The Digital Identity Revolution

From eID to Mobile ID
From eID to Mobile ID

The delivery of successful and secure digital identity is fundamental to the modernization of states and dematerialization of public services. It is also critical to support the digital transformation of their economies and the development of trusted public and private digital services.

Governments are ideally placed to deliver this foundation for our digital future. Whether they are seeking to protect citizens online, boost economic growth, achieve greater efficiency or reduce the spiraling cost of public services, what is certain is that any national digital identity platform must be based on a backbone of trust.

One of Gemalto’s greatest assets is the ability to extend smartcard-based national eID and digital identity schemes to mobile. Gemalto Mobile ID Smart App is a cutting-edge application that enables governments to offer strong authentication and identity validation services to their citizens by transforming the device in all our pockets into a mobile trusted digital ID.

The need for mobility and convenience

Accessibility is key to the success and adoption of digital services. Given the sheer volume of devices worldwide, smartphones clearly offer a compelling proposition for governments seeking to provide citizens with secure and convenient access to online public services.

On average, an individual has to handle 27 different login and password combinations to access online services. Not surprisingly, password fatigue is becoming a real problem. Users want a secure digital identity and frictionless mobile experience, replacing passwords with simple mobile-based PINs and biometric authentication to take full advantage of the wealth of fast and convenient digital services available.

If they knew the app was secure, 70% of online service users would want digital ID documents on their smartphone.

Accelerating the shift towards mobile ID schemes

Governments around the world are capitalizing on the mobile revolution. Many national mobile ID initiatives are underway, notably including Estonia, Norway, Belgium, Qatar, Oman and The Netherlands.

Many of these initiatives are either government-driven or government-supported, with the goal of serving the entire economy by providing a single trusted digital identity to protect both public and private online services.

Government-backed digital ID schemes can quickly achieve critical mass by focusing initially on public services and then expanding out to serve the wider economy. Once a scheme has a critical mass of active users, it becomes an extremely attractive proposition for the private sector, which can leverage the national digital ID scheme to secure their online channel or securely integrate new customers.
An inclusive solution
The Mobile ID Smart App is inclusive. It works on any smartphone, anytime and anywhere, to ensure governments can address all citizens and residents.

One mobile ID, many use cases
Mobile ID Smart App enables a rich, convenient and trusted online experience where citizens can prove who they are online, authenticate to websites, confirm transactions and digitally sign documents. All this can be done in a matter of seconds, while better engaging with public and private online service providers.

A SINGLE MOBILE ID FOR:

**USER IDENTIFICATION / ID PROOFING**
Citizens can prove who they are in an online environment, safely sign up for new online services and undertake real-time ID checks. It also helps online service providers comply with know-your-customer policies.

**ONLINE AUTHENTICATION**
A mobile ID is a strong authentication tool enabling citizens to securely log in and validate transactions online.

**DIGITAL SIGNATURE**
Thanks to PKI technology, citizens can use their mobile ID to digitally sign documents in a few clicks.

Multi-level security
This PKI-based mobile authentication solution covers all levels of security, right up to the highest (e-IDAS High, NIST Authentication Assurance Level 3, ISO LoA 4). The level of assurance is scalable and can be adapted to suit the risk and nature of the services being accessed. This enables government bodies and service providers to have a rich and adaptive security policy that can be adjusted to all situations and complies with relevant regulations.

Modularity by design
Leveraging smartphone features such as NFC, cameras and fingerprint readers, Gemalto’s Mobile ID Smart App was designed with modularity in mind. Using the latest biometric authentication functionalities, it delivers the most enhanced and safest online self-registration and authentication experiences for citizens.

Enhanced user experience
Complex enrollment and authentication processes are the last thing citizens need when looking for safe and fast access to online public and private services. That’s why Gemalto has placed both security and user convenience at the heart of its proposal, from enrollment right through to everyday usage.
Delivering a unique end user journey

It all starts with an easy first time registration

A seamless onboarding experience for mobile ID is critical. People have no time for cumbersome processes and a good first impression is key to widespread adoption.

Gemalto leverages its identification and biometric expertise to provide a more agile registration process through a wide range of identification and enrollment scenarios. This enables governments to be inclusive and offer solutions that address all user profiles as well as their own pre-requisites.

