUBLIC & PRIVATE SERVICE PROVIDERS
Banks, restaurants, pharmacies, with connected mode (QR code) and non-connected mode (same traditional barcode as exists on the current physical licences).

INNOVATIVE APPROACH TO DIGITAL ID IN TERMS OF...

> A specific organization to rely on the best expertise while retaining the intellectual property of developed solutions: It can be difficult to get the right resource in-house, transformation projects requiring specific expertise. To build their solutions as internal projects, the ADOT outsourced the expertise (but not the contract) and hired 60 to 70 individual contractors. As a result, they have entire ownership of the intellectual property, along with their solutions, and benefit from more flexibility and control over their project management.

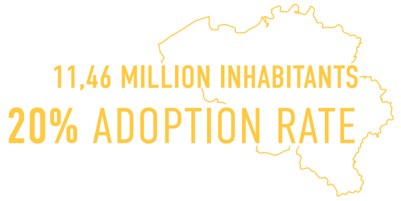


TECHNOLOGY IMPLEMENTATION

> Computer web-based face recognition to access online service for enhanced authentication method.

THE FOLLOWING COUNTRIES HAVE NOT BEEN COVERED BY IN-PERSON INTERVIEWS. THE DIGITAL ID SCHEMES DESCRIBED ARE THE RESULT OF DOCUMENTARY RESEARCH AND EXPERIENCE FROM THE ONEPOINT AND SIA TEAM.

FOCUS ON BELGIUM



11,46 MILLION INHABITANTS

20% ADOPTION RATE

ITSME®

CROSS-INDUSTRY LED (BANKS AND MNOS)

FEDERATED SCHEME

MOBILE APP rooted to banking apps

LIVE SINCE 2017

✓ IDENTIFICATION *online only*

Online identification to create a new account or apply a Know-Your-Customer process (eID card and Itsme)

✓ ID ATTRIBUTES SHARING

✓ AUTHENTICATION

Allows users to log in using Itsme or Belgium eID card

EIDAS NOTIFICATION (HIGH) FOR BOTH EID CARD AND ITSME APP

✓ ELECTRONIC SIGNATURE

Qualified Electronic Signature with eID card (eIDAS regulation) widely used in the professional sphere

✓ CROSS-BORDER RECOGNITION

Itsme will soon be tested in Luxemburg with ambitions to address other EU markets.

700+ PUBLIC AND PRIVATE E-SERVICES ACCESSIBLE WITH ITSME®

34% represent access to government e-services

66% represent access to private services

NATIONAL REGULATION FRAMEWORK: ROYAL DECREE ON EID IN 2004 - LAW ON ACCESS TO PERSONAL DATA IN 2012.

CONTEXT & OBJECTIVES

Itsme was created and is owned by a private consortium (Belgium Mobile ID) composed of four banks and three Mobile Network Operators in the country with the goal to offer a unique mobile ID solution that would be used to secure access to their own services, increase their users' satisfaction and monetize the security solution amongst third party service providers.

In January 2018, the Belgium government recognised Itsme as an official digital ID to secure access to public services and as a result notified itsme to the EU commission, resulting in cross border recognition.

VALUE PROPOSITION

Itsme mobile app complements existing digital ID scheme based on the eID card, and brings the necessary additional level of convenience and addresses demands for mobility.
Itsme is built around an intuitive mobile application that enables a highly portable, ubiquitous means of identification, supported by a secret five-digit code or fingerprint scan. As a result, it addresses many of the issues that currently compromise the user experience in digital domains, including password fatigue, vulnerability to cyber-attack and a lack of control over personal information.

For service providers, the scheme allows an easy KYC process, with onboarding of customers based on verified and 100% accurate ID data. They also benefit from high end security solutions for their online services at a fraction of the cost and only pay depending on volume of users, type of transactions and level of services (identification, authentication, digital signature). Over 140 private service providers have joined the scheme to leverage Itsme to secure their online channel.

