VERIDOS
Identity Solutions
by Giesecke+Devrient
and Bundesdruckerei

WHITE PAPER

DATE: Oktober 22

eGovernment comes of age

Digital IDs are removing the barriers to public services for citizens, improving quality and efficency for providers

CONTENTS

1 Introduction – unlocking the potential of eGovernment

Today much of the world's population enjoys the benefits of an increasingly digital age. We shop online, pay for purchases with our watch and keep track of our steps with a fitness app. During the COVID-19 pandemic our mobile phones have even alerted us when we have recently been in close proximity with someone who has subsequently tested positive for the virus.

But for many official aspects of our lives we still rely on printed documents. That may include a passport that allows us to cross national borders, a license to show we are authorized to drive a vehicle or a certificate to prove our educational achievements to a potential employer. But this, too, is changing as eGovernment rapidly comes of age.

Broadly defined as the employment of the internet and the world-wide-web to deliver government information and services to the citizens, the availability of eGovernment services worldwide increased by 40% in just two years that elapsed between the 2018 and 2020 surveys. The UN's E-Government Development Index for 2020[1] shows 163 countries now offer at least one online transactional service, while the global average stands at 14 uses per country – a figure that is rising rapidly.

What exactly is eGovernment?

The United Nations defines eGovernment as: 'the use of ICTs (information and communications technologies) to more effectively and efficiently deliver government services to citizens and businesses. It is the application of ICT in government operations, achieving public ends by digital means. The underlying principle of eGovernment, supported by an effective e-governance institutional framework, is to improve the internal workings of the public sector by reducing financial costs and transaction times so as to better integrate work flows and processes and enable effective resource utilization across the various public sector agencies aiming for sustainable solutions.'

Registering a new business, applying for a business license, applying for a birth certificate and paying for public utilities are the most widely available services today. But as eGovernment becomes more widespread, the range of applications it can be used for is broadening, too, extending into such important areas as health and education as well as the provision of driving licenses and national identity cards.

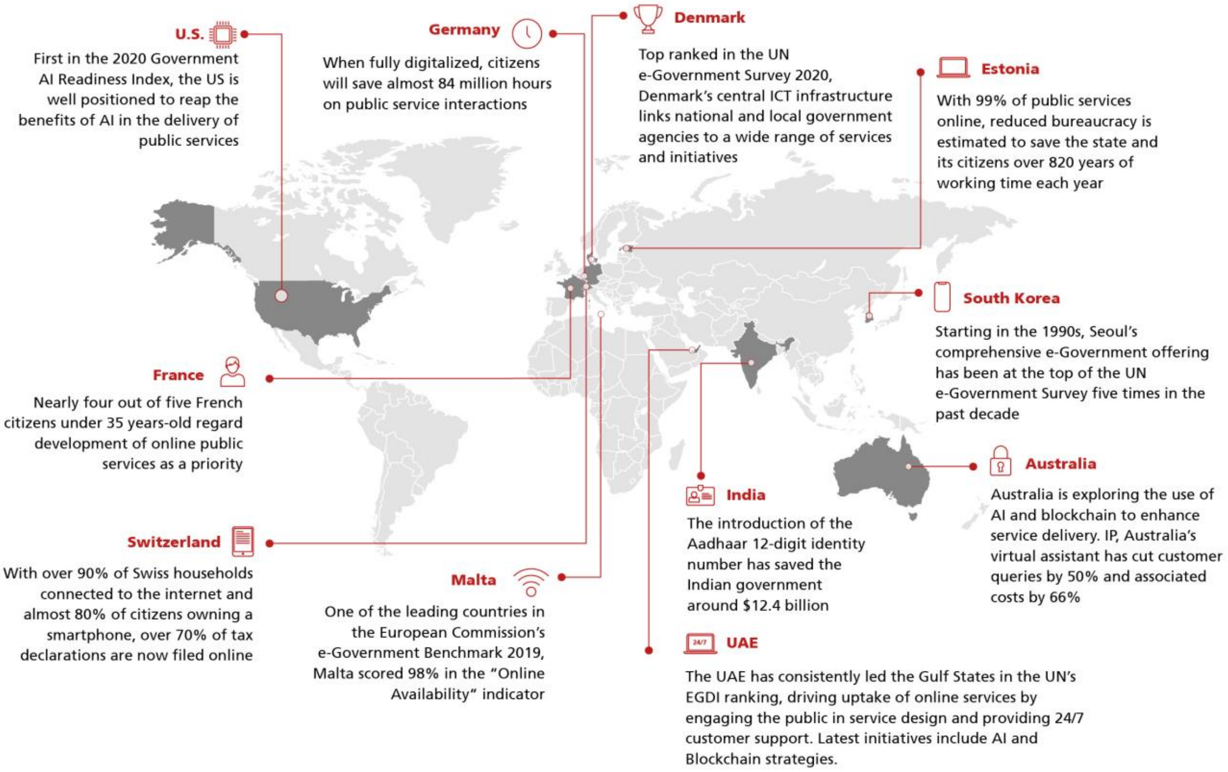
Furthermore, as the UN points out in its *2020 E-Government Survey*, the growing technological capacities allow policymakers to process ever-larger and more complex data sets, providing better insight and foresight and making e-services more efficient, accountable and inclusive. “Shifting from ‘gut instinct’ to data-centric policymaking is now a viable alternative and is rapidly moving towards becoming a strategic imperative,” it concludes. The COVID-19 pandemic has simply added further impetus to the strong momentum already evident in the development of eGovernment infrastructures worldwide.

Market figures reflect this trend. The market for digital ID solutions is now expected to grow at a rate of about 16% a year, to reach approximately US$33 billion by 2025. While this figure also includes private sector integrations, it still indicates the sheer scale of the demand for digital identities in the future.

The key objective for governments is to provide infrastructures for their citizens so they can securely access public – and maybe even private – services using a digital ID. While the challenges and baselines are the same the world over, the level of maturity of e-Government services in any given country is a key issue.

The pace of growth will vary quite significantly between individual countries, which is why service providers in this space need to ensure that their offerings address the key issues for each country as well as the existing level of maturity and planned development of its digital ID ecosystem.

Low ranking countries on the UN’s E-Government Development Index (EGDI) will require significantly different offerings to those near the top. Those countries lacking the basic infrastructure required for a digital ID ecosystem and eGovernment services will need end-to-end integration and turnkey solutions and consultative project management to help them transform their existing analogue processes into fully functioning digitalized eGovernment services – with realistic potential for the widespread adoption needed to deliver the benefits of cost-efficiency as well as user-convenience.



U.S.
First in the 2020 Government AI Readiness Index, the US is well positioned to reap the benefits of AI in the delivery of public services

Germany
When fully digitalized, citizens will save almost 84 million hours on public service interactions

Denmark
Top ranked in the UN e-Government Survey 2020, Denmark's central ICT infrastructure links national and local government agencies to a wide range of services and initiatives

Estonia
With 99% of public services online, reduced bureaucracy is estimated to save the state and its citizens over 820 years of working time each year

South Korea
Starting in the 1990s, Seoul's comprehensive e-Government offering has been at the top of the UN e-Government Survey five times in the past decade

France
Nearly four out of five French citizens under 35 years-old regard development of online public services as a priority

India
The introduction of the Aadhaar 12-digit identity number has saved the Indian government around $12.4 billion

Australia
Australia is exploring the use of AI and blockchain to enhance service delivery. IP, Australia's virtual assistant has cut customer queries by 50% and associated costs by 66%

Switzerland
With over 90% of Swiss households connected to the internet and almost 80% of citizens owning a smartphone, over 70% of tax declarations are now filed online

Malta
One of the leading countries in the European Commission's e-Government Benchmark 2019, Malta scored 98% in the "Online Availability" indicator

UAE
The UAE has consistently led the Gulf States in the UN's EGDI ranking, driving uptake of online services by engaging the public in service design and providing 24/7 customer support. Latest initiatives include AI and Blockchain strategies.

Which countries are leading the world in eGovernment?

The UN's 2020 E-Government Survey identifies that many more countries and municipalities are pursuing digital government strategies, and that some are radically different from those guiding earlier eGovernment initiatives. These new approaches include the delivery of eGovernment as a platform, integration of online and offline multichannel delivery, the development of digital services supported by whole-of-government and whole-of-society engagement and integration, the expansion of e-participation and partnerships, the adoption of data-centric approaches, the strengthening of digital capacities to deliver people-centric services and the innovative use of new technologies such as artificial intelligence (AI) and blockchain, especially in the development of smart cities.

2 The role of digital IDs in evolving eco-systems

The availability of digital IDs has been an essential element in this growth. While there are different forms of digital IDs, including centralized, federated and self-sovereign, and different types, which contain common structured features. A digital ID can be represented electronically, proving an individual's identity and therefore their right to access specific information or services online. It is important to note that digital IDs are much more than a digital image of an identity card, for example, on a smartphone. Also known as digital credentials, these are electronic documents that use a digital signature to bind a generated key pair with an identity and confirm that this key pair belongs to a specific individual. A digital ID is issued by a certification authority and signed with that authority's private key. The data contained will typically include the owner's public key and name, the expiry date, the name of the issuer and the serial number of the digital ID and the digital signature of the issuer.

> “ A digital identity …
> is a grouping of digital identifiers. So, if you interact with any technology connected to the Internet, or to a mobile network, you have a digital identity.” (ID2020)

Digital IDs also have the significant benefit of eliminating unsecure usernames and passwords and replacing them with secure, trustworthy authentication methods, thus enabling the provision of new trusted services.

The way in which such services are provided very much depends on the existing approaches already in place to administer and deliver them to citizens. Some are provided on platforms that can be readily adapted to facilitate an eGovernment online approach, while others may require a more tailored approach that allows either a complete transfer or provision of online access in parallel to the legacy approach.

All can be facilitated, but the key to success lies in careful consideration of the design of the approach to achieve the optimum solution, one delivering the greatest benefits to the service provider and the service users. The extension of services fully online, furthermore, may well require legal considerations to be taken into account and possibly new legislation at national level to ensure the acceptability of digital IDs and of digital signatures.

However, while eGovernment has achieved significant momentum in recent years, the variations in the pace of citizen adoption demonstrates the overarching need for solutions to be developed which meet real needs, conveniently and effectively, and that command the trust of issuers, users and other stakeholders.

