

Ezio Strong Authentication Server for e-Banking Services

||||| A comprehensive and powerful authentication solution



FINANCIAL SERVICES & RETAIL > OFFER

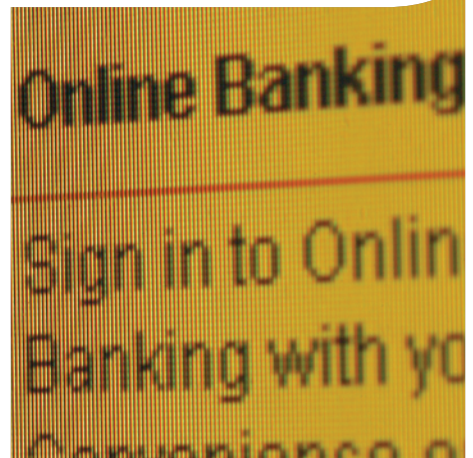
ENTERPRISE

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

Ezio Strong Authentication Server

||||| Protecting your online business through flexible, standard and convenient security

Enhanced security with two-factor user authentication

Whenever consumers access online banking services, they want to feel confident that their identity credentials and their financial information are protected. On the other hand, as a bank, you need to be certain of the identity of the customer logging on or signing transactions. One-time password devices answer these requests. To automatically check and validate that these passwords are correct and have never been used before, you need an expert you can trust: Ezio SA server.

A single server to manage the authentication, easy to deploy, and highly scalable

According to market segmentation, different e-Banking applications may require different authentication methods (e.g. smart cards, tokens or SMS-OTP). Ezio SA Server can manage each of them simultaneously, whatever their number of users, and even when that number evolves through time, up to millions.

Main benefits of CAP/DPA OTP with Ezio SA Server

Thanks to Gemalto large experience in EMV cards, Ezio SA Server fully implements the last releases of MasterCard CAP and Visa DPA specifications. It gives financial institutions the flexibility to adapt the security level they want to account access and transactions:

- Simple OTP
- Challenge / response
- Transaction signature

> In addition, Ezio SA Server:

- Manages concurrently all types of banking cards that the bank may have
- Manages authentication for accounts using several different banking cards
- Secures sensitive data in accordance with payment card industry security standards, using one or more HSMs for cryptographic functions



Without any software installation for the end-users, Ezio SA Server supports various devices based on standards: (MasterCard CAP and PLA/AA4C, VISA DPA, HOTP and TOTP OATH)

- **EMV Banking cards:** The OTP is generated by the end user's banking card, using a standalone generic reader
- **Time Token:** The OTP is generated by a dedicated device. To minimize the threat of phishing, the OTP generated is only valid for one attempt and during 30 seconds
- **Mobile phone:** the OTP is sent in a SMS or computed by the SIM card and displayed by the mobile phone

EZIO SA Server offers full administration capabilities

- Management of users, devices, security policies
- Management of user role and permissions
- Audit of authentications and all other operations in database
- Events reporting
- Data provisioning tools using batch files
- Web admin portal
- Self service portal

Technical specifications

- Operating systems:
- Windows® 2003
- Linux Red Hat release 4
- IBM AIX 5.X

> Database:

- MS SQL 2005
- IBM DB2 UDB 9.1
- Oracle 9i and 10g

> HSM:

- nCipher Payshield
- Bull Cryptopay
- Thales HSM 8000
- Others on demand

> Authentication and administration interface:

- XML over HTTP(s) API

> Application server:

- Tomcat Apache
- IBM Websphere