A PRIVATE SECTOR FUNDED BUSINESS MODEL

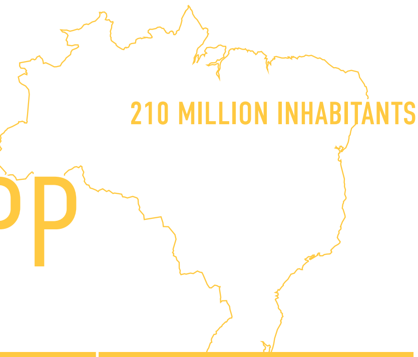
> "Belgium Mobile ID" consortium launched and is operating Itsme mobile ID.
> The scheme is based on privacy principles with no data monetisation.
> Itsme is free for citizens. Service providers bear the costs with a taylored plan to fit each need. A per-transaction fee was first trialled then dropped as it deterred engagement, and replaced by an annual subscription model based on volume of users and type of services (simple login, full check in with verified data, full digital including transactions approval).

SECURITY & PRIVACY CHOICES

> Very strong compliance respect of PSD2, GDPR and eIDAS, certified to ISO/IEC 2700.
> Itsme enables end-users to create an account without ID data sharing or link an existing account with itsme®.
> Onboarding to itsme can be done through eID card online reading or through verified ID from banks and mobile operators.

PROJECT MILESTONES

2002	2017	2017	2018	2020
Deployment of the national eID card: Belgium becomes a pionner in e-gov system.	100% of the population has the national smartcard eID.	Private consortium Belgian Mobile ID launched Itsme mobile app.	400.000 Itsme users. Belgian eID card is recognized for e-IDAS high level of assurance.	Itsme and FAS (Belgian government's Federal Authentication Service) notified by EU Commission. 2 Million Itsme users in June 2020. Over 8 million itsme transactions performed every month.



210 MILLION INHABITANTS

CPF ID WALLET APP

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM	DIGITAL WALLET APP WITH BIOMETRIC AUTHENTICATION	LIVE SINCE 2020

✓ IDENTIFICATION *online & offline*	○ ID ATTRIBUTES SHARING	✓ AUTHENTICATION *using biometrics (face recognition)*	○ ELECTRONIC SIGNATURE	○ CROSS-BORDER RECOGNITION

CONTEXT & OBJECTIVES

The Brazilian national digital identity program (Identificaçao Civil Nacional - ICN) was announced by the government in 2017. Brazil's Superior Electoral Tribunal (TSE) operates the program which has been especially designed to cut down on election and voter fraud.

The program includes the centralization of all the biometric data (photos and fingerprints) collected during the elections in the 27 different states and from the IRS (Individual Taxpayer Registry), into one nation-wide centralized biometric database.

The project is government-driven, with an intention to privatize various public tech companies contributing to the development of the Digital ID:
- Serpro, the federal data processing service, which has developed the Digital ID application,
- Dataprev, a social security technology firm,
- Brazilian telecom company Vivo, in charge of biometric registration for the country.

In parallel, Brazil's digital government strategy (2020-2022) will consolidate 1500 government websites into a single portal and in expection of wider cloud adoption and broader access to open government data.
In 2020, the Brazilian government has launched a new app (CPF ID Wallet App) that unites the social security card and the driving licence. The goal is to provide main utilized documents, such as the ID card or the birth certificate, available under a single app.

VALUE PROPOSITION

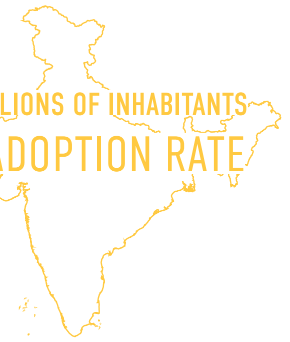
The digital versions of the documents are available through the new CPF ID Wallet App and are validated through a QR Code. The app provides citizens access to several services linked to their CPF with the Federal Revenue of Brazil, Ministry of Economy and Federal Government. Since 2019, Brazilians can access the government services using their social security number.

Enrollment will be done through the mobile app by using biometrics with in-person validation checks by a government agent at specific locations.
Only public authorities (Executive and Legislative powers of the Union, the States, the Federal District and the Municipalities) have access to the ICN database. They may create their own database from ICN content (excluding biometrics).