Success stories include Estonia, for example, whose eID system facilitates authentication, data storage and sharing and digital signature through chip-based card or mobile enabled digital keys. Launched in 1997, Estonia's eGovernment project now makes 99% of public services available to citizens as e-services. During the past 15 years over 400 million digital signatures have been given in Estonia – more than in all the other EU member states combined, and the country is now estimated to save over 1,400 years of working time and 2% of GDP annually through its digitized public services.[2]

At the other end of the scale, Nigeria's national eID, which was launched by the public sector in 2014 in partnership with Mastercard, had a very slow rate of adoption in its early years, something now being addressed with the help of the World Bank, Agence Francaise de Development and the EU.

The United Nations E-Government Development Index (EGDI), which is published every two years, gives a broad indication of the levels of maturity of the eGovernment infrastructures in the 193 UN member states and the progress achieved compared to previous surveys.

Comparing the 2018-20 and 2016-18 survey results indicates there has been a slackening in growth momentum, with the average growth for all countries surveyed declining from 16% a year in the former to 11% in the latter. A substantial factor in this, however, is that there was a surge in the performances of many African countries in the 2016-18 survey. Coming from a base of close to zero activity, the top 10 growth countries in that region recorded growth rates above 50%. But between 2018 and 2020, African and Asian countries continued to increase their index performance, albeit at a slower rate. The most notable improvements were recorded by the Ivory Coast and Lesotho, while in Europe Cyprus outpaced the growth rates of most already highly developed eGovernment countries, such as France and Germany.

Looking ahead, it is likely that many less developed countries, especially in Africa and Asia, will continue to mature their eGovernment capabilities, both in terms of the underlying enabling digital infrastructures and the range of services provided. This growth potential will be supported by further development of their ICT infrastructures and, in particular, the increased use of smartphones in these regions. Thus, the conditions required for widespread adoption of eGovernment services using a digital ID are rapidly improving.

The pace of that growth will vary quite significantly between individual countries, however. Service providers in this space therefore need to ensure that their offerings address the key requirements of each country as well as the existing level of maturity and planned development of its digital ID ecosystem.

Countries with a low ranking on UN's EGDI will require significantly different offerings to those with a high score. Those lacking the basic infrastructure required for a digital ID ecosystem and eGovernment services will need end-to-end integration, turnkey solutions and consultative project management to help them transform their existing analogue processes into fully functioning digitized eGovernment services – with realistic potential for the widespread adoption needed to deliver the benefits of cost-efficiency as well as user convenience.

More digitally mature countries face different issues. Having already established strong infrastructures and wide-ranging services, the focus for these countries is largely on enhancing the experience for their citizens. They are keen to identify solutions and components to optimize their infrastructures in such areas as analytics or enhanced security, for example. Here the challenge for service providers is to work closely with governments, identifying opportunities to supplement or replace components in their already well-developed digital architectures to deliver these benefits, thus optimizing performance and security.

> “Countries lacking the basic infrastructure required for a digital ID ecosystem and eGovernment services will need end-to-end integration, turn-key solutions, and consultative project management.
>
> More digitally mature countries must focus on enhancing the experience for their citizens.

But whether working with countries at the start of their eGovernment journeys or ones already well advanced, consultation is at the core of the relationship. The specific solutions may differ significantly but many new technologies are becoming readily available that all governments can benefit from when thinking about building flexible and scalable ID ecosystems. Not only will they be future-proof for a world with an exponentially growing number of identities, they will also amplify their users' experiences, giving them ever-greater control of their own identities. Self-Sovereign ID, (discussed later) which can be enabled through Decentralized ID infrastructures, is one of the most exciting innovations in this field currently.

3 mGov brings everything a step further

Advances in technologies and infrastructures have played an important role in the rapid growth in eGovernment services around the world. ICT infrastructures have become more reliable and improvements in digital security have increased the level of trust between service providers and their users. Tablets and smart phones, too, have become widely available and affordable, leading to an important subcategory of eGovernment, known as mobile government or mGov, which enables citizens to use mobile apps and mobile websites to interact with a range of services.

Progress in secure mobile ID technologies, furthermore, is one of the most important factors in this new wave of expansion in eGovernment services, with digital IDs and Derived Credentials helping to unlock the true potential of mGov. Reductions in administration costs are attractive to governments, while savings in time and convenience are major benefits to citizens. In the new mGov era official services can be conveniently accessed anytime, from anywhere and with an unprecedented level of security.

Mobile Government (mGov) enables citizens to use mobile apps and mobile websites to interact with a range of services.

For service providers, furthermore, the use of mobile IDs brings improvements in service quality as well as big savings in time and administrative costs. More than this, governments around the world are discovering that they can use digital technologies to transform the way they operate, share information, make decisions and even engage and partner with citizens to solve policy challenges of public concern. The COVID-19 pandemic, for example, has focused the minds of governments as never before on how they can use ICT to promote health and safety and keep their economies and societies working.

It is the ubiquity of the mobile phone, therefore, which is currently proving to be one of the single most significant drivers of eGovernment services, with the increased support for secure mobile access directly tied to the near universal adoption of mobile devices.

Adoption of mobile devices worldwide by adults

93%	High-income economies
79%	Developing economies

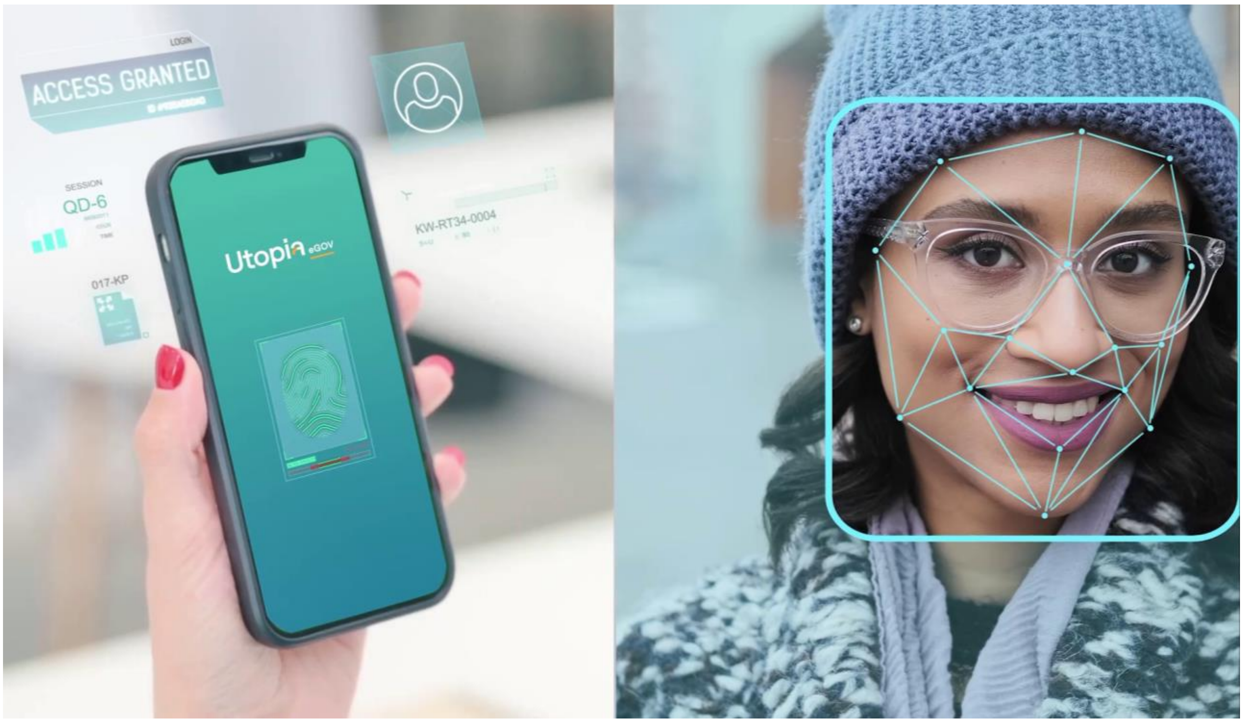
The widespread availability of affordable smartphones capable of running mobile apps and performing payment transactions has also occurred alongside a significant shift away from conventional desktop and laptops. Citizens are switching more and more of their online activities onto their smartphones and tablets, relegating their PCs and even laptops to the work environment. At the same time, however, there are still many citizens who do not own a smartphone or who live in more remote areas and may have limited or poor quality access to the internet – or even no access at all. These citizens cannot be excluded from access to government services. The availability of strong root credentials, for example those used to underpin the issuance of physical identity cards, is therefore an important consideration in ensuring equality of access for all citizens.

The rise of digital currency has been another big influence on the growth of mobile devices. For example, in an effort to reduce money laundering and cash hoarding in the world's second most populated country, India launched a demonetization drive in November 2016 which has led to a sharp increase in demand for smartphones and a boost in the demand for mobile wallet applications.

Many smartphones now come equipped with advanced encrypted authenticators as standard, while digital technology–based biometric identification cards have also provided another way of lowering barriers to bank account ownership. In India, where 90% of people without a bank account also lacked proof of identity issued by the national government, the provision of the Aadhaar national biometric ID cards has been a significant factor in the rapid decline in the number of unbanked adults.[4]

Elsewhere across the world mobile apps have made financial services increasingly available to the unbanked and under-banked. The World Bank's Global Findex, which tracks financial inclusion, shows that mobile banking is helping historically unbanked regions, especially in sub-Saharan Africa, gain financial access.

With a growing proportion of citizens, therefore, now using mobile devices to access information, make purchases and conduct other forms of business, many governments at national, state and local levels have started adopting the approach of "think mobile first" and are according mGov priority in the development of their strategies. mGov presents major opportunities for developing countries, in particular, to leapfrog what have already become legacy technology issues for some early eGovernment adopters. For example, many proprietary systems have limited flexibility in terms of integration with partners and even between different public sector ID issuers within a single country.



The use of mobile IDs brings improvements to service providers in service quality as well as substantial savings in time and administrative costs.

4 Setting standards as a way of winning trust

Trust and security remain the highest priority in any development involving mobile technology, whether or not it is to be integrated into an existing back-end platform or created as a standalone app. That includes protection of every mobile-based transaction and ensuring the privacy of every piece of personal information used.

International standards and certification are a vital component underpinning trust and security, both in eGovernment in general and mGov in particular. Governments across the world rely on standards to provide, at a minimum, the broader parameters within which they can develop their own more specific national standards.

Interoperability between identification systems with sufficient coverage and robustness can also create the opportunity to reduce or eliminate redundant aspects of the identity ecosystem. This can include avoiding duplicate data collection and eliminating obsolete databases or credentials. Moreover, a high level of interoperability helps to reduce operating costs within a State's identity ecosystem and may generate administrative savings.