Easy first time registration:
- Supports multi-channel registration, including face-to-face as well as remote self-onboarding, with various scenarios to fit with each user’s profile (multi-channel)
- Supports remote ID proofing from both electronic and non-electronic ID documents to suit the ecosystem
- Employs the latest biometric authentication features to deliver frictionless, optimized user experience
- Enables step-up identification

Easy first time Registration
Multiple Registration Channels
- In-Branch at Registration Authority office
- From PC
- From Self-service Kiosks
- From Smartphone

Onboarding Modularity by Design approach

<table>
<thead>
<tr>
<th>MODUS OPERANDIS</th>
<th>REACH</th>
<th>ASSURANCE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>eIDAS HIGH NIST LoA 3 ISO LoA 4</td>
<td>Android</td>
<td>eIDAS HIGH NIST LoA 3 ISO LoA 4</td>
</tr>
<tr>
<td>eIDAS HIGH NIST LoA 3 ISO LoA 4</td>
<td>Android</td>
<td>eIDAS Substantial NIST LoA 2 ISO LoA 3</td>
</tr>
<tr>
<td>eIDAS HIGH NIST LoA 3 ISO LoA 4</td>
<td>Android</td>
<td>eIDAS HIGH NIST LoA 3 ISO LoA 4</td>
</tr>
</tbody>
</table>
Followed by a smooth everyday authentication experience

Empowered with Gemalto Mobile ID Smart App, citizens can securely authenticate and confirm any online transaction using their smartphone as their secure online national identity.

The app supports one of the widest range of authentication methods citizens can choose from, depending on their preferences and profile (PIN code, geometric patterns, fingerprint, facial biometrics, etc).

How it works:

To logon and open a session, end users receive a push notification on their smartphone inviting them to authenticate through the app. Next the user either enters their PIN, scans a fingerprint or runs face recognition to be granted access to various online public and private eServices.

**Step Up Authentication:** For specific public eServices which require the highest level of security with a strong signature, such as access to online medical records, Gemalto’s Mobile ID Smart App can also turn into an NFC document reader for official contactless eID documents. In such cases, the user authenticates using the Mobile ID Smart App in NFC mode with their contactless eID card and PIN. This not only offers the highest level of authentication, but also allows for a Qualified Electronic Signature (QeS), a legally-binding equivalent to a handwritten signature within many national legal frameworks.

Other authentication options include using the app in NFC mode with an ePassport combined with face recognition. Whenever a QeS is required, and following the same principle, the Mobile ID Smart App can also turn into an NFC document reader to communicate with contactless eID documents such as eID cards, ePassports, eDriver’s licenses, etc.

These options, using secure communication between the app and an electronic ID document in NFC mode, make Gemalto’s Mobile ID Smart App the logical choice for eServices requiring the highest protection.

Our solid experience and leadership in secure eDocuments and contactless technology means that, when it comes to mobile ID solutions, we are at the forefront of innovation.

A modularity by Design approach to Authentication
Managed through an intuitive digital identity self-care portal

Convenience is about more than easy registration and smooth day-to-day usage. It also demands straightforward digital identity management. Gemalto’s self-care portal was designed with the user interface and user experience in mind, providing citizens with an intuitive digital identity management platform from which they can manage their digital identity and credentials easily and efficiently throughout their entire lifecycle, from the creation of a digital identity right through to revocation.

Fully compliant with the European GDPR (General Data Protection Regulation), the platform puts citizens in control of their data. In just a few clicks, they can easily manage and update information on their persona and ID attributes, as well as setting up their data sharing consent policy and preferences.

Advanced features of the self-care portal also enable citizens to manage identity delegation.

Intuitive Digital Identity Management

Citizen’s self-care portal

Digital ID Life-cycle Management

| Creation | Credential | ID Sharing Consent | Personal Data | Rights’ Delegation | Revocation |

Mobile ID Smart App – hard at work, behind the scenes

Back end management of the Gemalto Mobile ID Smart App is handled by the Gemalto Digital ID Services platform, which orchestrates and powers the entire life-cycle management of the trusted mobile identity, from user registration to verification of mobile authentication, digital signatures and connection to the certification authority and online service providers.

Both authentication and signature are processed out-of-band, ensuring a stronger and more secure authentication solution.

Mobile ID Smart App is based on PKI technology and stores the user’s digital ID, keeping their digital credentials protected and secured at all times. When the user wants to authenticate, the back end platform sends a challenge response to the Mobile ID Smart App. This is signed by the user, thanks to the PKI keys securely stored in their mobile app or from a secure document. The user authenticates with either a PIN code, fingerprint or face recognition.

This solution uses multi-factor authentication to allow service providers to define different authentication scenarios, depending on their security policy.

They can choose from:

- Something the user has (Mobile ID Smart App, eID card, ePassport, etc.)
- Something the user knows (a PIN, a pattern, etc.)
- Something the user is (biometric data such as fingerprint, face, etc.)

A mobile ID with built-in software security and privacy principles

A winning multi-layered approach to security

Mobile brings convenience, but comes with its own security challenges. The use of mobile devices indeed opens up new areas of vulnerability, so it is crucially important to protect mobile applications that run within such environments.

We take a multi-layered approach to security to combat ever more sophisticated hacking techniques. The app is built on Gemalto Mobile Security Core, our comprehensive in-house mobile application shielding offering, for which our expertise was recognized in the latest Gartner report. It integrates all the best practices that Gemalto has built and implemented over the years to secure mobile applications and guarantee their data integrity.