OTHER SPECIFIC SERVICES & USE CASES:
> Access to emergency aid scheme for financially vulnerable citizens.
> Includes a chatbot to help submit the annual income tax declaration.

PROJECT MILESTONES

2008	2017	2019	2020	2022
Biometric registration of voters begins	Set-up of the legal framework for the National Digital Identity program	About 50% of Brazilians are biometrically registered	Finalization of the implementation of the digital ID program	Objective: 40 million of digital IDs to be issued



1,353 BILLIONS OF INHABITANTS
98% ADOPTION RATE

AADHAAR

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM	AADHAAR NUMBER (12-digit) and biometrics	LIVE SINCE 2010

✓ IDENTIFICATION *online and offline*	✓ ID ATTRIBUTES SHARING *The e-KYC is paperless, consent-based and private, non-repudiable and instantaneous. As a result, accurate and reliable CDD (Customer Due Diligence) data is shared with the reporting entity in real time.*	✓ AUTHENTICATION *> Authentication is done using the number and biometrics (usually a fingerprint), with a POS (point-of-sale) device.* *> Banks and payment network operators have embedded Aadhaar authentication into micro-ATMs to provide branchless banking anywhere in the country in a real-time, scalable and interoperable manner.*	○ ELECTRONIC SIGNATURE *Based on an open API, a new eSign feature is intended to eliminate the need for "wet ink" signatures. Online requests for a digital signature would result in eKYC checks against the Aadhaar database and proof of address / identity verification from Aadhaar. Authentication would either be via biometric or one-time-password.*	○ CROSS-BORDER RECOGNITION **FRAMEWORK: THE AADHAAR ACT, ADOPTED IN 2016 (7 YEARS AFTER AADHAAR LAUNCH) BY THE LOWER HOUSE OF THE PARLIAMENT OF INDIA** PROVIDES A LEGAL AND REGULATORY FRAMEWORK FOR AADHAAR.

CONTEXT & OBJECTIVES

Aadhaar is the name given to the largest and unique state biometric-based program worldwide. It has been created for inclusion purposes by the Indian government to issue an identity to each citizen that enables them to access basic services, empowering them to become economic actors. Aadhaar reinforces social and financial inclusion and dignity: every citizens can claim their rights.
The program is managed by the UIDAI (Unique Identification Authority of India), an autonomous entity under the Ministry of Electronics and Information Technology.

VALUE PROPOSITION

Aadhaar is a system-based digital ID with no physical credential. After an enrollment based on biographic and biometrics data capture, UIDAI is mandated to issue an easily verifiable 12 digit random number as a Unique Identity (Aadhaar) to all residents of India. Each citizen receives a document containing their Aadhaar number, which can be cross-referenced with the biometric data held in the database.

Many online and offline services and transactions are now securely accessible and facilitated thanks to Aadhaar. For example, access to subsidized food through ration shops is now protected: the claims are authenticated thanks to Aadhaar with a remote digital ID system, rather than at the discretion of local officials. The scheme also helped in the fight against child labor and marriage, by providing proof of age.

BUSINESS MODEL

> Initially financed by government, enrolment and use is free of cost for citizens.
> Enrolling partners are hired by the government at a fixed cost of around half of 1$ US (to date, more than $US300M for the enrollment part paid by the governement) while UIDAI only provides the technical mandatory guidelines.
> To ensure rapid up-take by relying parties, UIDAI initially kept all authentication services free for all to lower the barrier to entry and only began charging relying parties in 2019. Since then, private organizations are charged US$0.007 for Aadhaar authentication and US$0.3 for e-KYC transactions. It remains free for government services.

SECURITY & PRIVACY CHOICES

> Data are encrypted and digitally signed: any changes make the digital signature invalid. Extensive use of PKI/HSM for encryption of data during transmission and storage and for protecting access to API.
> Only KYC data (demographic data and a photograph) are shared by UIDAI with user consent and no data is given during authentication process: only a YES or NO response on authentication request is given to service providers. The biometric data are never shared with anyone.
> Citizens can access their authentication history with time stamped and digitally signed logs of all transactions, can contest authentications and update their information online.
> No comprehensive data protection law or independent data protection authority. A Personal Data Protection bill has been under discussion for years.