There has been significant progress over recent years in the setting of relevant standards internationally. In the US, for example, the National Institute of Standards and Technology has created standards for Personal Identity Verification derived credentials and issued federal guidelines for electronic authentication.

In Europe for the past five years the EU's eIDAS regulation on electronic identification and trust services for electronic transactions[5] has ensured that people and businesses can use their own national electronic identification schemes to access public services available online in other EU countries. It has also created a European internal market for trust services by ensuring that electronic signatures, electronic seals, time stamps, electronic delivery service and website authentication work across borders and have the same legal status as their traditional paper based equivalents.

Why interoperable?

- ✓ Reduce or eliminate redundancies
- ✓ Reduce operating costs
- ✓ Ensure easier adoption

FIDO Alliance: An open industry association with a focused mission of setting authentication and device attestation standards to help reduce the world's over-reliance on passwords.[6]

eIDAS: An EU Regulation that seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

Arguably one of the most significant developments in the area of standardization is the recent arrival of the ISO 18013-5 compliant mobile driving license, intended to ensure global interoperability while at the same time supporting data privacy and combatting fraud. As a secure and trusted verifier of ID this also facilitates multiple use, providing ways in which verifiers other than the mDL issuing authorities, such as police, government services or building access systems, can ensure that the data of the mDL holder is authentic and therefore trustworthy.

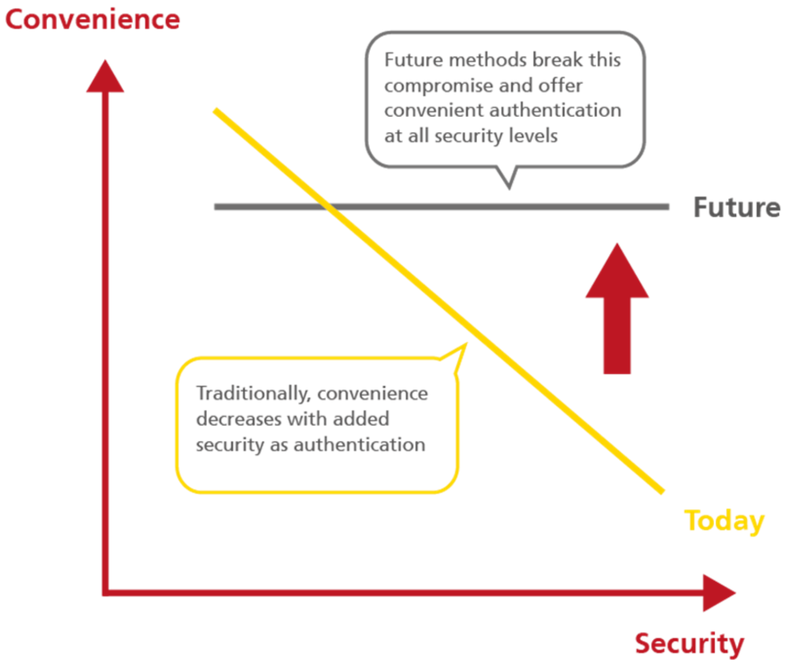
The ISO/IEC 29115 (Entity Authentication Assurance Framework), which provides a framework for managing user authentication guarantees, has established four levels of assurance for entities, stipulating the criteria and providing guidelines for each of the defined levels.

Work on setting the international standards that will unlock the potential of the next wave of mGov, covering such topics as mobile documents, mobile virtual documents and national mobile IDs, is only really commencing now. However, progress on these is likely to be rapid, driven by considerable enthusiasm amongst governments, international agencies and service providers for the benefits expected to result.

A list of the most important regulatory requirements related to the implementation of eGovernment is provided in Appendix 1.

5 Achieving a balance between security and convenience

Citizens are only likely to adopt services that can be shown to be both trustworthy and convenient. High levels of assurance can be achieved but each additional step makes the process more cumbersome and expensive – and potentially less convenient. So governments and their agencies need to achieve a balance between security requirements and ease of use, ideally determined by the specific use case requirements. Identity is not just a matter of authentication, it also encompasses individual attributes and personal information and the level of security needs to reflect the differing levels of trust required. A straightforward evidence of someone's age, for example, may be considered significantly less sensitive by an individual than access to their detailed medical records.


Convenience
Future methods break this compromise and offer convenient authentication at all security levels
Future
Traditionally, convenience decreases with added security as authentication
Today
Security

Balancing convenience and security in authentication processes

Conventionally, access to online services using a fixed login is protected by a combination of a username and password. As additional security many eGovernment services add a third item as part of the process – for example, a government-issued electronic ID (eID). For this purpose the eID will typically be built into another officially produced type of identification, such as a national ID, a driver's license or a registered voter card. The login eID uses microprocessor-based smartcard technology to store and protect personal information, making it a more secure way to authenticate the user's identity before granting access to the online service and releasing attributes/personal information, which may be required by some services.

Because the information stored within the eID is protected from copying or tampering and the authentication process uses cryptography, using an eID as part of a fixed login process makes it much harder for it to be compromised by scamming or identity theft. The addition of a PIN code and/or biometrics, furthermore, can make the authentication process even stronger and help prevent unauthorized use if the electronic ID is lost or stolen.

On the other hand, using a smartcard-based eID for a fixed login process may also make the login more cumbersome if special software and hardware, such as a card reader, is required. The use of additional protections, such as a fingerprint or facial biometric, may also require additional equipment.

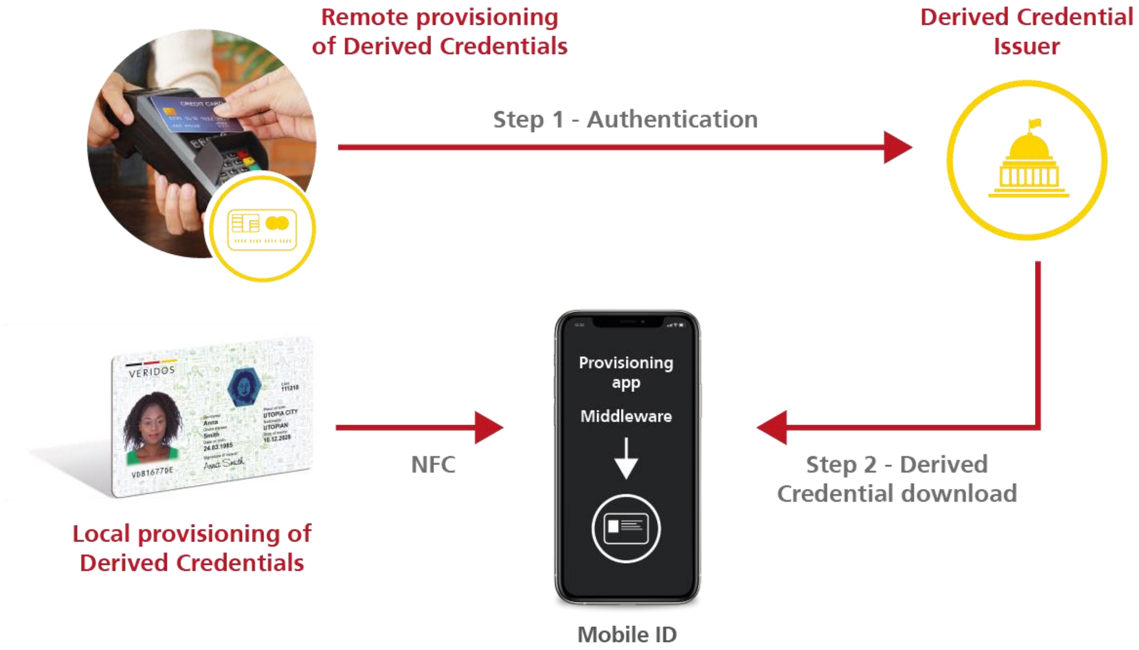
5.1 Derived credentials – same security level, no additional hardware

One successful solution, eliminating the need for additional equipment or software and delivering the same high level of security, is a derived credential, with the information needed for secure online access stored on the mobile device.

Starting with a genuine, verified eID, the derived credential uses the information associated with that verified electronic ID to generate a credential that can be securely stored on the citizen's portable device. Once it is within the device the derived credential supports mobile access much as an eID does for fixed access, following the smartcard standards for cryptography and the other security mechanisms that create a strong authentication – but without needing any dedicated hardware or software components.

A derived credential is an alternative token of a trusted (root) identity token, to create strong authentication using alternative devices such as smart phones, tablets or other wearables.

Many governments have found that the best starting point for this approach is by way of proven, verified eIDs associated with smartcards, which are governed by national or internationally recognized standards. Over many years and trillions of authentications, smartcard eIDs have proved to be a highly trusted means of personal identification. The digital credentials derived from them can enjoy the same high level of trust, which is why chip cards in this context are also referred to as the "Root of Trust". Because their validity follows an identity proofing by government, chip cards enable digital credentials to be derived with no requirement for any additional verifications.



Process of deriving credentials for onboarding mobile IDs

Embedded secure elements (eSEs) and embedded SIM cards (eSIMs) used to support derived credentials also play an important role in the widespread acceptability of derived credentials because they are compatible with existing contactless smartcard infrastructures. This means they can be authenticated using existing methods, where required, while the built-in compatibility with the existing infrastructure assists in deployment and can reduce the cost of ownership. This, in turn, means that the mobile device can quickly become an extension of existing smartcard eID programs that already support such things as user authentication, signing and decrypting email, physical building access or in-store and internet payments.

Derived credentials are an excellent complement to card-based eIDs.

This high level of security also means that a derived credential can serve as a single sign-on (SSO) to provide access to a number of different services, including those required for strictly regulated environments or services. At the same time, the format is sufficiently versatile and easy to implement and use that mGov applications so supported can encompass a varied set of services, maintaining the varying levels of security required for each of them.

Derived credentials, therefore, are an excellent complement to, rather than replacement of a tangible, card-based eID, with benefits for both citizens and governments. They are also of great assistance to governments seeking to achieve the United Nations Sustainable Development Goals[7] regarding legal identity and access to economic and social opportunity.

The goal set by the UN in 2015 was that the 20 per cent of the world's population without legal identity, some 1.8 billion people, would be provided with such identities, including birth registration, by 2030. This effort to provide individual identity as a right for everyone will also facilitate the adoption of eGovernment services everywhere. Much progress has been made since then and the World Bank puts the number of people without a legal identity at one billion[8].

