Coesys eGov and mGov

Helping public services go digital – and mobile

The digital revolution is impacting all sectors of society. One of the most visible changes is the multichannel 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. As use of the Internet continues to grow, so does the sophistication and resolve of these attacks.
**Tamil daily, individuals, businesses and governments are exchanging data at ever-increasing speed. Everyone needs digital security. But there are two sides to the digital security equation:**

> **People:** who want to access a service of some kind, using any device. To do that, they’ll need a digital ID.

> **Service providers:** who need to check that the ID is valid – and manage and protect the data in their care.

To trust each other, these two sides need to be linked by a continuous chain of security. Our purpose is to design solutions that enable our clients to bring trusted and convenient digital services to billions of people.

The ability to prove that we are who we say we are is a strategic imperative. A step further is our identity. "Identity" is in essence the link connecting the individual to the community as a whole. Protecting identity against fraud or theft is the key to maintaining confidence in this union. **The big challenge is to ensure a requisite degree of match between an online identity and a real identity:** in other words, its uniqueness. Establishing identity and secure access to services is brought about both by an authentication process and an identification process (verifying the identity of the person). Together they give this person rights or access to circles of trust and services.

---

**Government - Building the framework**

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. Public sector organizations and agencies are therefore deploying national trusted identity schemes to not only streamline services and processes in areas such as social services, tax, local voting, democracy and administration, but also foster secure private services and boost the digital economy while reducing costs.

Secure, efficient, accessible and trusted government services are also enabling citizens to contribute more effectively to public decision-making and to participate more directly in public life.

---

*Source: Secure Identity Alliance*
COESYS eGov: digital security enables trusted interactions

**Identity Providers** are responsible for authenticating individuals and issuing assertions about them, on behalf of the relying party. They could also provide the identity of individuals.

Identity Provider a **key Role in the digital identity ecosystem**

- Trust
- Convenience
- Privacy

**Identity Provider**

> Reduce fraud
> Increase usage
> Reduce cost

**Authentication - Identity-Attributes**

**PEOPLE**
Want to access to services and need to use a digital ID

**SERVICES PROVIDERS**
Need to check the ID is valid - and to manage & protect the data they care.

Delegates authentication of an individual and transaction authorisation

Coesys operates at the level of the identity provider and/or authentication operator. In essence, the identity provider runs the end-user authentication and/or the identity services in a secure manner on behalf of the service provider[s] running the government services. The solution enables multi-channel access via PC, mobile, smart phone, tablet etc.

Coesys eGov solution and the Identity value chain

The identity provider could interact with, or fulfill the roles of, attributes providers and/or identity brokers. The identity provider is responsible for managing identities, or running the federation services and authenticating the public or private service providers delegated to it.
Key benefits

What it brings:
- Convenience: Federation services - SSO
- Digital security: strong authentication and digital signature - certificate- and public-key-based
- Ready to integrate in any national identity scheme (CA, SPs, attributes providers etc), based on standards

Key eGov differentiators:
- Modular and flexible architecture to easily integrate to existing authentication systems and infrastructure (certificate authorities, attributes providers, service providers, HSM etc)
- Future proof: standards-based such as SAML, Open ID Connect, OAuth, Oasis DSS etc
- SConnect is easy to deploy and maintain, supports any kind of smart card
- Neutral approach through support for any authentication method
- Simplifies cross border transactions
- Ready to leverage new identity initiatives such as national identity schemes, Mobile Connect etc

Coesys eGov: Federation, Authentication and Signature

Main features
Federation services
> SSO (SAML and OpenID Connect)
> Service provider management
Adaptable trust level
> Assurance level definition
> Step up authentication
Strong authentication (2nd factor)
> eID PKI, Mobile PKI
> Connectors to 3rd party (OTP etc)

Digital Signature
> Card-based signature
> Server signing
> ETSI formats – OASIS DSS

SConnect™
Server-based universal browser plug-in connected to PCSC card reader

MyMobileID
Mobile application - OOB

Privacy
> eIDAS - Pseudo, Persona, User attributes consent
Coesys adaptable trust level of assurance

Based on risk management, Coesys eGov enables an adaptive and step up level of assurance from Level of Assurance (LOA) 1 to LOA 4, providing a very flexible approach for service providers. Depending on the service concerned, the risk and sensitivity of the data will vary: accessing general information does not require strong authentication, but accessing personal medical personal data, signing an online contract or registering a birth requires the highest LOA.

Coesys Federation Services and Single-Sign-On (or SSO as it is sometimes abbreviated) refers to a system where the user is authenticated once, then granted access to multiple resources without entering their authentication credentials again. This is particularly popular with consumers who do not want to remember multiple login credentials or prefer the convenience of having their credentials automatically transferred to requesting service providers. Federated login technologies, such as SAML and OpenIDConnect, have gained in popularity.