PROJECT MILESTONES

2009	2015	2016	2018	2019	2020
Creation of UIDAI and launch of Aadhaar	UIDAI is attached to the Ministry of Electronics and Information technology (instead of Planning Commission)	Passage of the Aadhaar Act which provides a legal and regulatory framework.	339M of Aadhaar have been linked with bank accounts. 1.7BB authentication requests in 3 years.	+27B authentication requests. 1.2B Aadhaar numbers issued.	95% of adults have Aadhaar with a satisfaction rate of 92%.

1.9 MILLION INHABITANTS
40% ADOPTION RATE

EPARAKSTS

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

ePARAKSTS MOBILE (APP-BASED) + NATIONAL eID CARD & ePARAKSTS SMART CARD

LIVE SINCE 2018

✓ IDENTIFICATION *online*

✓ AUTHENTICATION

✓ ID ATTRIBUTES SHARING

eParaksts is able to provide specific user attributes available in the registery (e.g. age) to online service providers which need to ensure the presence of specific conditions to provide the service.

✓ ELECTRONIC SIGNATURE

✓ CROSS-BORDER RECOGNITION

+90 public and private SP integrated eParaksts services

EIDAS NOTIFIED SINCE 2019 FOR SEVERAL LEVELS OF ASSURANCE (INCLUDING HIGH) DEPENDING ON THE CHOSEN SOLUTION.

CONTEXT & OBJECTIVES

In order to promote the use of eGovernment and reduce administrative overhead generated by physical documents and services, the Latvian government launched its first eID card including e-signature in 2012. The eID card is currently optional but will become mandatory in 2023.

In 2018, the Latvia State Radio and Television Center (LVRTC), a national trust service provider launched eParaksts: Qualified Cloud Signing services enabling users to perform secure authentication and QeS from mobile devices, eliminating the need for physical smart card connectivity.

VALUE PROPOSITION

With eParaksts solutions, users can access both online governmental and private services. As the solution includes QeS, it is possible to send signed requests also for offline services, like certificates or other legal documents.

The eParaksts mobile application (working on iOS and Android smartphones) enables individuals to sign documents electronically, identify and authenticate on a variety of self-service portals for institutions and companies, including municipal services, house management, medical and insurance service providers.

Users can still use their eID card or eParaksts card to access online services and digitally sign documents but this use requires smart card readers as well as free computer software eParakstītājs.

eParaksts solutions have significantly reduced the necessity for onsite visits and customer services. It became a very important tool to maintain business and Parliament activity during the COVID-19 outbreak..

The eParaksts mobile enrollment process can be done remotely with an eID (or eParaksts card) or in person via courier for people who cannot use National ID or smartcards, based on a bank link authentication. To facilitate the access to eParaksts onboarding, the Latvian state sponsors the carrier services. In 2021, 116 state-appointed notaries will become Registration Authorities. Six months after the launch, notaries will charge customers a one-time fee to cover on-boarding service cost.

LVRTC also issues electronic seal certificates on cards or software for organisations. LVRTC facilitates the integration of its solutions for companies by organizing workshops to demonstrate available APIs to Systems Integrators. The API integration only takes few minutes.

A GOVERNMENT FUNDED BUSINESS MODEL

> Latvian government fully financed the Digital ID scheme.
> eID card and eParaksts solutions are free of charge for end users (except for onboarding fees via notaries from mid-2021).
> eParaksts is free of charge for private and public service providers, including ready made integrated API solutions (except for services which are outside of the National Identification Scheme, such as qSeals, website qAuthCert and NQC certificates).