More recently the management of credentials in the cloud is also helping to accelerate the acceptance of derived credentials, with the higher levels of processing power available to run authentication checks facilitating the use of AI. Veridos' national ID solutions, for example, use a cloud-based enrolment system, IMAGO, which matches facial images and other biometrics to form the basis for trust anchors for issuing new documents. The cloud is open to all kinds of architectures and solutions.

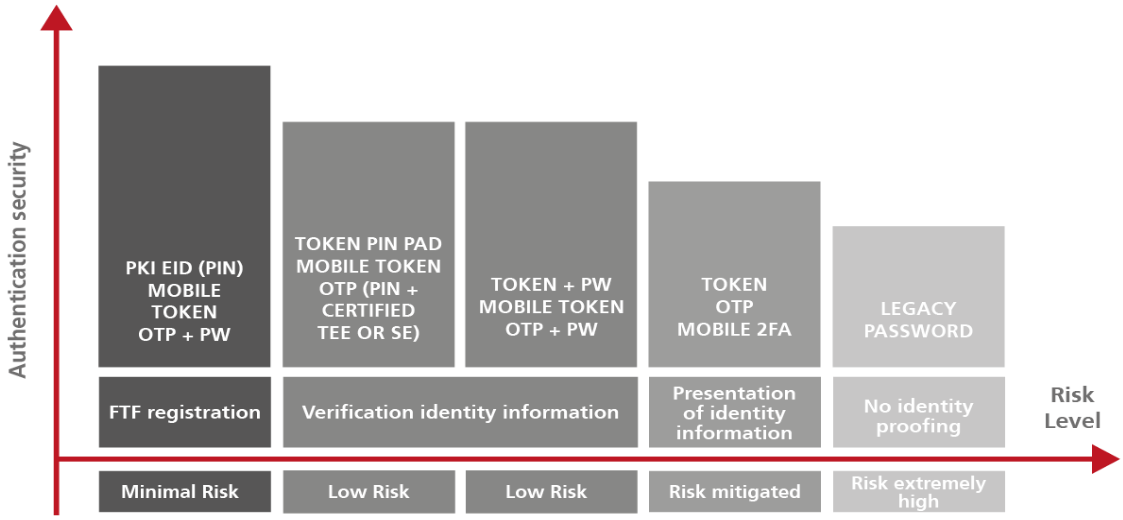
Translating the eID into the mobile environment with a derived credential creates new levels of convenience, ease of use and freedom while achieving mobile security and is therefore increasingly seen by many as the best way forward in implementing mGov. However, there are a number of issues to be taken into consideration when adopting this approach. For some countries, especially those which do not yet have a physical national ID card, a progressive approach which commences with chip cards to establish root credentials may well be the best way forward in their development of eGovernment and mGov solutions.

5.2 Primary credentials

The physical documents used to generate eIDs and to derive credentials from them – the "root credentials" – are at the heart of translating the eID into the mobile environment in a convenient, citizen-friendly way. Typically the root credential will be a primary one, such as a birth certificate or national eID card, which is only issued by way of a well-established process of identity proofing.

Using a primary credential as the source of the derived ID, the "root ID" is then held in a secure document. Additional electronic IDs can be derived from and even chained with this root eID and can be generated for various end-user devices to be stored either within the device itself or remotely in the cloud. Support for a broad range of devices helps maximize mobility for the most people and adds convenience with inherent compatibility across devices.

When granting access to any government service the level of assurance – that a credential is neither fraudulent nor stolen and that the person attempting to use it is the person to whom it was issued – needs to meet the requirements of a given use case. These requirements usually reflect the balance between security, convenience and cost. They could range, for example, from a high risk Level 1 legacy password only, up to a minimal risk Level 4 employing a public key infrastructure (PKI) eID PIN and two passwords, including a mobile token one-time-password.


Authentication security
PKI EID (PIN) MOBILE TOKEN OTP + PW
TOKEN PIN PAD MOBILE TOKEN OTP (PIN + CERTIFIED TEE OR SE)
TOKEN + PW MOBILE TOKEN OTP + PW
TOKEN OTP MOBILE 2FA
LEGACY PASSWORD
FTF registration
Verification identity information
Presentation of identity information
No identity proofing
Risk Level
Minimal Risk
Low Risk
Low Risk
Risk mitigated
Risk extremely high

Service offering based on level of assurance (LoA)

Issuing a single ID that encompasses every application, a well-designed credential management process makes it possible for governments, as well as private organizations, to create a single entry point for multiple services. This approach to identity management overcomes limitations inherent in traditional efforts to accommodate multiple services using a single eID card, which usually requires the alignment and agreement of stakeholders on a smartcard card design and profile. A single ID, however, can be securely linked to multiple applications and allows the addition of new use cases over time, so that the cost of ownership goes down as the number of service options rise.

The derived credential thus brings further convenience to multiple usages in the mobile environment. For example, a health authority might accept a national ID or driver's license to grant access to its services if it trusts the issuer and may choose to link its own health card credentials to those of the driving license or national ID.

> Governments should invest in issuing a unique lean ID to encompass every application. This will reduce the cost of ownership while the number of service options rise.

Most importantly, using derived credentials in mobile devices helps to eliminate the traditional trade-off between security and convenience because the next-generation ID methods currently in development are context-aware and therefore secure yet easy to use in the mobile format.

This context awareness may encompass a wide range of factors – such as the identity of the user, the purpose of the connection, the time of day or the location of the applicant at that time. With context awareness, for example, the authentication process might use one set of requirements if an access request comes from a network within a government office during normal working hours and a different set if it comes via public Wi-Fi in the early hours of the morning.

Where higher levels of authentication are desirable the methods used may depend on the capabilities of the mobile device. Many smartphones already offer biometrics, such as fingerprint, facial or voice recognition, for example. But where these are not available or are not acceptable, alternatives such as a PIN number, a Transaction Authentication Number (TAN), dedicated biometric ABIS systems, or a password can be used as the basis for authentication, as well as combinations – multi-factor-authentication – of authenticators can be used.

With the rapid pace of change now in evidence in the evolution of mGov, there is a growing awareness amongst governments of the significant advantages afforded by the adoption of open platform mobile ID solutions. These make it much easier to develop localized solutions than proprietary ones, with better support available from local system integrators and improved affordability. Localized solutions also enable local partners to quickly tailor mobile life cycle workflows and configure services.

Furthermore, open platforms open the door to innovative flexible private sector cost/revenue sharing models, making state-of-the-art ID programs ever more affordable and facilitating the continued integration of best-in-class technologies over time.

6 Privacy and trusted technologies

Veridos and its sister companies are engaged in innovation in many of the key areas of opportunity within the eGovernment and mGov sectors. Privacy and trusted technologies are critical areas of development for the company. While PKI encryption, for example, is highly standardized, work is underway on the development of secure but convenient apps and secure mobile credentials, including enhanced shielding technologies to protect applications and credentials on a mobile device.

To gain a high level of trust amongst both users and service provider the ways data is collected and stored must ensure adequate measures to safeguard the privacy of users while guaranteeing appropriate levels of trust for the information exchanged. The resulting benefits may be far more than strictly economic. A trusted identification system, for example, could give citizens confidence in a growing digital society, using new ways of communicationand of engaging with an ever-growing range of public and private services.

One of the key tools now regarded as an essential aspect of this is the development of applications that protect themselves against static and dynamic attacks through a process of active application hardening. This approach typically uses binary level code obfuscation to prevent attackers from seeing a functional view of an application and uses integrity checks to ensure the application code has not been altered. This active approach changes how protections are applied to prevent attackers from gaining an understanding of exactly how the apps are being protected and utilizes cryptographic protection. Designing and developing applications according to these principles also helps to establish real-life implementations of trusted eGovernment solutions that could be based on, for example, Self-Sovereign Identity infrastructures.

6.1 What lies ahead for eGovernment?

6.1.1 Self-Sovereign ID (SSI)

Decentralization has been ongoing in many developed democracies where citizens demand privacy and self-sovereignty. This will result in the introduction of more innovation in systems and technologies that put the citizen at the center of the release of any information about themselves, bringing proof and verification processes into the digital world – for example, by giving citizens full control over what data can be shared and with whom. The challenge is to develop ways of integrating and establishing these new technologies and methodologies into a multitude of established IT infrastructures and processes.

A number of government-funded projects are underway across the world to create prototyping in Self-Sovereign Identity (SSI)[10] and Decentralized Identifier Systems (DID)[11]. Applications involving SSI, such as enabled wallets and mobile ID, for example, are currently being piloted in Europe. Technologies like machine learning and deep learning are playing more important roles in making it possible for identities to be accurately processed, verified and authenticated at scale. In fact these types of technologies may be key to enabling security become an integral part of convenience.

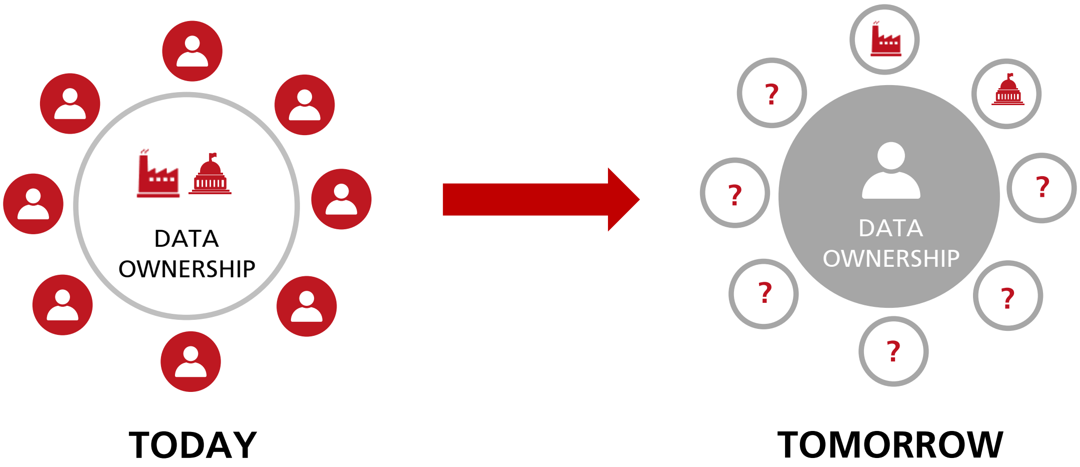
Today, as the industry moves towards "single sign-on," the creation of centralized, company-issued identities allows people to use a single identity to log into multiple otherwise unconnected systems and platforms. People have become used to using their Facebook, Google, LinkedIn or Twitter accounts to log in to a variety of apps, websites, comment platforms etc.

