thalesgroup.com

THALES
Building a future we can all trust

Thales Gemalto
Confirm Authentication Server

Security with a flexible architecture enabling a seamless deployment in any bank's IT infrastructure - preventing eBanking user credential security breaches and supporting the widest range of authentication and signing methods in the industry.

Thales Gemalto Confirm Authentication Server

Security with a flexible architecture enabling a seamless deployment in any bank's IT infrastructure - preventing eBanking user credential security breaches and supporting the widest range of authentication and signing methods in the industry

Banking & Payment Services

Thales is the world leader in Digital Security, and a key supplier of products and services, e.g. mobile solutions, fraud management, smart cards and readers, personalisation, tokens and secured browser to banks everywhere. Our Thales Gemalto Confirm Authentication Server is the heart of the world's most versatile, scalable and secure authentication solution dedicated to protect eBanking, eCommerce and mBanking.

The Thales Gemalto Confirm Authentication Server is a field-proven authentication solution designed to enhance online banking services, support the launch of new services and provide a convenient user-experience - fully committed to offer flexible, secure and easy deployments.

Open eBanking security solution

In an environment of constant change and increased fraud attacks, banks need a security solution that is adaptive and reacts to market changes. A strong, comprehensive, scalable and cost-effective solution that allows freedom of choice - without compromising on the security, speed of deployment and convenience offered to end-users.

The Gemalto Confirm Authentication Server is the natural starting point of any eBanking security set-up. Highly customisable, it allows banks to combine different authentication schemes with all many types of software and hardware tokens - enabling secure authentication and consistent user-experience across various types of online banking channels.

This server supports both standard multi-factor authentication such as One Time Passwords (OTP) and Challenge/Response, and more advanced transaction verification and signing methods such as EMV/ CAP/ DPA, OATH and OCRA and the Thales Gemalto patented Dynamic Signature technology.

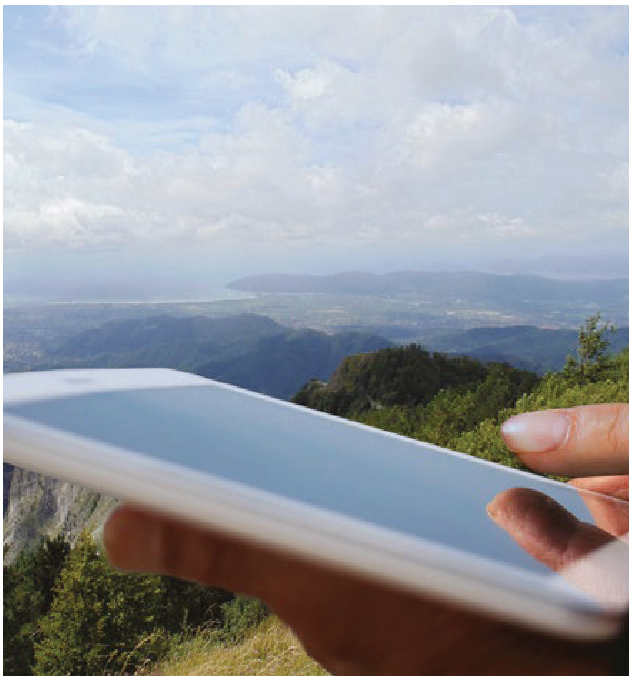
A field proven server

The Gemalto Confirm Authentication Server authenticates millions of online banking and eCommerce users every day, authorises remote access and internet transactions and protects sensitive data from fraudulent online attacks.

Various devices can be used, in combination, to provide a secure, yet flexible authentication realm. This allows banks to issue different tokens - all being authenticated with the same server.

Multi-tenant ready architecture, multi devices

A key benefit of the Thales Gemalto CAS is that it allows banks to pick and mix from our selection of channels and installations — from eBanking, mBanking, phone banking and from eCommerce to eBroker or multi-tenant setups. Or even as an Authentication-as-a-Service setup.



Thales Gemalto Confirm Authentication Server

Key features

Identity Assurance and Access Control

- Strong 2FA of OTP
- Multi-Tenant Ready Architecture
- Comprehensive audit logging and reporting
- Clustering and load balancers support for high-availability and disaster recovery
- Application firewalls support
- Centralised web-based administration for managing the system

OS

- Red Hat Linux
- Windows Server

A flexible solution supporting open standards

- Directory Access Protocol (LDAP)
- Remote authentication dial-in user service (RADIUS)
- Initiative for Open Authentication (OATH)
- OpenID Connect / OAuth2

Authentication & signing methods

- OATH, OCRA (Event based, Time based)
- EMV CAP
- OATH Dynamic Code Verification
- Dynamic signature enhancements

Authentication & signing form factors

- Supports a wide range of 2FA tokens, both hardware and software
- Mobile Based Authentication
  - SMS OTP
  - Mobile Token
  - Mobile Out-of-Band (Push Notifications)
- OTP Tokens
  - QR Token
  - 1 button
  - PinPad
- EMV CAP readers
  - Connected or unconnected
- Dynamic CV cards and mobile

Webserver

- Apache Tomcat
- IBM WebSphere
- The chosen architecture allows "High Availability" and "Fail-Over" configuration relying on operating systems, databases and monitoring mechanisms.