SECURITY & PRIVACY CHOICES

> LoA High for National eID card, eParaksts smart card and eParaksts mobile app
> LoA Substantial for unsupported smartphone models
> qSeals, qWebsiteAuth certificates

PROJECT MILESTONES

2012	2018	2019	2020	2021	2023
Launch of the national eID card, including e-signature	Launch of eParaksts solutions Tax revenue service, state portal and 68 state e-services integrated eParaksts in March.	eIDAS notification for the national digital ID scheme	Upgrade of eParaksts to QeS level	Launch of a new app bringing more functionalities and better user experience	eID card becomes mandatory for all Latvian citizens

2,8 MILLION INHABITANTS
100% OF THE POPULATION IS EQUIPPED

OMANUNA

GOVERNMENT-DRIVEN CENTRALIZED SYSTEM

EID CARD + MOBILE ID (SIM-BASED)

LIVE SINCE 2014

✓ IDENTIFICATION *online and offline*

Offline identification only through eID card reading with match on card identification.

✓ ID ATTRIBUTES SHARING

61 accessible public and private service providers

✓ AUTHENTICATION

Two-factor authentication with a multi modal approach (eID card or mobile ID). Highest LoA as per US NIST standards and reaching e-IDAS High (EU).

✓ ELECTRONIC SIGNATURE

Qualified electronic Signature (QeS), reaching the highest level of digital signature with legally binding effects. Used by all actors (citizens, residents, businesses and civil servants).

○ CROSS-BORDER RECOGNITION

FRAMEWORK: LAW ON ELECTRONIC TRANSACTIONS (2008) ISSUED BY DECREE SET UP THE LEGAL FRAMEWORK OF THE DIGITAL ID SCHEME AND GIVE ESIGNATURE LEGAL RECOGNITION

CONTEXT & OBJECTIVES

To set up their national digital identity scheme, Oman ITA (Information & Technology Authority) was willing to leverage eID cards and e-Resident cards already in the field as well as benefit from Oman's high mobile phone penetration (189%) to launch a mobile ID companion to the card. Oman was the very first country in the Middle East to complement its national electronic ID card with a mobile ID scheme to bring more convenience. Everyone is equipped and the solution is fully inclusive, addressing any user's profile.

A total of 61 different entities have joined the successful scheme including banks, mobile operators, as well as public entities at all level ministries, municipalities and Chambers of Commerce to build a powerful centralised IT system. An agreement with mobile network operators has been signed to take charge of onboarding citizens to the national mobile ID.

Omanuna is a public driven initiative with the ambition of:
> Smoothing public services delivery
> Increasing efficiency and citizens satisfaction
> Improving Goverment-2-Consumer interactions
> Reducing operational costs by mutualizing the cost of online public services security and access management.

VALUE PROPOSITION

People and businesses in Oman can seamlessly access public and private online services, engage with public authorities through a friendly interface and sign legally binding forms without the need to physically go to admin desks, saving them time and efforts.

Public services delivery is optimized and users can securely log on to the Omanuna government portal using either their national eID card / eResident card with a smart card reader connected to a PC and a PIN code, or simply using their mobile ID app to authenticate and sign online.

The top eServices used by Omani citizens, residents and businesses are register a business, book medical appointments, private clearance, building permits, legal complaint registration, job seeker application, etc.

A GOVERNMENT FUNDED BUSINESS MODEL

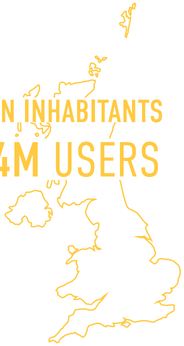
> Omani government fully financed the Digital ID Scheme to best support the digital transformation of the country.
> Free of charge for end users and for public service providers willing to leverage on it to secure their eServices.

SECURITY & PRIVACY CHOICES

> Oman opted for the highest level of security and reaches Identification Assurance Level 3 (IAL3) for onboarding as well as Authentication Assurance Level 3 (AAL3) for access as per NIST standards. B> ased on secure element (from a smart card or a SIM card), Oman digital ID schemes also reaches EU e-IDAS high.