In order for companies to monetize this functionality, they have created business models that collect and sell user data. Data collection has become more complex, and therefore more valuable, as different systems and platforms link and correlate user data. This has allowed these companies to create detailed profiles to distribute targeted advertising. Digital identities, therefore, are currently traded for revenue by private companies and technology giants.

But by developing and issuing a Digital ID that not only enables eGovernment services but also integrates private services and physical use cases, governments can send an important signal to the world about their role in providing a useful digital ID to their citizens. Combining the private and public sectors can create a holistic model that fundamentally changes the way citizens use digital IDs.

6.1.2 Self-Sovereign ID (SSI) – giving control of identity and data back to the individual

The SSI and DID revolution is not just confined to individuals. The advent of the IoT (Internet of Things), for example, which is based on the unique identification of devices, requires a dramatic increase in identities of all forms. Against this background, the flexibility and scalability of systems is becoming increasingly important. Furthermore, the interoperability between individual identity systems will play a key role in the future when it comes to user-friendliness and convenience in ID ecosystems.



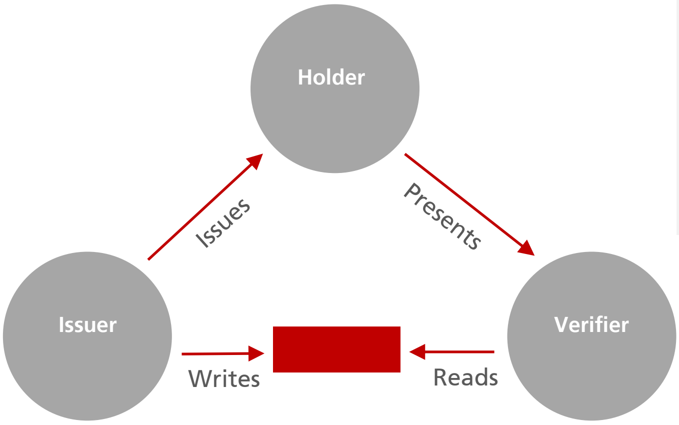
- End consumer registered in several public/private databases
- Companies manage respective ID with only limited control by the end consumer

- End consumer in control of data usage
- Managing variety of identities in digital age

Many countries around the world recognize the need for such systems and are actively looking for solutions based on state-of-the-art technologies in this area. Thanks to technological advancements in the field of decentralized data storage, in particular, the concept of Self-Sovereign Identities (SSI) now offers a way to implement a flexible and efficient identity ecosystem using the highest encryption mechanisms available.

6.2 Understanding Decentralized Identities – Triangle of Trust. How to create trust even when there is no connection to the issuer?

Due to their flexibility and scalability, decentralized identity ecosystems are seen as a key driver for the further development of the "Internet of Things" in particular. In the future, decentralized ecosystems like SSI may be the solution to handle large volumes of authentication processes and interactions between people, institutions, things or robots. A sustainable solution today must therefore be able to handle SSI in the future in order to exploit the full potential of this technology.



- Verification independent from Issuer connectivity
- Reduced complexity for systems and API's allows for system decoupling
- Allows for the exponential growth of Identity

The triangle of trust

Self-Sovereign Identity can therefore be seen as a disruptive innovation with the potential to solve future issues of flexibility and scalability in the context of digital ID ecosystems. While further innovation in this area will primarily be driven by new startups, it is likely that governments will increasingly be willing to embark on pilot projects, including proof-of-concept implementations. In Germany, for example, the Government of North-Rhine Westphalia is using decentralized ID technology to grant journalists physical access to high-security areas. In Zug, Switzerland, it is being used to unlock shared city bikes while in Sierra Leone individuals can securely share their credit scores with financial institutions. Most recently, health authorities in both Spain's autonomous Basque Country and the UK have used decentralized ID in the issuance and validation of COVID-Clearance certificates and vaccination passports. Elsewhere, governments already satisfied as to viability are evaluating broader applications of SSI

SSI is a form of digital identity on decentralized networks that allows individuals to assert their own identity. Personal data can be securely shared and credentials can be requested and confirmed by governments, businesses or educational institutions. It is based on a set of standards and protocols that can use technologies such as blockchain to store immutable records or make privately stored data available only to those with current credentials. Data permissions can be verified, denied or revoked. Individual identities can be verified and anonymized at the same time.

solutions. The government of Ontario, Canada, for example, having assessed the possibility of introducing a digital ID based on SSI, is now exploring the potential involvement of the private sector, along with funding models to establish the infrastructure.

During these various discussions and implementations, governments are supported by a growing landscape of market players – mostly startups. But the functionality spans a wide range of verticals, from public services such as government, healthcare and universities, to private sector commercial services and financial institutions. Most use cases revolve around passwordless authentication and the issuance/validation of portable credentials.

The SSI marketplace is still in a state of evolution. Most of the focus is currently on the provision of infrastructure on which SSI applications can run. Apart from proprietary implementations, ledger protocols are already consolidating, with companies providing protocol-specific or protocol-agnostic solutions. Hyperledger and Sovrin have emerged as two leading protocols. While some big players such as IBM and Accenture have focused on implementations for Hyperlegders, others, including Microsoft, are developing agnostic solutions for both protocols.

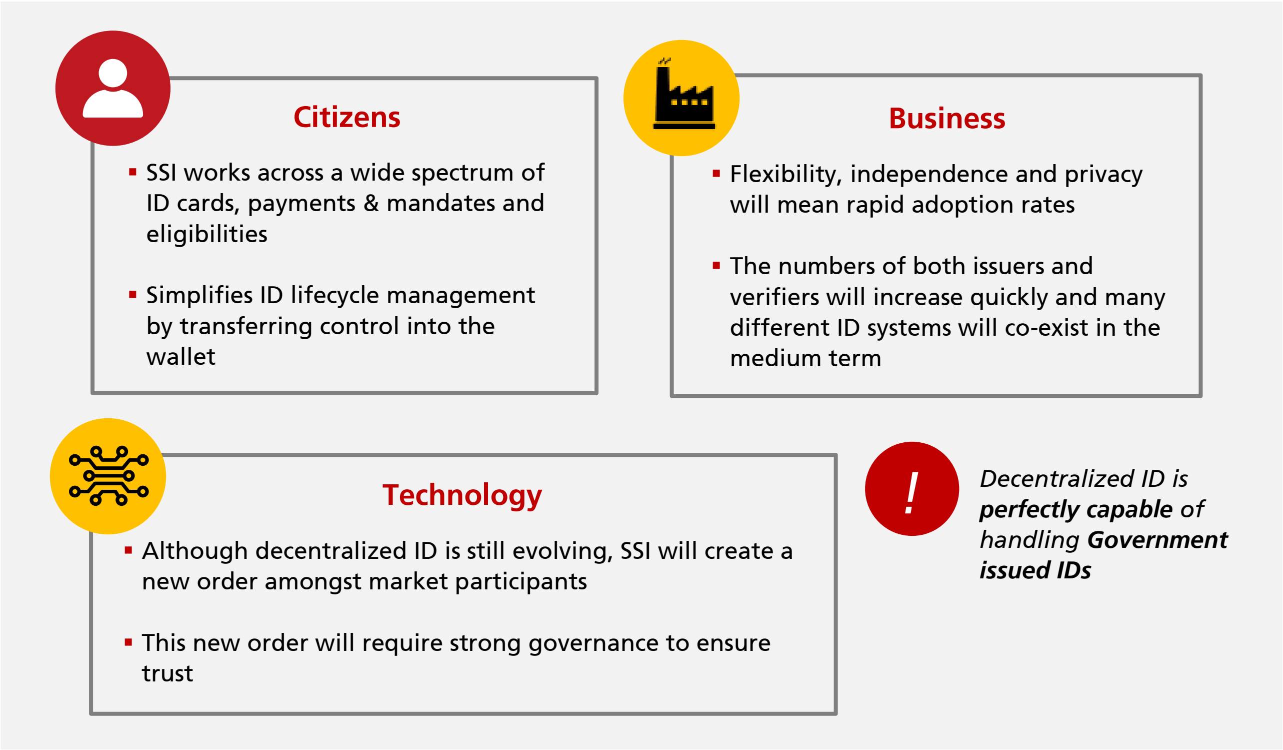
Some integrations are already moving past the proof-of concept stage. However, the three-sided market structure (holder/issuer/verifier) is slowing down adoption for large-scale implementations, which is why most integrations are currently in closed markets.

SSI radically expands the existing spectrum of digital identity technologies and meets the requirements of the GDPR as well as eIDAS (Regulation on Electronic Identification and Electronic Trust Services). It is taken into account in the upcoming ISO eID standard (ISO/IEC 23220). But it is not a stand alone "silver bullet". It requires the establishment of a new ecosystem with new standards and protocols and some significant issues are still the subject of debate.

The issue of "zero trust" has not yet been finally clarified, for example, and the question of how an identity is initially verified before entering the decentralized system is a major topic in current discussions on implementation. There are also many options with respect to future governance and delegation of roles within such a system, each offering benefits – but also drawbacks – compared to others. Until these important aspects around SSI have been clarified the technology will be mostly confined to pilot and proof-of-concept projects. But when they have been resolved SSI can be expected to be the basis for digital ID ecosystems for years to come.

In summary, therefore, while Decentralized ID is still in a relatively early stage of its evolution it is already clear that SSI has the potential to significantly redefine the roles of the current market players. Enabling all kinds of ID cards, eligibilities, payments and mandates, SSI shifts a big part of the ID lifecycle management and controls to the wallet.

Due to its advantages of flexibility, independence and privacy, a rapid rate of market adoption is to be expected, with the number of independent issuers and verifiers growing quickly. In the medium-term, therefore, it is likely that a number of different systems will co-exist. However, while decentralized ID is perfectly capable of handling government issued IDs, governance will be required to evaluate the trust levels of independent issuers.



