Coesys eGovernment Authentication Gateway

For secure, accessible and trusted eGovernment services

FINANCIAL SERVICES & RETAIL
ENTERPRISE
INTERNET CONTENT PROVIDERS
PUBLIC SECTOR & TRANSPORT>SOLUTIONS
TELECOMMUNICATIONS
eGovernment framework

Governments around the world are seeking to boost efficiency and transparency in many essential functions aiming to better serve their citizens in a reliable, secure and transparent way. Public Sector organizations and agencies are thus deploying electronic infrastructures to streamline services and processes in such areas as Social services, Tax services, local Democracy & Administration services, but also fostering secure private services.

Secure, efficient, accessible and trusted eGovernment services are also enabling citizens to contribute more effectively in public decision-making and to participate more directly in public life. Broader collaboration between members of the public and governments could ultimately yield smarter policies and greater social cohesion.

To get these benefits, eGovernment services must first be implemented or deployed. Here are some obstacles and challenges to full implementation:

- Not everyone has adequate access to the Internet.
- To be widely used, eGovernment services must offer a reliable and secure access to private information. In short, people must trust the service. This is the lesson we learnt from our customers. This is the challenge we address with our solution.
- There are legal, administrative, social, and political hurdles to be overcome as well.

Requirement For A Common Authentication to Public Services and Information

As several surveys on eGovernment initiatives in different countries around the globe demonstrate, many countries already provide information and access points to their administrations. Many are now considering the need for a single integrated harmonized access point to public services and information and even for some private services as well: so called one-stop government portal. One-stop government portal refers to the integration of public services from a user’s - any customer of public services - point of view. It allows citizens, businesses and other authorities to have 24 hours access to public services from their home, their offices or even on the move.

A lack of trust among citizens, businesses and public administration in the security of Internet communications could jeopardize electronic markets and the social modernization effects that go hand in hand with electronic communications.

A strong User Authentication Needed as well

Trust is certainly the keystone of success for such services and applications to be widely used. Authentication and a set of standards for determining identity are major tools to achieve this goal. It is a way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so. Such authentication service enables personal and non-anonymous access to e-Gov web services.

European Parliament voted as early as 1999 a directive on Electronic Signature giving electronic signature momentum. It has given the necessary initial conditions for deployment of products & systems to market.

Granularity is a key part of authentication. Different applications require different levels of security, which need to be defined through business policies. Potentially, a user will present a credential — a password, certificate, smart card or token — to access to the appropriate applications.

Basic user's personal medical file, to digitally sign tax declaration services or officially ask for a specific personal administrative request.

The validity of online user signature requires first strong user authentication while keeping user's friendly experience.

To declare annual tax or get access to personal medical file requires user to be authenticated first. Considering the associated impact and level of security threats on the Internet, there is a need for solutions based on Public Key Infrastructure. Passwords policies are no longer secure enough to access information or make official transactions.

Coesys eGovernment Authentication Gateway

Coesys eGovernment Authentication Gateway provides strong user-authentication, by securely verifying the identity of a person who is attempting to gain access to a web-based resource, and that all communication actually comes from that person.

The person subject to authentication is using his/her personal ID card (in the form of a Smart Card ID) to access a dedicated web resource, typically to access private medical data of the user's personal medical file, to digitally sign tax declaration services or officially ask for a specific personal administrative request.

Such solution provides a solid foundation for providing online value-added services through smart cards, in areas such as Healthcare, eGov portals, Tax declaration, on line education portals, to name a few.

The Coesys eGovernment Authentication Gateway Suite

The Coesys eGovernment Authentication Gateway suite contains the following products:

- eGovernment Authentication Server (GAS)
- eGovernment Authentication Module (GAM)
- eGovernment Authentication Gateway (GAG)
- eGovernment Authentication Client (GAC)
Coeyes eGovernment Authentication Server

The Coeyes eGovernment Authentication Server (GAS) is a standalone server software that performs authentication of users attempting to access eGovernment services with their smart card ID.

GAS uses a challenge-response protocol to authenticate users accessing a resource. This data will be used during the authentication process in order to verify the identity of the user.