Databases

CAS stores OTP related data and User data if needed (DB mode) in:

- Oracle
- MySQL
- IBM DB2
- MS SQL

User repository

CAS can be connected to the following LDAP when users' accounts are managed externally (Mixed mode):

- Microsoft Active Directory
- Novell eDirectory
- Open LDAP
- Any other LDAP could be supported through a specific development

Authentication services interface

- Web Service REST API
- RADIUS requests:
  - Microsoft NPS
  - FreeRADIUS
- AD FS

Security models

- SafeNet Network HSM
- SafeNet PCI-E HSM
- SafeNet Payment HSM
- Thales PayShield
- Thales nShield
- Software Security Module

Performance

- One Gemalto CAS node supports 400 OCRA transactions per second

Thales Gemalto Confirm Authentication Server

Thanks to its unique flexibility and the ability to support several authentication devices and solutions simultaneously, the Gemalto Confirm Authentication Server allows you to easily segment your customer base to support different customer needs. It allows banks to assign different kind of security devices for different use cases based on risk profile, usage pattern and preferences.

The server platform includes all components needed to deploy strong authentication for banks with a low total cost of ownership. This is realised through packaged plug and play solutions that are adaptable to existing networks and AAA servers and built according to open OATH standards and CAP.

The Gemalto Confirm Authentication Server offers the highest level of security for two-factor authentication. You can choose from a wide range of connected or unconnected form factors including payment cards, tokens, and mobile OTP.

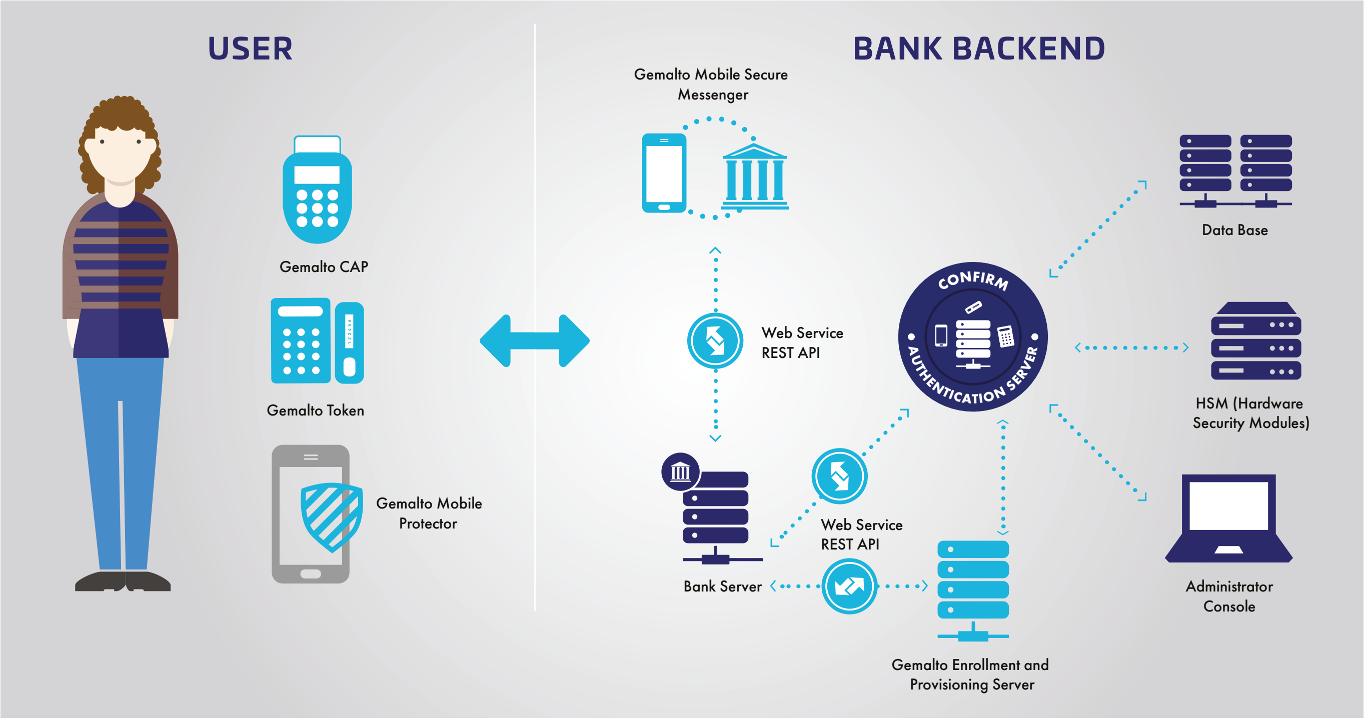
Admin and User features are available through Web Service REST API. It allows banks easy integration in their existing portal, further admin and user features.

This server works with multiple operating systems and server configurations and modules support industry standard protocols for seamless integration with existing bank architectures.

To provide the most advanced level of user identity protection, the software security module or an external hardware security module (HSM) is linked to an authentication server to store and use cryptographic keys. Using standard frameworks and protocols such as HTTP/HTTPS, authentication modules interact with existing data servers to maintain and update user authentication information. Multiple database options are supported.

Our software solutions are open, scalable and evolutive and support either an on-premise or cloud deployment model.

> **With the Gemalto Confirm Authentication Server as your authentication solution you can secure your current investment as well as technology roadmap for the future.**


USER
Gemalto CAP
Gemalto Token
Gemalto Mobile Protector
BANK BACKEND
Gemalto Mobile Secure Messenger
Web Service REST API
CONFIRM AUTHENTICATION SERVER
Data Base
HSM (Hardware Security Modules)
Administrator Console
Bank Server
Web Service REST API
Gemalto Enrollment and Provisioning Server