Citizens

- SSI works across a wide spectrum of ID cards, payments & mandates and eligibilities
- Simplifies ID lifecycle management by transferring control into the wallet

Business

- Flexibility, independence and privacy will mean rapid adoption rates
- The numbers of both issuers and verifiers will increase quickly and many different ID systems will co-exist in the medium term

Technology

- Although decentralized ID is still evolving, SSI will create a new order amongst market participants
- This new order will require strong governance to ensure trust

*Decentralized ID is **perfectly capable** of handling **Government issued IDs***

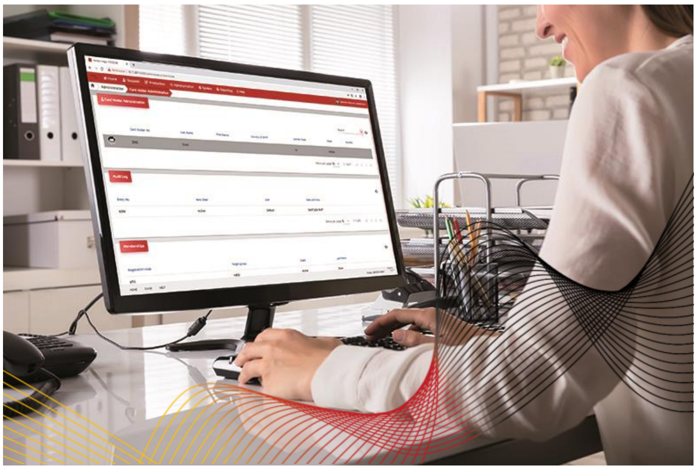
SSI is perfectly capable of handling Government issued IDs

7 Veridos’ leading edge solutions help unlock eGovernment potential

As a leading provider of identity solutions, Veridos is actively involved in the innovation needed to create state-of-the-art end-to-end lifecycle solutions for different eGovernment requirements – from the establishment of a unique identity of an individual through to the actual issuance of the digital ID.

7.1 IMAGO

Through its IMAGO lifecycle management framework for identity credentials, for example, Veridos supports a full spectrum of enrolment scenarios and has already installed IMAGO[12] enrolment systems in more than 40 countries worldwide. Registration officers can use IMAGO to acquire all required attributes and query biographical information. Once verified, this data will become the trusted anchor for the issuance of new digital IDs.



IMAGO verifies the quality and validity of biographic and biometric data such as fingerprints, face, iris and signature images captured during enrolment and ensures compliance with both ICAO standards and EU regulations. It also interfaces with Automated Biometric Identification Systems (ABIS) to verify biometric data and check the biographic record against the stop/blacklist systems on a national and/or international level (e.g. INTERPOL), as desired. Additionally, the framework supports all major hardware and can be used with enrolment and document personalization devices from all major manufacturers. The IMAGO suite is compatible with all state-of-the-art software platforms and databases.

To further automate the enrolment process Veridos offers self-enrolment kiosks to provide the establishment of unique identities. Applicants can use the terminals to perform the enrolment, providing biometrical data into the platform. They can also register their smartphone during the enrolment to connect the mobile ID to a verified device to enhance mobile security. In the future it is likely that iris scans and contact-less fingerprint sensors will provide alternatives to facial scans, helping to speed up the process of identification, verification and authentication.

7.2 VeriGO® TrueID

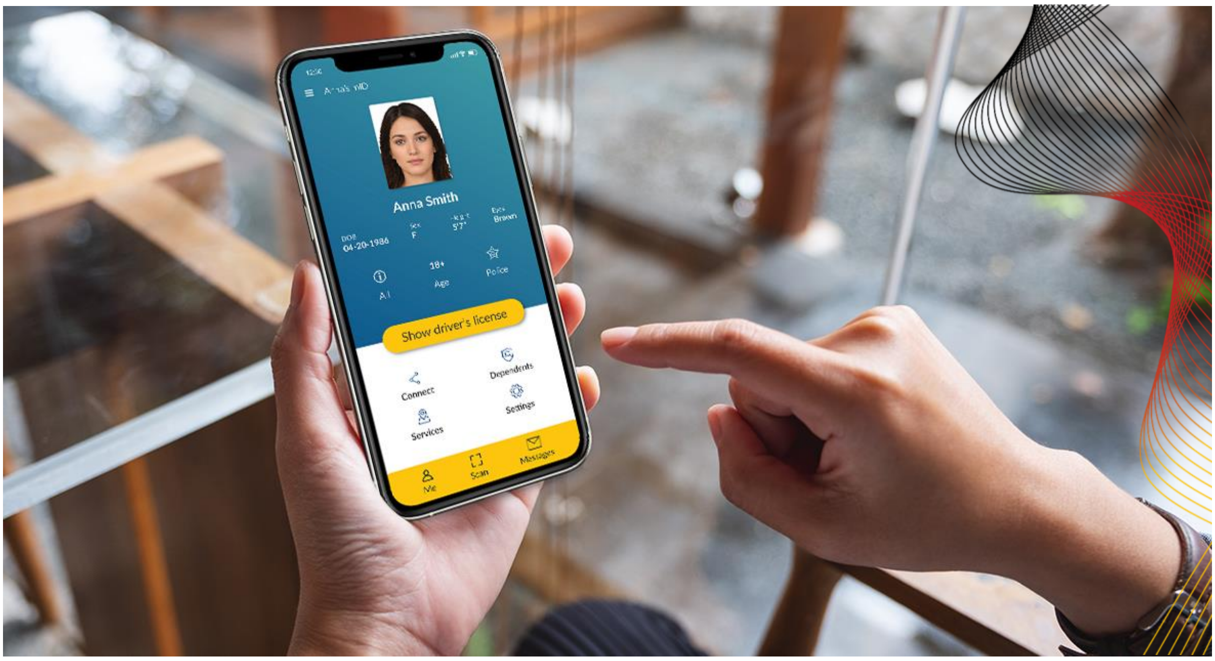
VeriGO® TrueID makes it easy for citizens to carry out such tasks as renewing official documents or registering a birth. The cutting-edge technology allows citizens to easily verify their identity via face recognition. Citizens no longer need to visit an office in person, they can simply download the smartphone app and access the desired service from wherever they are. This increases accessibility in remote regions while also cutting costs for governments. The mobile face authentication solution consists of a mobile app for face detection and a server-side matching service. The citizen does not need to enroll in advance to access the service, as the matching is performed against an existing national biometric database. Liveness detection helps to prevent spoofing attacks. The VeriGO® TrueID solution can be seamlessly integrated into an existing eco-system and works on all commonly used smartphones on a BYOD (bring your own device) basis.

7.3 VeriGO® DriveID

Complying with the new industry ISO 18013-5 mDL Standard, VeriGO® DriveID goes far beyond providing a simple image of a license held on a phone or in a digital wallet. Using a secure backend system, it provides encrypted access to data held on the original driver's license database which is then made securely available through the driver's license app on the holder's smartphone. It is a state-of-the-art infrastructure that opens doors to a comprehensive, cost-efficient modern identity management system.

Supported by cryptography, the DriveID solution provides secure and reliable verification of the document and user ID and access to up-to-the-minute data contained in the issuing database. Neither a substitute for a physical card nor an attempt to replicate its printed security features, an mDL is user-centric and privacy friendly, allowing for data minimization.

Easy to implement, it provides rapid verification using standard interfaces across operating systems and devices and can be readily expanded using document lifecycle management to register and verify users and manage data.



Through this platform, citizens can access virtually every government service and complete transactions via a secure multi-channel communication protocol, if desired. The services could include establishing their digital identities, voting in elections, paying their taxes and applying for a driver's license or passport, along with a multitude of other public services.

7.4 D4FLY seamless border control

Complemented by Veridos’ innovations in the context of seamless access management, users can be identified and granted access to specific areas solely by passing through specific gates. By using the triple blinding functionality, the citizen can be sure of his or her anonymity regarding his identity trail. In a current project with the European Union, D4Fly (Detecting Document frauD and iDentity on the fly), for example, Veridos is improving border-crossing experiences for travelers. The D4FLY solution consists of a border control kiosk equipped with enhanced enrolment, verification and detection capabilities, smartphones applications for improved performance and verification capabilities and a non-stop on-the-move system for biometric verification.

7.5 Software and Hardware tokens

Both types of tokens have potential roles to play in the development of ID authentication. Software tokens are a safe and mature solution, being both easy to use and well protected, if used in the right context of services.

Hardware devices are proving to be increasingly attractive to users. The StarSign® Crypto-USB-Token[14] from G+D, Veridos' parent company, for example, is a highly secure PKI-based token that has already stimulated considerable market interest and is currently being used, for example, as an authentication token by the German tax authorities. The StarSign® Key Fob is a convenient alternative that can be carried on a key chain or neckband with an integrated fingerprint sensor. Both the USB and fob use a Bluetooth® 5 module for easy integration into a wide range of applications and can be used on any USB enabled host system.

Employing similar highly secure technologies, the StarSign® Wristband comes with a wide range of applications and makes it an ideal multi-purpose wearable. Users can use it open up systems or gates anytime, everywhere by way of a simple tap with the band on an NFC reader. Fully waterproof, it is also ideal for outdoor use, while the GlobalPlatform® compliant JavaCard™ operating system allows the installation of third party applications, even in the field on the fly.

The Trusted Application Kit produced by Veridos sister company Build 38[15] is a software security framework that helps to protect mobile applications and corresponding assets. It incorporates many different layers of software technologies to strengthen the level of security, e.g. binary code obfuscation, white-box cryptography, device binding, secure monitoring and secure end-point communications. Easily integrated in Android and iOS mobile applications, TAK allows sensitive and confidential data to be stored on the device without extra hardware or special platforms and is therefore widely scalable.

StarSign® Key Fob
(FIDO™ U2F, FIDO™2)

StarSign® Wristband
(FIDO™ U2F, FIDO™2)

8 Case study

8.1 Project OPTIMOS[16] – Potential for the new mainstream?

Today's consumers use their smartphones to access numerous services requiring a high level of security. For example, they unlock car sharing vehicle doors, open bank accounts and register new addresses with city authorities. To do this, they usually set up an identity (eID) directly with the provider of the service, which then has to be verified in a trustworthy, but usually time-consuming, process. But up to now digital technologies with an adequately high protection level which offer this functionality on a smartphone have been lacking.

The second phase of Germany's project OPTIMOS, funded by the Federal Ministry of Economics and Energy (BMWi), is set to change this.

The OPTIMOS 2.0 project has created the bases for an open ecosystem that provides the technologies for secure eID services enabled via a citizen's smartphone. These technologies will allow eID service providers to offer mobile eID services consistent with the EU eIDAS regulations, meaning that it can be used across the whole of Europe.

Providers of mobile services wishing to store sensitive data other than the eID on smartphones can benefit from the open mobile ecosystem, too. For example, airline companies will be able to store boarding passes, transport companies a personal annual season ticket and car sharing companies or hotels digital car or room keys.