An overview of the GAS operation is illustrated in the figure 1 diagram.

Optionally control databases that currently interface with GAS are:

- Lightweight Directory Access Protocol (LDAP)
- SQL
- MS Active Directory
- Text file

An API is also provided, which allows third party database products to be interfaced with the GAS.

A powerful feature within the Coeyes eGovernment Authentication system is that of “inter-domain authentication”. This refers to the ability for one GAS to authenticate servers from more than one domain. An example of this is illustrated in the figure 2 diagram.

The owner of domain A.com is a partner of the domains B.com and C.com. Users on B.com can be redirected to the GAS located at A.com, in order to receive a credential that allows them to access resources on B.com. Furthermore, if users attempt to access resources on C.com they are redirected to A.com where they can receive a valid credential for this domain as well. However, users of D.com cannot access resources on A.com, as they are not trusted by the GAS located there. This feature provides reliable user security across the Internet.

It is also possible to implement Single-Sign-On (SSO) functionality amongst separate domains, enabling users to roam from site to site without the need to re-authenticate each time.

Coeyes eGovernment Authentication Module

The Coeyes eGovernment Authentication Module (GAM) is a software component that integrates easily with a web application server in order to protect it against unauthorized access. It acts as a gatekeeper for the web application server by verifying that each user-request to access a resource on that particular server possesses the credentials necessary to do so. If a user does not have the credentials necessary to view the resource, the GAM re-directs him/her to the GAS in order to attain the proper credentials by authenticating with his/her smart card.
The GAM is compatible with the most important subset of web application servers including, Apache Web Server, Microsoft IIS and iPlanet/Netscape Web Server.

**Coesys eGovernment Authentication Access Gateway**

The Coesys eGovernment Authentication Access Gateway (GAG) secures web portals and PKI-enables existing legacy applications. It is a high performing SSL gateway with extended PKI (public key infrastructure) capabilities that can be used by any client-server application to achieve strong encryption, revocation control and PKI-based access control.

Coesys eGovernment Authentication Access Gateway is based on an implementation of the TLS/SSL (Secure Socket Layer) protocol that is a global de facto standard for network encryption, and also the most frequently used security solution for Internet commerce. It provides a platform for a generic SSL server side tunnel that can be applied to any static TCP-protocol, such as HTTP, Telnet, POP3 and ICA.

The GAG is an alternative to the Coesys eGovernment Authentication Module.

**Coesys eGovernment Authentication Client**

The GAC is browser-based client software that performs the vital functionality of providing the cardholder with an interface to the Coesys eGovernment Authentication Gateway back-end system.

The GAC performs the functions of prompting for and validating user input, providing status information, and card data retrieval.

The client also acts as an intermediate between the user’s card and the rest of the Coesys eGovernment Authentication Gateway system, by retrieving the relevant credential information needed for authentication and then relaying this data back to the correct source inside the system.

The GAC is compatible with the major Internet browsers on the market including Microsoft Internet Explorer, Netscape Navigator.

The GAC is a very flexible product where all user interfaces are customizable for every identity provider – authentication server (GAS).

The GAC has a built in Web Update function that keeps the product update after installation in an effortless way.
Authentication within Coesys eGovernment Authentication Gateway

One of the main premises in Coesys Gateway is the notion of the authentication method.

An authentication method refers to the procedure involved in verifying an end-user's identity. It entails the sequence of events that must be performed in order for a person to prove that he or she is who they claim to be. The authentication method defines what is required for a successful entry, and thus who is allowed access and who is not.

In the Coesys eGovernment Authentication Gateway system there are currently 8 authentication methods available. A combination of one or more of these authentication methods can be used to control access to protected resources. Below we will describe the most relevant authentication methods for public sector business.

Many parameters have to be considered when determining what authentication method is best suited for a particular system.

Generic Form Username/Password Authentication

This is the simplest form of authentication in the Coesys eGovernment Authentication Gateway system, and does not require a smart card in that case. The client provides the user with a browser-based form into which they must enter their Username/Password credentials. The GAS validates these credentials; if correct the user is successfully authenticated, if not he/she is informed that one of the credentials entered is incorrect or invalid.

