



MULTI-CHANNEL TWO-FACTOR

Financial institutions and other worldwide on-line service providers have embraced multiple interface channels, such as internet and mobile banking, for business, corporate and retail use, allowing them to reduce costs and better service their customers. 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

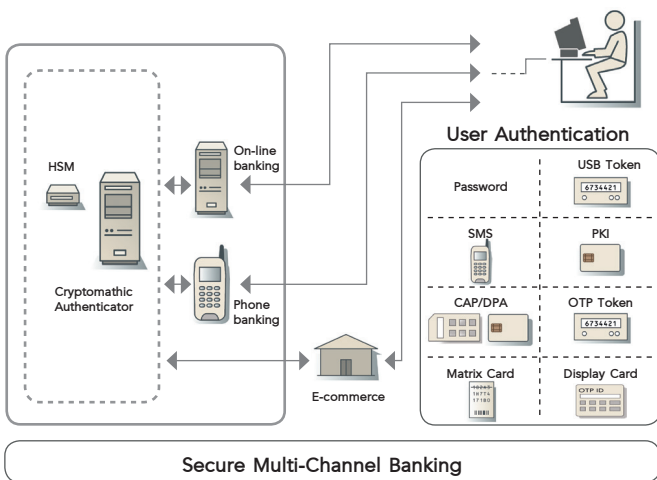
The Cryptomathic Authenticator is a server solution designed to act as an integrated service to compliment any remote user interface where strong authentication is a must. As such it is especially suited to banking and eGovernment applications or any other platform for providing strong, two-factor authentication. Authentication methods include one-time-password tokens (including the OATH HOTP algorithm), MasterCard CAP / VISA DPA, paper-based TAN lists, Grid Cards, SMS, PKI cards, as well as more traditional static passwords, PINs and partial passwords.

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



duties and dual controls. As part of a live environment, the Cryptomathic Authenticator supports fail-over and clustering to provide redundancy and scalability. The system is also highly optimised for performance, and is designed 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 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.



Cryptomathic Authenticator

Best-practice system 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

Enterprise Authentication Server	Feature	Cryptomathic Authenticator
At most 10s of authentications per second required	Performance	100s or 1000s of authentications per second may be required
Large corporate may require 10,000 users	Users	Up to 10,000,000 users must be supported, with room to expand
No need for clustering support	Scalability	Must scale to support larger customer bases and higher load
Single server suffices for most availability environments; large corporate redundancy may require fail-over	Availability	Must offer 24/7 availability through multiple redundancy of all components
Server administered directly, access controlled via password	Administration	Strong controls required: remote administration; chip-card administrator log-in; separation of duties; dual controls
Log authentication attempts	Logging	Log authentication attempts and all administrator activity. Administrator log must be tamper-evident

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 (web based, phone based, e-commerce)
- Multiple authentication mechanisms in parallel
- Configuration of validation parameters
- Modular architecture

Authentication Methods

- Grid cards
- MasterCard CAP
- Visa DPA
- VISA CodeSure
- SMS
- Static passwords
- TAN cards
- Vasco Digipass
- OATH HOTP / TOTP / OCRA
- Display Cards
- Oberthur WebSTIC
- Partial Passwords

Operating Environment

- Microsoft Windows
- Red Hat Enterprise Linux
- IBM AIX

Database

- Oracle 10 and 11
- Microsoft SQL 2005 and 2008
- ODBC

Hardware Security Modules

- SafeNet
- Thales / nShield
- IBM
- Utimaco
- HSM specific firmware
- Software HSM emulator

INDEPENDENT FUTURE PROOF SOLUTION

The Cryptomathic Authenticator is an independent solution for a number of reasons. Firstly, it is independent of token vendor suppliers so customers are not tied to any particular authentication vendors or technologies when choosing the Cryptomathic Authenticator.

Secondly this level of independence applies to HSMs, also allowing the Cryptomathic Authenticator to support the customers preferred HSM brands and models.

Finally, Cryptomathic Authenticator can be deployed on multiple operating systems to meet the exact operating requirements of the end user.

Cryptomathic Authenticator is also modular in design which allows for simple support of new token types and algorithms, often with no impact on the existing token functionality and existing interfaces.

Through a wide and growing range of user and transaction authentication methods, the Cryptomathic 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. Since 1986, Cryptomathic has assisted customers by providing systems for e-banking, PKI initiatives, card personalisation, ePassport, card issuing, and advanced key manage-

ment 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.

Learn more at cryptomathic.com