Gemalto’s Mobile Security Core encompasses the full range of anti-tampering and hardening capabilities, such as anti-debugging, anti-hook, white box cryptography, obfuscation, and jailbreak or root detection.
As a result, our **Mobile ID Smart App** can withstand the dynamic nature of malware, and has the capability to defend itself in the field, detect unsecure environments and react accordingly.

To ensure it is always a step ahead of hackers in terms of security, the app benefits from regular updates with the latest security patches available on the market.

Self-protected Mobile ID Smart App enabled to:

**DEFEND**
- Integrity of Mobile App
- Sensitive assets

**DETECT**
- Unsafe environments
- Attempted attacks

**REACT**
- Stop execution
- Perform custom actions such as warning users or sending an alert to a risk management server

Privacy in an era of digital identity

As our society becomes increasingly digital and data-dependent, digital security and privacy protection have become public policy priorities. People want to be in control of how their personal information is used and shared.

With this in mind, Gemalto has opted for a privacy-by-design approach. Our Mobile ID Smart App is fully compliant with the GDPR and offers built-in principles that ensure:

- Data minimization
- Data protection
- User’s privacy rights management

A strong value proposition for all stakeholders

**Governments** using Gemalto’s Mobile ID Smart App benefit from a **field-proven** mobile identity solution designed to guarantee wide adoption from both eService providers and citizens. The solution is **future-proofed** through Gemalto’s commitment to delivering an app and related security that is always up to date, and compatible with all handsets, the latest OS, and the most recent security patches.

**Public & Private eService Providers** benefit from the robust security provided by the mobile ID national scheme without having to bear the cost of it. They can adjust the level of security to suit the nature of their services and can offer an improved online experience to their customers. This in turn will positively impact the volume of transactions.

**Citizens** can enjoy a unique and simplified login experience to securely access an array of online services, eliminating password fatigue. Multiple and remote enrollment scenarios are available to suit every user profile. Accurate biometric recognition means fast enrollment for everyday use. Moreover, citizens can benefit from a robust digital identity for all their online interactions, with enhanced user privacy features and protection against the risk of identity theft. With such a **user-centric approach**, citizens are in total control of their digital identity and can manage it, along with their personal data, through an intuitive self-care portal.
We have the technology to enable digital transformation through trusted mobile ID solutions

Gemalto has unrivaled experience in identity and document verification, authentication, digital signatures, biometrics, mobile device and software security. We integrate all the technologies needed to seamlessly capture and verify user identities and digitalize them securely.

As a result, governments can rely on us to provide trusted mobile identity schemes that will accelerate their digitalization strategies, enable them to launch new online public services, fight fraud and meet regulations.

A trusted partner for your trusted digital identity projects:

> **Mastering the full chain of trust** throughout the entire mobile ID credential life cycle (from identification and enrollment through to revocation).

> **Field proven technology trusted around the world** in 18 mobile identity and online federated identity platform references.

> **Mobile identity designed to win adoption.** Our solutions are tailored to accelerate the digital transformation of a country by meeting your individual needs, your local needs, and those of your citizens and online service providers.

> **Richest multi-channel registration scenarios.** When onboarding to the Mobile ID Smart App, Gemalto has a truly differentiated offering in identity verification. It sets us apart from the competition in terms of security, flexibility, resilience and service availability.

> **Expertise in biometrics.** We have the technology to verify that a person is who they claim to be! Building on the acquisition of Cogent 3M, Gemalto benefits from 27 years of biometric technology expertise. We offer world class biometric algorithm accuracy, ranking amongst the top biometric experts, according to the latest NIST benchmarks (US National Institute of Standards and Technologies).

> **Future-proof solutions.** By choosing Gemalto for your mobile ID scheme, you are choosing a provider that is already working on tomorrow’s technologies. The mobile environment is ever-changing, with new smartphones entering the market every year and regular OS updates. Governments deploying a national mobile ID scheme need to be able to trust their mobile ID app to work at all times, on all devices, throughout the years ahead. Gemalto, with deep expertise in telecommunication and software security, commits to delivering a continuously updated app and security scheme, through an active policy to maintain mobile ID compatibility with your market’s needs.

> **Consulting services.** With a track record of deployed mobile identity schemes in various environments and ecosystems, no company is better placed to share the expertise and best practices that your project could benefit from. Ultimately, there is no ‘one size fits all’ solution; identity is very much tied to a country’s cultural characteristics and regulatory framework. Through consulting services, Gemalto can help define a successful digital ID scheme that will best reflect these local factors too.

> **Industry recognition.**

**ABI research**

Phil Sealy, Senior Analyst at ABI Research: "Gemalto continues to innovate at the forefront of the digital identity market, in line with future market trends. The company is placing the emphasis on eGovernment enablement regardless of the device used by citizens – computers, smartphones, tablets and more."

Frost & Sullivan recognized Gemalto with two 2018 Global Company of the Year Awards for its comprehensive mobile security suite to support the secure transition to digital-first interactions, delivering identity verification, user authentication, transaction verification, and fraud prevention to create a seamless user experience, regardless of device.