Smart Card Based Username/Password Authentication

This method of authentication makes use of the Public Key Infrastructure (PKI) to validate a user's identity. During card personalization, keys are stored on the card in the form of a certificate and corresponding private key.

During authentication:
• The Username/Password credentials are stored onboard a smart card. In order to gain entry to the system the user must insert his/her registered smart card into a valid reader.
• Access to this card is protected by a PIN (Personal Identification Number). The user is prompted to enter this PIN by the GAC.
• If the PIN is successfully entered the GAC accesses the Username/Password attributes on the card. If not, the GAC prompts the user to re-enter the PIN. The user has a configurable number of attempts to enter the correct PIN, after that the card is blocked.
• Username and Password are then validated by the GAS. If successfully validated the user gains access to the system, if unsuccessful the user is informed.

Smart Card Based Public Key Infrastructure Authentication

This method of authentication makes use of the Public Key Infrastructure (PKI) to validate a user's identity. During card personalization, keys are stored on the card in the form of a certificate and corresponding private key.

During authentication:
• The user inserts his/her registered smart card into a valid reader.
• The GAC prompts the user to enter a PIN in order to allow access to the card. If the PIN is correct the application is allowed access, otherwise the user is informed that they have entered an incorrect PIN.
• During authentication processing the GAS signs a random piece of data using S/MIME and sends both this data and the signature to the GAC as the challenge.
• The GAC formats and sends this data to the smart card. Once this data is validated onboard the card, the challenge is then signed and this signature sent back to the GAS via the GAC along with the certificate (public key) and the original GAS challenge.
• The GAS recalculates the signatures to ensure they are correct. The GAS also has the ability to perform external 3rd party checks on the certificate (public key) such as OCSP, CRL, etc.
• If verification is successful the user is allowed access. If not the user is informed that the attempt has been unsuccessful.
Coesys eGovernment Authentication Gateway is a mature product. It consists of individual components that have been groomed and refined so that they perform their individual tasks with efficiency and accuracy.

The modular structure of Coesys eGovernment Authentication Gateway makes it flexible and easy to configure inside an existing system infrastructure, thus reducing downtime and increasing productivity and profitability.

Why Gemalto?

Gemalto is a reliable and trusted partner for all your public sector ID initiatives including ePassports, eVisas and other international and national identification schemes as well as healthcare and social security programs.

We offer a complete range of secure solutions that are tailored to local markets, and we deliver what you want where you want it with the support of a strong network of local partners.

- Our Sealys Secure Documents offer physical, visual & electronic security for travel documents, eIDs and eVisas. These innovative products are designed with durability and security in mind. With over 10 FIPS140 certificates and 50 Common Criteria certificates we meet the most stringent international certification for highly secure applications.

- Our Coesys Secure Solutions - such as Coesys eGovernment Authentication Gateway - are designed to be YOUR turn-key solution. They are evolutionary and serviced by local support teams.

And because we know the success of your project does not rely on products and solutions alone, we offer you our Allynis Secure Services for operational excellence and financial & industrial engineering.

Gemalto in brief

Gemalto is a leader in digital security with pro forma 2006 annual revenues of €1.7 billion, operations in about 100 countries and over 10,000 employees including 1,500 R&D engineers.

Gemalto was formed in June 2006 by the combination of Axalto and Gemplus.

In the public sector, Gemalto aims to make each interaction between citizens and public sector organizations and agencies more secure, easier and private. Security, durability, reliability of exchanges and the protection of citizen’s privacy are non-negotiable when it comes to digital identity.

Gemalto supports key identity applications in the public sector such as ePassports, eVisas and other international and national identification initiatives as well as in healthcare and social security. Gemalto serves the market with secure documents, solutions and managed services, covering authentication, enrolment, issuance and complementary applications.

Our solutions are tailored to local markets in partnership with local players.

Our considerable practical experience - in major ePassport and eID card projects; some of the world’s biggest eHealthcare programs; and numerous driving license, vehicle registration and tachograph projects – is at your service.