From Multiple Digital Identity to One trusted Digital ID

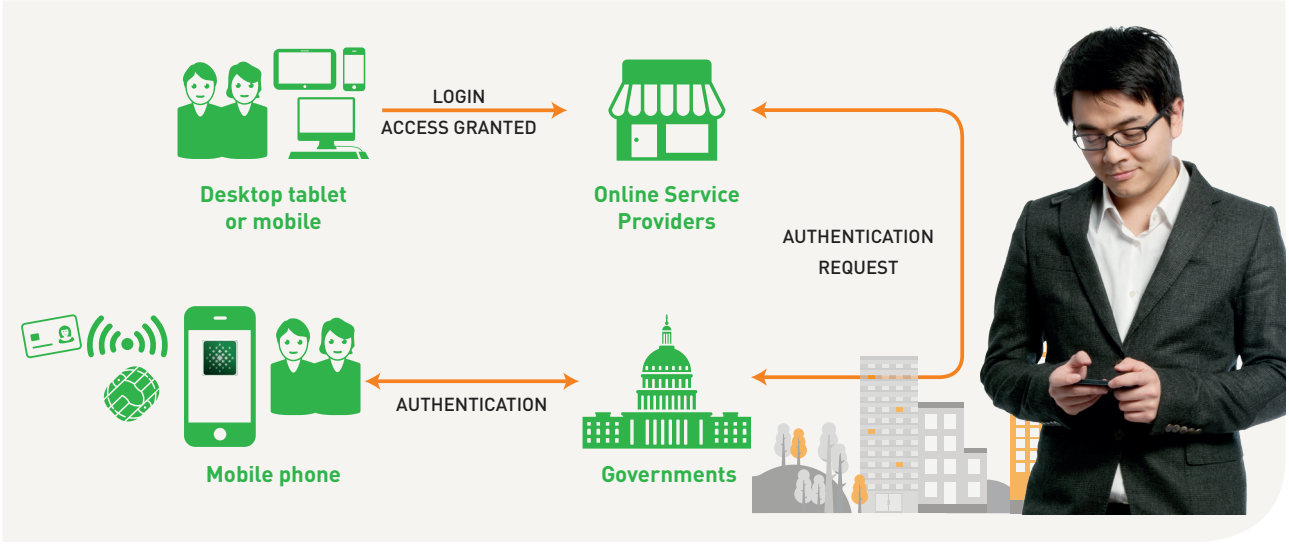
Coesys mGov

Secure digital mobile lifestyle

The digital revolution is impacting all sectors of society. One of the most visible changes is the advent of multichannels access to online services via Internet or mobile apps. While this extraordinary growth in digital usage has changed the way we conduct our business, it has also triggered a new industry of malicious software bent on stealing users' online credentials.

Governments around the world are seeking to boost efficiency and transparency in many essential functions, with the ultimate aim of better serving their citizens in a reliable, secure and transparent manner.

One challenge is to ensure reliable match between an online identity and a real one.



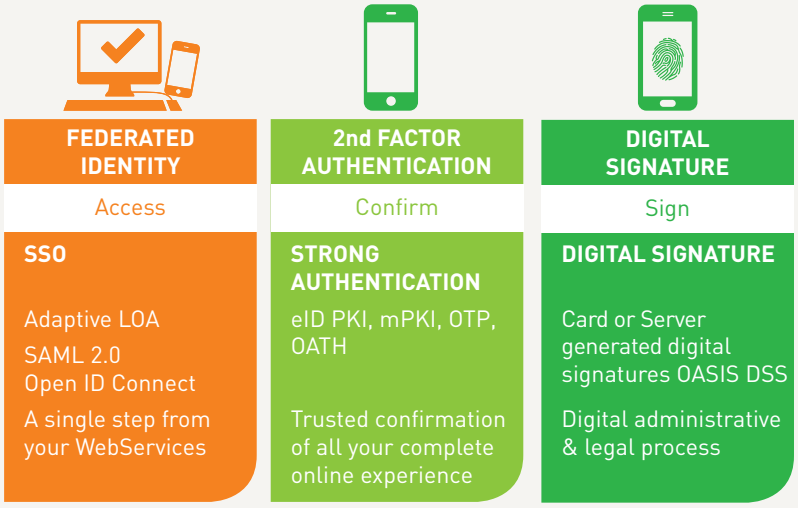
Coesys mGov enables citizens to securely access online services. This state-of-the-art mobile application enables strong authentication and digital signature using a combination of contactless national eID card and NFC phone. As a result, countries can put in place Trusted National Mobile ID schemes. Based on standards, it perfectly fits with governments' existing digital identity and security schemes.

MyMobileID is a app which communicates with Coesys Gov Server to perform **out-of-band** authentication and signing. This duality of communication channels offers, by design, a stronger authentication solution. OOB mobile digital signatures with contactless cards can be used for user authentication and authorization with any online service, including e-banking and corporate VPN access, or for signing emails and files.

Different Mobile ID solutions can be implemented, such as using the phone as a reader [Credentials can also be stored in the Secure Element of the eID or a SIM card].

Coesys mGov targets high level of assurance using a PKI-based mechanism. The user's private key signs a challenge sent from Coesys eGov.

Coesys mGov provides both security and convenience giving citizens and governments confidence in trusted online transactions.



Credentials & Attributes storage SE: eID / SIM / eSE / TEE

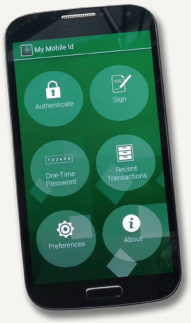
Derived Credentials from an eID to another SE

To further simplify the user experience, Gemalto's Mobile ID solutions such as Coesys mGov supports the creation of Derived Credentials on the SIM card itself, or any Secure Element (TEE, eSE...) This key figure addresses expected future needs of digital societies.

Derived Credentials can be used not only for authentication and signature purposes, but also to create a **Digital Companions.**

Main features

- Mobile signatures for authentication services, authorization or non-repudiation services, such as transaction signing
- Both connected and unconnected OTP
- Simplified operation allowing QR-code driven registration and signing
- Proof of Possession code
- Allows white-boxing to include customer's look and feel
- Standard government contactless smart card support using NFC and PACE
- eIDAS compliant
- Works with Sealys Mobile Link



STANDARDS

- **Authentication:**
  - SAML 2.0
  - OpenID Connect
  - OAuth 2.0
- PACE, IAS V4, APDU NFC, USB standards
- **Digital signature:**
  - PAdES, CAdES, XAdES
  - Timestamping
  - OASIS DSS
  - Participated in ETSI plug tests
- **Other Standards:**
  - X.509
  - LDAP
  - PKCS#1 PKCS#7
  - XMLdSIG

GEMALTO.COM

gemalto
security to be free