The OPTIMOS 2.0 project aims to create a platform that relieves service providers of time-consuming tasks and ensures a high level of hardware-based security at the same time. The initial mobile ecosystem will focus on the following roadmap:

Infrastructure

- Service Provider API
- TSM
- ID applications
- API to smartphone and services
- Cryptographic API for eSE and eSIM

ID services

- Notification
- eSE Certified devices
- Federal services portal
- Integration of notified EU
- ID systems Certificates
- Vehicle registration
- Integration in service and citizen accounts
- eSE and eSIM certified devices
- integration in public services

Travel and border control

- Prototype driver's license

Healthcare sector

- eHealth card
- e-prescription
- Other services

Regulated markets

- Insurance, banks
- More ID documents

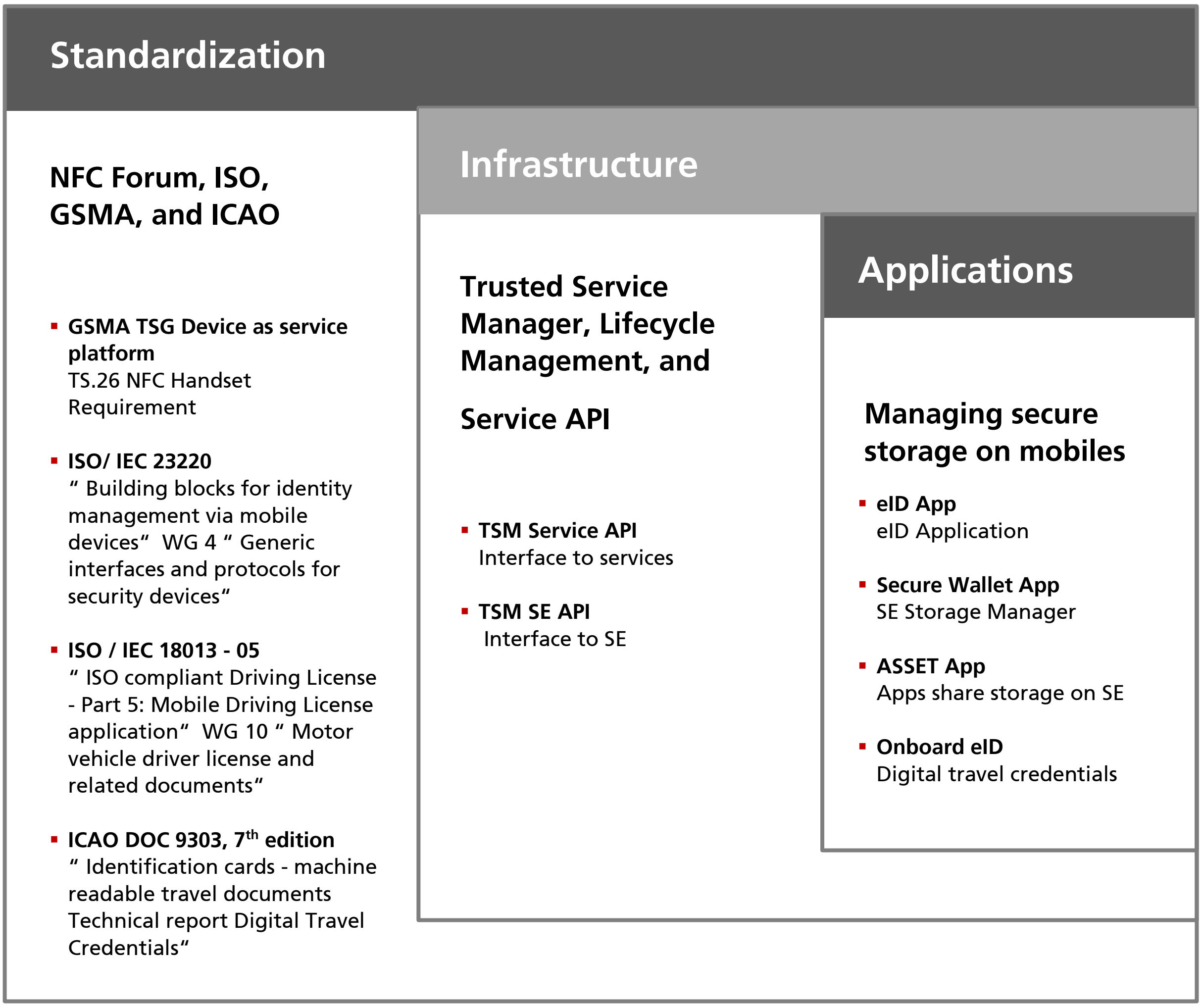
Administration

- Certificates
- Vehicle registration

Funded by Germany’s Federal Ministry for Economic Affairs & Energy, in collaboration with Ministry of the Interior, Building and Community and the Office for Information Security as part of the “Smart Service Welt II” program, the research part of the OPTIMOS 2.0 project concluded in November 2020. It has built the foundations for a new German mobile ID, which becomes available in early 2022.

The project has focused on three main areas:

Compliance with standards currently being developed, e.g. ISO/IEC 18013-05 or ISO /IEC 23220, as well as with existing ones, s e.g. ICAO DOC 9303, 7th edition for travel documents.



Standardization

NFC Forum, ISO, GSMA, and ICAO

- **GSMA TSG Device as service platform**
  TS.26 NFC Handset Requirement
- **ISO/ IEC 23220**
  “ Building blocks for identity management via mobile devices“ WG 4 “ Generic interfaces and protocols for security devices“
- **ISO / IEC 18013 - 05**
  “ ISO compliant Driving License - Part 5: Mobile Driving License application“ WG 10 “ Motor vehicle driver license and related documents“
- **ICAO DOC 9303, 7th edition**
  “ Identification cards - machine readable travel documents Technical report Digital Travel Credentials“

Infrastructure

Trusted Service Manager, Lifecycle Management, and

Service API

- **TSM Service API**
  Interface to services
- **TSM SE API**
  Interface to SE

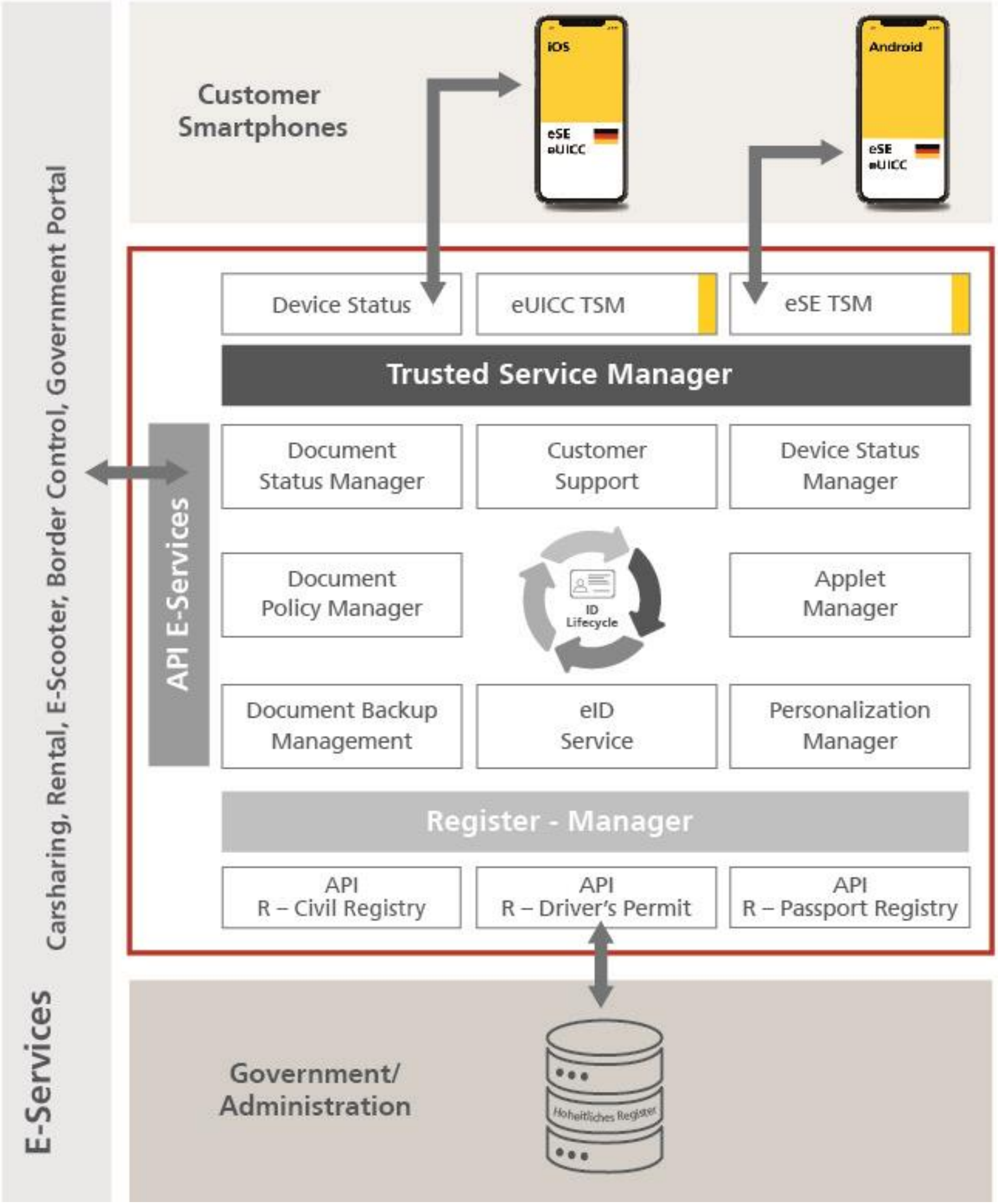
Applications

Managing secure storage on mobiles

- **eID App**
  eID Application
- **Secure Wallet App**
  SE Storage Manager
- **ASSET App**
  Apps share storage on SE
- **Onboard eID**
  Digital travel credentials

OPTIMOS’ overview and activities

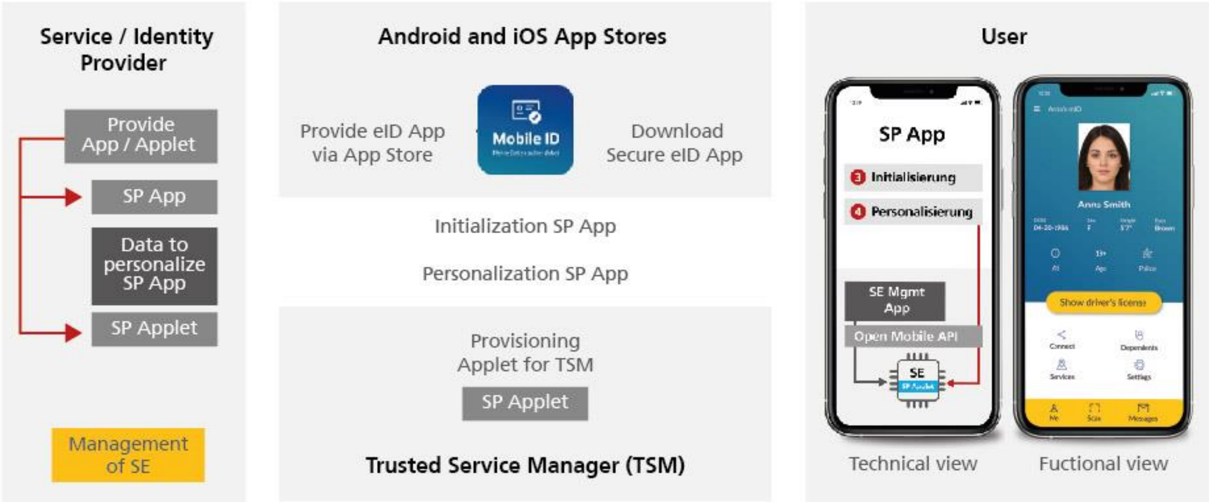
Providing the necessary infrastructure for a seamless citizen onboarding, the integration and management of device specific eSEs and eSIMs, providing secure channels to trusted service managers (TSMs) and enabling online authentication for services.



