



Two-Factor Authentication for Banking

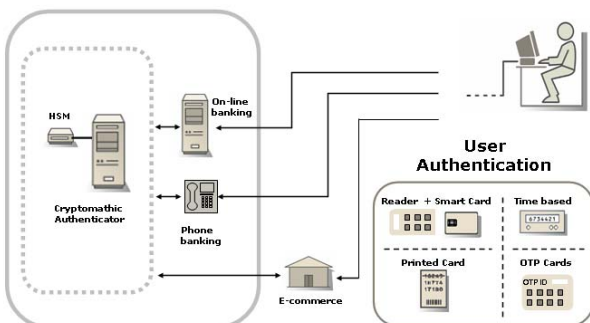
Banks worldwide have embraced Internet and phone banking for business, corporate and retail use, allowing them to reduce costs and serve customers better. However, attacks on banking websites have proliferated, and are now an established criminal technique. These attacks include phishing, pharming, PC trojans and man-in-the-middle. Improved customer authentication has been widely accepted as a necessary investment in order to prevent these attacks and preserve customer trust.

System Architecture

The Cryptomathic Authenticator is an authentication server designed specifically for banking applications. It is an ideal platform for providing strong, two-factor authentication. Authentication methods include one-time-password tokens, card-and-reader tokens (including MasterCard CAP / VISA), paper-based TAN lists and SMS, as well as traditional static passwords.

The Authenticator is designed for simple integration with both banking applications and customer management systems. The architecture and interfaces are designed to minimise modification to legacy systems. In addition, by taking responsibility for all customer authentication, application development is simplified and the overall system security improved.

Secure Multi-Channel Banking



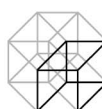
Cryptomathic Authenticator

Best-practice banking security is provided by the use of hardware security modules (HSMs) to protect cryptographic keys and all authentication data. Administrative controls include chip-card log-on, separation of duties and dual controls.

As part of a bank's live environment, the Authenticator supports fail-over and clustering to provide redundancy and scalability. The system is highly optimised for performance, and is able to support very large customer bases and high throughput.

Cryptomathic partners with leading token vendors and HSM providers, but the Authenticator product itself remains independent of any specific vendor. Coupled with the wide range of authentication mechanisms, this provides the flexibility to adapt to future banking authentication requirements.

Cryptomathic Authenticator is a one-stop solution providing a complete package consisting of, server software, HSMs, installation, training, maintenance & support. This ensures a short time to market to address new security threats or other market drivers.



Technical Specifications

Application Architecture

- Multiple servers
- Multiple HSMs
- Simple integration
- Remote administration
- Application-level clustering
- High availability

Security Architecture

- AES protected network communication
- Access control via smart cards
- Secure environment using HSMs
- Tamper evident audit log of all events
- Dual controls for sensitive / critical commands
- Flexible role-based separation of duties

Authentication Architecture

- Integration into multiple channels (on-line banking, phone banking, e-commerce)
- Multiple authentication mechanisms in parallel
- Configuration of validation parameters

Authentication Methods

- Grid cards
- MasterCard CAP
- Visa dynamic passcode authentication
- SMS
- Static passwords
- TAN cards
- Vasco Digipass
- Modular architecture - new methods available

Operating Environment

- Microsoft Windows Server 2003

Database

- Oracle 8i and 9i
- Microsoft SQL 2000

Hardware Security Modules

- Eracom ProtectServer Orange (validated to FIPS 140-1 level 3)
- nCipher nShield F3 (validated to FIPS level 140-2 level 3)
- nCipher netHSM (validated to FIPS level 140-2 level 3)
- HSM specific firmware
- Software crypto available (no HSM)

Independent Future Proof Solution

The Authenticator is an independent solution for a number of reasons. Firstly, it is independent of token vendor suppliers so banks are not tied to any particular authentication vendors or technologies when choosing the Authenticator. The same level of independence applies to HSMs (Hardware Security Modules), allowing the Authenticator to support banks' preferred HSM brands and models.

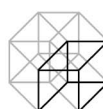
Through a wide and growing range of user and transaction authentication methods, the Authenticator is able to adapt to future requirements, safeguarding the value of the initial investment.



About Cryptomathic

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With almost 20 years of experience, we have assisted our customers by providing systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing, and advanced key management through best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with its established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

www.cryptomathic.com



CRYPTOMATHIC
www.cryptomathic.com