It enables easy integration of service providers. Service providers need to know the user identity [not necessarily the real id; a pseudonym is sufficient to link the user to the account named user principal]. They also need to know some information for authorization: the group the user is in, billing information, and post address named user attributes. Coesys eGov provides service providers with capabilities such as:

- selection of authentication method [each service provider needs a different level of security – the level is set by internal policy - can affect user experience (e.g. some methods need more time)]
- definition of the level of assurance [some credentials are more reliable than others (National ID, user PKI card) - strength of authentication should be managed on the credentials level, not the method level]

Level of Assurance

Level of Assurance (LOA) in an authentication system is a measure of confidence that the authentication is done in a manner consistent with the security guidelines. Although many organizations define their own matrix for LOA, it is best to use the guidelines provided by standards or by industry or government organizations. For example, NIST Special Publication 800-63-1 addresses the Electronic Authentication Guideline, and defines the following four levels of assurance for authentication systems. Complementary to this, the eIDAS initiative in Europe for boosting electronic transactions defines three levels.

Levels of Assurance in Authentication Systems
Coesys Strong Authentication services or Multi-Factor Authentication (MFA) imply the use of two or more distinct and separate authentication credentials. Strong Authentication or Multi-Factor Authentication implies the use of two or more distinct and separate authentication credentials (2FA). Asking for two credentials from the same class of factor is not considered Multi-Factor Authentication. For example, asking for a password and the answer to a security question is not Multi-Factor Authentication: it is a simple factor repeated twice and therefore vulnerable to the same attacks.

Coesys eGov provides a unique set of strong authentication solutions based on smart cards, OTP (One Time Passwords), fingerprints etc. In order to provide the highest level of assurance needed in a governmental ecosystem, the solution has been designed to offer different public key infrastructure (PKI) based methods using Mobile PKI or eIDPKI.

> Based on public key infrastructure / certificate with public key signed by certification authority
> Signature of random data by the private key – proof that user possesses the private key
> Strength can depend on protection of the private key – crypto token (smart card, usb token, hardware secure module)

Privacy

The desire and ability of individuals to withhold certain parts of their personal information from wider society is growing stronger and stronger. People would like to manage their personal information and attributes by giving consent or having the option not to disclose it.

> Persona management: The user wants to disclose as little information about themselves as possible. Their identity needs to be hidden for some services [e.g. access to email does not require knowledge of real name]. Choice of identity after authentication.
> Pseudonym: User does not want to have the same username for all services. That would allow tracking of their activities
> User attributes: User wants to send attributes only to selected service providers – attributes are filtered before sending.

Coesys Digital Signature services allow citizens to sign transactions and documents.

> From smart card-based signature up to server-based solutions
> SWYS : Sign What You see
> ETSI : Cades, Pades, Xades

SConnectTM is a unique smard card connectivity solution

SConnect is a cross-browser and cross-platform technology solution that allows web applications and services to connect to smart cards and to use security services provided by these cards without the need to install and maintain software on the end-user PC.

For citizens this is an easy to use Plug & Play solution with a simple User Interface (UI) that requires no installation process. The user can immediately use his or her eID. SConnect is a universal plug-in enabling installation of the middleware on the server. OS and browser agnostic, it is extremely easy for governments to deploy and maintain and ready to use on all types of user machines. There are no setup requirements or need for pre-installed software on the end-user PC. It is also highly interoperable and flexible as it supports multi-card functionality with seamless upgrade for new cards.
A secure digital mobile lifestyle: from e-ID towards Mobile ID

From Multiple Digital Identity to One trusted Digital ID

My Mobile ID mobile application
Coesys mGov enables citizens to use their phones as an authentication and signature tool. This state-of-the-art mobile application uses a combination of contactless national eID card and NFC phone. Credentials can be stored in any Secured Element.

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.

In addition, the level of assurance can be adapted according to the nature of the online services being accessed.

Mobile Identity Ecosystem
A number of pioneering countries are already tackling the challenge of Mobile Identities (m-ID). For some, the answer lies in operator level approaches. For others, it is rooted in the existing physical and digital identities created by government. Whatever the approach, the most successful m-ID services already launched are highly dependent on collaboration between public authorities, banks, telecom operators and the private sector. The first key success factor is the role of government in creating a trusted framework. The second is to provide user protection when utilizing online services.
Coesys mGov Solutions

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.

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
**MyMobileID application**

MyMobileID is an app which communicates with Coesys mGov 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.