E-Services and lifecycle management

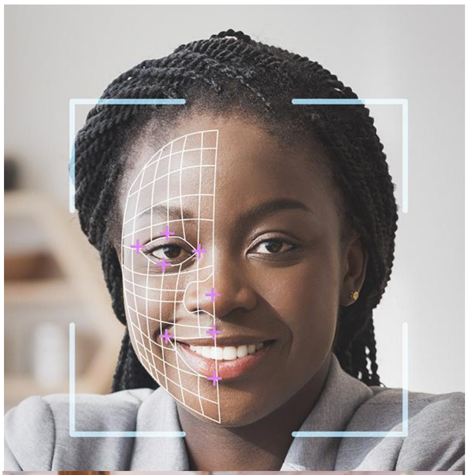
Mobile interfaces for citizens, with apps that allow user interaction and provide convenient interfaces to services provided by either the public or enterprise sector.

OPTIMOS therefore now provides a smartphone based secure ID derived from the national ID document along with secure managed storage for additional ID's or high value assets. With applications for government services and mobile registration, it demonstrates the benefits of a mobile ID and is an open, practicable framework for mobile IDs and mobile assets.



Mobile ID provisioning processes

9 Conclusion



As in previous waves of industrial and technological revolution, initial progress in the development of eGovernment services was characterized by individual, usually proprietary approaches. Early adopters obtained the benefits of improved services but many are left with often inflexible legacy systems as a result.

In the current wave of eGovernment, which is already well advanced, both the established leaders in the field and the later arrivals are increasingly attuned to the benefits of working to new international standards through the adoption of open system solutions. One thing seems abundantly clear from the experiences of the past decade: the pace of change over those 10 years was far greater than anyone would have predicted at the outset of this era and is showing no signs of slowing down. The technological solutions now being developed, therefore, will almost inevitably be superseded, and quite probably in a relatively short period, by better solutions.

Governments hoping to take advantage of such improvements in technology, therefore, are well advised to keep their options as widely open as they possibly can by selecting solutions today that can be expanded, upgraded and enhanced, or even entirely replaced, with the minimum possible disruption to service delivery and cost. Establishing robust "root credentials" and employing sophisticated but open authentication and verification technologies will help them improve the delivery of every kind of public service, for the benefit of their citizens today and tomorrow.

Watch these videos

How2eGov

eGov ecosystem

eGov through a lifetime

10 About Veridos

Veridos is a world-leading provider of integrated identity solutions. Governments and public authorities in more than 100 countries trust the company's uniquely comprehensive product portfolio.

We support our customers with secure, reliable and holistic solutions, expert guidance, and future-proof technology to enable local infrastructure and empower citizens worldwide.

Our Vision

We believe unique identities are a human right, granting access to the physical and virtual world.

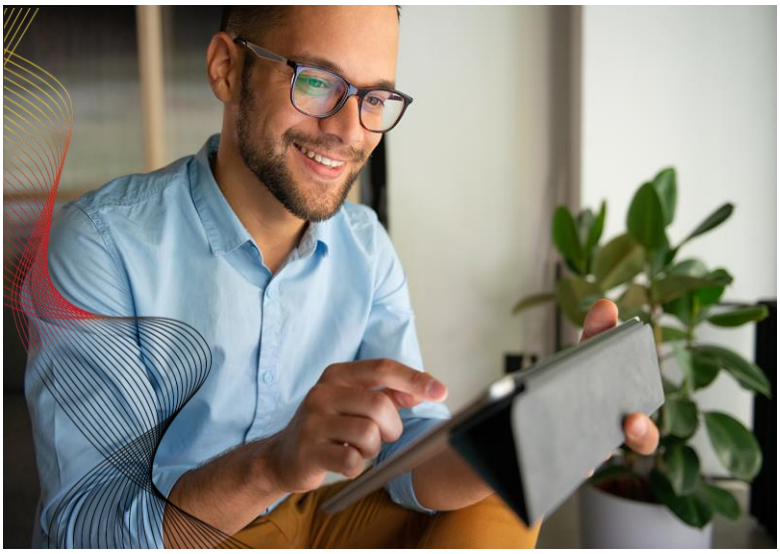
Our Mission

We secure trusted identities for everyone by delivering holistic solutions to governments and their citizens.

Our mission to secure trusted identities for everyone by delivering holistic solutions to governments and their citizens. These range from paper to security printing, electrical chip components, enrollment, personalization and issuance, and border control solutions including eGates. Governments can acquire best-in-class passports, ID cards, driver's licenses, and more, or even the facilities to manufacture their own.

Our broad portfolio gives us the rare ability to cover the full identity value chain at the scale or complexity required. We consult our clients to provide bespoke identity solutions with a high certainty of success. This means maximum convenience for customers and citizens, as we provide support through increasing complexity while securing the future viability of ID infrastructures.

Governments appreciate the flexibility of our modular, standardized components. Designed to perfectly complement one another, these range from individual parts to customized end-to-end solutions and comprise analog, digital, and mobile solutions, identity management systems, and complete identity infrastructures, as well as individual components and self-sufficient ID factories.



Veridos combines state-of-the-art technology with best-of-breed innovation through in-house R&D and by pooling the expertise of its parent companies, Giesecke+Devrient GmbH (60% ownership) and Bundesdruckerei GmbH (40% ownership). Our customers benefit from this strong tradition of innovation, heritage, and natural synergies.

Veridos is headquartered in Berlin with an office in Munich, and Veridos employs more than 400 people worldwide. These include subsidiaries, production sites, and local representatives everywhere from the United States to Canada, Mexico, Greece, the United Arab Emirates, and beyond.

Learn more about our products and components, how we develop and integrate custom identity solutions, our operational and maintenance services, and complete factory solutions for independent ID manufacturing at www.veridos.com.

11 Useful Links

Veridos focus page on eGovernment: **www.veridos.co/how2eGov**

eGovernment use cases throughout a lifetime: **www.veridos.co/eGov**

Download Veridos' eGovernment brochure

Download eGovernment services brochure: **www.veridos.co/eGov_services_brochure**

About Veridos: www.veridos.com/en/interactive-company-brochure.html

12 Appendix 1

12.1 Regulatory requirements

A variety of standards are used in the development of capabilities to ensure interoperability between identification systems. None of these are directly enforceable as part of a regulation but there are some regulatory requirements regarding power and frequencies for wireless connections (such as NFC) and privacy regulations to be taken into account (such as the EU's GDPR Directive).

- (GDPR) (Regulation (EU) 2016/679)
- eIDAS EU Regulation 910/2014
- ISO 18013-5 interoperability standards for mobile drivers licenses
- ISO/IEC CD 23220-1 Cards and security devices for personal identification — Building blocks for identity management via mobile devices
- NIST 800-63
- NIST 800-157 standard for PIV derived credentials
- ICAO 9303 regarding electronic passports (MRTD)
- ISO/IEC 7810 standard for identification cards
- ISO/IEC 7816 standard for smart cards
- ISO/IEC 14443 standard for proximity card (contactless smart card)
- ISO/IEC 15693 standard for vicinity card (contactless smart card)
- ISO/IEC 17830 Biometric on card
- ISO/IEC 18013 standard for electronic driver's license
- ISO/IEC 24760 framework for identity management
- ISO/IEC 24761 authentication context for biometrics
- ISO/IEC 24727 standard API for eID
- ISO/IEC 24789 standard for identification cards
- ISO/IEC 29003 identity proofing
- ISO/IEC 29144 biometric technology in identity management
- ISO/IEC 29115 entity authentication assurance framework
- ISO/IEC 29191 anonymous unlinkable authentication
- ANSI/NASPO-IDPV-2014, Requirements and Implementation Guidelines for Assertion, Resolution, Evidence, and Verification of Personal Identity

13 References

1. 2020 United Nations E-Government Survey

https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey

2. Estonia – the Digital Republic Secured by Blockchain; PwC

https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

3. 2017 Gallup World Poll

https://news.gallup.com/poll/224375/gallup-top-world-findings-2017.aspx

4. World Bank Global Findex Report 2017

5. FIDO Alliance Specifications Overview

https://fidoalliance.org/specifications/

6. eIDAS Regulation

https://www.eid.as/#article1

7. United Nations Sustainable Development Goal Target 16.9 ("legal identity for all, including birth registration, by 2030")

https://unstats.un.org/legal-identity-agenda

8. World Bank id4d Global Dataset

https://id4d.worldbank.org/global-dataset

9. WBC: protecting cryptographic keys in software applications

http://www.whiteboxcrypto.com/

10. Web Of Trust Info / self-sovereign-identity Public

https://github.com/WebOfTrustInfo/self-sovereign-identity

11. WC3 Decentralized Identifiers (DIDs), Proposed Recommendation 03 August 2021

Decentralized Identifiers (DIDs) v1.0

12. Veridos IMAGO

https://www.veridos.com/en/document-management.html

13. VeriGO® TrueID

www.veridos.com/en/verigo-trueid.html

14. G+D StarSign®Crypto USB Token M

https://www.gi-de.com/corporate/Identities/Enterprise_Security/Hardware-based_authentication/Datasheet_Crypto-USB-Token-M.pdf

15. Build 38 Trusted Application Kit

https://build38.com/solution/

16. Project OPTIMOS

https://www.bundesdruckerei.de/en/innovations/optimos