PROJECT MILESTONES

2002	2003	2008	2009	2011	2014
National Registry centralized citizen's database	Deployment of eID cards	Law on electronic transactions	Launch of Omanuna government eServices Portal	Electronic voter authentication services added to the eID card	Launch of Digital ID scheme and IDP platform with eID card and Mobile ID to secure online interactions



66,65 MILLION INHABITANTS

7,4M USERS

GOV.UK VERIFY

GOVERNMENT-DRIVEN
(soon to be led by the private sector)

FEDERATED SCHEME **Credentials and authentication processes depend on the IDP:** 2 factor authentication with most IDPs, using the mobile phone

LIVE SINCE 2014

○ IDENTIFICATION

✓ ID ATTRIBUTES SHARING

✓ AUTHENTICATION

Authentication with an equivalent of level of security Low and Substantial (not eIDAS notified)

○ ELECTRONIC SIGNATURE

✓ CROSS-BORDER RECOGNITION

FRAMEWORK: **ELECTRONIC COMMUNICATION ACT (2000)** PROVIDED THE LEGAL FRAMEWORK FOR PRIVATE SECTOR IDENTITY PROVIDERS TO BE USED TO ACCESS DIGITAL PUBLIC SERVICES. **GENERAL DATA PROTECT REGULATION (2016)** UNDER WHICH THE INFORMATION COMMISSIONER'S OFFICE (ICO) ACTS AS AN INDEPENDENT DATA PROTECTION AUTHORITY.

22 **government accessible services**

The UK government is hoping to export its model to other countries through standardization. For example, core technical assets of the UK scheme have been given "open-source" to the Australia's Digital Transformation office, which aims at creating a similar ecosystem in Australia. UK on-going alignment to eIDAS as yet undefined in the context of Brexit. However, benefits of continued interoperability are clear.

CONTEXT & OBJECTIVES

The UK does not have a unique foundational identity database and people use a wide range of credentials to assert identity (driving licences, passports, birth certificates, bank statements, etc.).
In 2014, the UK government launched GOV.UK Verify, a digital identity scheme that would enable UK citizens and residents to authenticate themselves through their choice of Identity Provider when accessing public and private sector digital services.
The government's objective was to establish a private sector market of identity services certified as meeting government defined standards.

To date, over 7 million digital identities have been issued. It did not achieve the registration target. The British government launched a public consultation following which the number of identity provider has diminished. However, the COVID-19 outbreak caused a spike of applications for Universal Credit (low income or unemployment benefit) through Gov.UK Verify. The demand exceeded the platform capacity, forcing the government to put additional investment into the service and retain control of the platform for at least another 18 months.

End of 2020, the UK Government launched a pilot of the Document Checking Service through which identity details can be validated against the passport database.

VALUE PROPOSITION

To register and then authenticate themselves online, users can choose between different identity providers, each of them offering different enrollment processes to serve all types of users. They can then use their identity account to easily sign in to other services that use GOV.UK Verify.

BUSINESS MODEL: GOVERNMENT FUNDED

> Initially financed by the government
> Free to citizen.
> Public and private sector services pay for the assertions of identity
> Public services pay Government Digital Service (GDS) on use. GDS pays Identity Provider selected by the citizen.

SECURITY & PRIVACY CHOICES

> The system was designed to protect privacy, avoid "tracking" of behaviour and prevent prejudicial decisions about an identity based on the person's choice of Identity Provider.
> Identity Providers cannot see which Service Providers the identity data is being sent to and Service Providers are unable to see which Identity Provider assured the identity.
> Private sector Identity providers were given access to the Document Checking Service through which a "Yes/"No" validation of passport biographic data could be obtained. However, the result of this check was not allowed to be used in the private sector until the new Document Checking service pilot, launched by the Government at the end of 2020

PROJECT MILESTONES

2012	2014	2016	2020
Policy announced by Minister for the Cabinet Office	GOV.UK Verify is launched in Beta test	9 companies joined in the scheme as Identity Providers. Brexit vote	Document Checking Service Pilot project launched by the UK Government to enable the private sector to verify passport information details against the national database. The Digital ID program is currenty under redefinition.