**Coesys mGov Derived Credentials services**

The implementation of mobile ID authentication according to the requested LOA is possible through several methods: e-ID card + NFC, or e-ID embedded in a secure manner in the phone. However, given the two billion e-ID smart cards already deployed, we believe that the card + NFC + mobile equipment approach is probably the one that will generate the fastest take-up, offering both the strongest level of security and optimum ease-of-use.

To further simplify the user experience, Gemalto’s Mobile ID solutions such as Coesys mGov support the creation of Derived Credentials on the SIM card itself, 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.

**Derive Mobile ID from ID card**

Option 1: Creation of Derived Credentials via Server

Option 2: Creation of Derived Credentials locally

ID derivation requires user authentication

Secure Element API

Provisioning App

ID card

NFC

Connection to eGov online services
Coesys Out of Band service

Out of Band (OOB) is a dedicated authentication method for mobile. Out of Band authentication is the use of two separate networks working simultaneously to authenticate a user. It is a type of two-factor authentication that requires a secondary verification method through a separate communication channel, along with the typical ID and password.

For example, if a user connects to an Internet portal through a web browser running on a PC, the out-of-band channel can be through the user’s cell phone.

STANDARDS

> Authentication:
  • SAML 2.0
  • OAuth 2.0
  • OpenID Connect

> Digital signature:
  • PAdES, CAdES, XAdES
  • Timestamping
  • OASIS DSS
  • Participated in ETSI plug tests

> Other Standards:
  • X.509
  • LDAP
  • PKCS#1 PKCS#7
  • XMLdSIG
As of 2014, Gemalto’s Mobile ID solution is enabling all mobile users in Iceland to use strong authentication and legally-binding signatures that are essential to securing banking and eGovernment services.

A trusted authority in eGovernment applications

Gemalto has extensive experience in the public sector, having contributed to more than 100 national government programs worldwide. These include passport, national ID, e-ID and mobile ID, residence permit, driver’s license and healthcare initiatives and solutions to modernize eGov services including project management.

User-friendly eGovernment services even more inclusive

Gemalto’s Coesys eGov, enabling strong authentication, centralized signature and identity federation, is now the basis of several national eGovernment infrastructures.

For example, Qatar authorities introduced Gemalto’s infrastructure for eGovernment services in 2014. Users can now digitally sign documents or application forms before submitting them, by using their eID with a 6 digit PIN code.

The solution also makes the user interface as simple as possible. A mouse click at connection activates the secure authentication process. Once connected, the user can access any of the various online services thanks to Single Sign on. Citizens have rapidly adopted this new tool and calls to the help desk have visibly dropped.

Winning hearts and minds

Mobile ID is transforming the Finnish eID scheme into a mobile success story by delivering a comprehensive mobile PKI platform to the leading Finnish MNOs.

Rollout of the mobile PKI and PKI SIM cards begun at the end of 2011 and every mobile phone user has the option of activating an eID credential for their mobile phone.

Moldova is introducing an innovative range of mobile-based eGovernment services called Mobile ID. This program offers citizens the speed, privacy, convenience and transparency of digital access to numerous government services and information sources, including online applications and copies of official documents. They will be able to confirm their identity and sign documents directly from their mobile phone by entering a unique PIN that they can choose themselves.

Gemalto is providing Orange (which has more than 50% of the country’s mobile subscribers) with an end-to-end solution that is compatible with all types of mobile phones – not just smartphones – and that will offer its subscribers in Moldova seamless access to Mobile ID.

Citizens and residents of Oman can securely access eGovernment services. Acting as a turnkey solution provider and systems integrator, Gemalto is delivering the complete Coesys eGov2.0 software suite together with related services including training, support and maintenance. The full solution encompasses strong authentication and digital signature using the Omani eID card.

As of 2014, Gemalto’s Mobile ID solution is enabling all mobile users in Iceland to use strong authentication and legally-binding signatures that are essential to securing banking and eGovernment services.
ABOUT GEMALTO

Gemalto is the world leader in digital security with 2014 revenues of €2.5 billion.

In the public sector, Gemalto provides secure documents, robust identity solutions and services for governments, national printers and integrators in the service of citizens. Its products and solutions are deployed in more than 100 government programs worldwide.

Leveraging on its Valimo Wireless activities, Gemalto is the leading solution provider for mobile user authentication and digital signatures with over 20 ongoing mobile Identity projects and enabling millions of mobile users to start accessing government services with enhanced security. Among those projects, 8 are used specifically in national eID schemes to secure the access to eGovernment services.

Our contribution to these projects provides us with an excellent overview of the technology involved, its applications and the quality of information systems, as well as the social context of its use. Gemalto also collaborates with its clients to report and share best practices from around the world.