ACKNOWLEDGMENT

This research was led jointly by Marie-Alice Manderscheid, Hélène Le Héricy and Corentin Marsily, under the direction of Yannick Ragonneau from onepoint, by Stéphanie de Labriolle (SIA) and Kristel Teyras, Market Owner Digital ID Wallet, Platform & Services (Thales). In addition, Vincent Rémon and Corina Fontaine from onepoint and Pavlina Navratilova (Idemia), Marie-Sophie Bellot (Idemia), Eric Piroux (Entrust), Fabian Bahr (Giesecke+Devrient), Olivier Dussutour (INGroupe), Michael Edwards (Veridos), Sebastian Zehetbauer (Youniqx), Andreas Zechmann (OSD) contributed to the analysis.

This independent SIA and onepoint initiative is based on SIA and onepoint's return of experience, official and documented analytical sources, as well as a cross analysis of 25 interviews with key international actors and country representatives.
We owe a debt of gratitude to:

Australia (Queensland)
Christopher J Goh, General Manager, Registration and Licencing Modernisation at Department of Transport and Main Roads of Queensland.
Austria
Herbert Leitold, Secretary-General Secure Information Technology Center
Azerbaijan
Jana Krimpe, Azerbaijan Public Private consortium representative and Co-Chair at Global Alliance for Mobile National Identities (GANMI)
Canada
Joni Brennan, President at Digital ID & Authentication Council of Canada (DIACC)
Sarah Kirk-Douglas, Vice President, Global Marketing & Communications, SecureKey Technologies Inc.
Andre Boysen, Chief Identity Officer, SecureKey Technologies Inc.
Colombia
Didier Alberto Chilito Velasco, Director Nacional de Identificación de la Registraduría Nacional del Estado Civil, Colombia
Sofía Romero Mondragón, Coordinadora del grupo jurídico.
Denmark
Charlotte Jacoby, Head of Office for Division for Infrastructure Development.
Estonia
Margus Arm, Deputy Director General, Estonian Information System Authority, Director of State Information System Branch.
France
Lionel Fouillen, Partnership Relations Manager, FranceConnect
Valérie Péneau, Director of the interministerial program France Identité Numérique.
Italy
Andrea Spallacci, Project Leader, Agenzia per l'Italia Digitale (AgID) - Servizio Accreditamento / Member of FESA, the Forum of European Supervisory Authorities for Electronic Signatures.
Latvia
Edmunds Belskis, Chairman of the Board, LVRTC.
Liechtenstein
Sylvan Fux, Head of Business Consulting Finance/Justice and E-Government.

The Netherlands
Michiel Van der Veen, Director Innovation & Development at the National Office for Identity Data, Ministry of the Interior and Kingdom Relations.
Nigeria
Aziz Aliyu, Head of the National Identity Management Commission (NIMC)
Olatunji Durodola, Senior Technical Consultant & Systems Integrator (NIMC)
Portugal
Andre Vasconcelos, eID Advisor to the Board of Directors, AMA (Administrative Modernization Agency)
Claudia Barroso, Head of International Relations Unit at AMA - Administrative Modernization Agency.
Singapore
Quek Sin Kwok, Senior Director, National Digital Identity Platform and Products GovTech Singapore.
USA (Arizona)
Eric Jorgensen, Motor Vehicle Division Director at Arizona Department of Transportation.
Vietnam
Lã Hoàng Trung, Head of the National Electronic Authentication Centre.

INTERNATIONAL ORGANIZATIONS

Council of Europe
Sophie Kwasny, Head of the Data Protection Unit of the Council of Europe.
Peter Kimpian, Data Protection Unit at Council of Europe.
eIDAS
GANMI
Jana Krimpe, Co-Chair at Global Alliance for Mobile National Identities (GANMI)
IIC, ID4Africa
Mory Camara, President of IIC (Identity Council), ID4Africa.
UNCITRAL
Eric A. Caprioli, Avocat à la Cour, Représentant France UNCITRAL/CNUDCI

SECURE IDENTITY ALLIANCE

onepoint.
beyond the obvious