

TECHNOLOGY AUDIT

Cryptomathic Authenticator – v3.2

Cryptomathic

BUTLER GROUP VIEW

ABSTRACT

Cryptomathic Authenticator is a server-based solution that has been architected to meet the needs of the banking and payment industry. The solution is vendor agnostic in its support for authentication tools at the front end, and Hardware Security Modules (HSM) at the back end. In Butler Group's opinion, this provides much needed flexibility to financial services organisations when required to roll out two-factor authentication technology to secure Internet banking and online payment facilities. Supported authentication includes: one-time password tokens, card-and-reader tokens (including MasterCard CAP VISA DPA), paper-based TAN lists, SMS-driven response codes, hardware and software PKI tokens, static passwords, partial passwords, and OATH HOTP. The role that has been set for Cryptomathic Authenticator is to eliminate, or at least considerably reduce, the incidence of successful Phishing, Pharming, and man-in-the-middle attacks as well as threats posed by Trojans, Spyware, and Keyloggers. The stated target market for Cryptomathic Authenticator is banks and transaction processing companies of any size, as well as the government sector.

KEY FINDINGS



Sensitive information (at the database as well as HSM level) is maintained in a secure environment.



A scalable solution that supports clustering and failover capabilities.



The banking fraternity has been slow in its adoption of strong two-factor authentication for customer-facing transactions.



Currently available on Windows, Linux, and UNIX platforms.



Offers support for a number of industry standard HSMs, including those from nCipher (Thales), IBM, and Safenet.




Offers support for a wide range of front-end authentication devices.



Provides an open capability to support all new authentication mechanisms as and when they gain market adoption.



Designed to operate with banking and customer management applications.

Key:  Product Strength  Product Weakness  Point of Information

LOOK AHEAD

Future development plans for the Cryptomathic Authenticator product set are defined by the company's internal roadmap, which is in turn governed by the business needs and priorities of its existing customers. Current work that is in the pipeline includes facilities to port the solution to the 64-bit IBM AIX platform, introducing redundancy and flexibility into OTP delivery via a mobile SMS approach, and providing support for other UNIX platforms.

FUNCTIONALITY

Customer use of Internet banking has gained considerable traction over the last few years as a popular new channel for self-service account management. From the institution's perspective, it has increased their global footprint and has enabled them to offer an increasing range of services across geographical boundaries. This has inevitably opened up the banking and payment industry, and in particular the retail division, to a wider range of threats. Of late this has also led to a number of high-profile security breaches and fraud statistics that continue to grow at an alarming rate. This situation has led customers, the media, and regulators to question how safe online transactions and, more importantly, customer identity data, really is, and what the banks are doing to improve things. However, the uptake in the use of strong multi-factor authentication has seen only a slow rate of adoption, mainly due to the costs and operational complexities associated with its roll-out.

Product Analysis

Cryptomathic Authenticator is an authentication server-based solution that has been designed to meet the needs of any access management or transaction-based authentication system. The solution, by its very nature, has found a reasonably high level of acceptance particularly within the commercial banking industry, and Cryptomathic has architected the product for use within banking applications and other customer-facing management systems. Cryptomathic Authenticator provides strong two-factor authentication to customers and/or businesses who would want to undertake secure financial transactions or access the bank's online customer services.

Butler Group believes the key strengths of the Cryptomathic offering come from its inherent ability to support a wide range of authentication tools at the front end of the solution and secure Hardware Security Modules (HSM) technology at the back end. The vendor-independent approach adopted by Cryptomathic ensures that banks and financial institutions have the option to select an appropriate authentication mechanism and the HSM that best complements the service that they wish to provide. The front-end authentication tools supported include any of the following options:

- Chip Authentication Protocol and Dynamic Passcode Authentication (CAP/DPA) – a high-security authentication mechanism for card-based transactions (Mastercard and Visa) where the user inserts their card into a hand-held reader which generates a One Time Password (OTP).
- One Time Password (OTP) tokens – hand-held, hardware form-factor tokens where the user is presented with a OTP upon the push of a button or by entering a static password.

- Hardware-based Public Key Infrastructure (PKI) tokens – are tokens with a hardware form factor which generate a digital signature that is then validated using a public key. This authentication method offers an extremely high level of security and represents a more viable alternative for business banking applications.
- Software-based PKI tokens – a derivative of the hardware-based PKI token, where the private key resides in a secure server and can be used to generate digital certificates for authentication purposes, following strong user authentication.
- Short Message Service (SMS)-based OTPs – this lightweight authentication approach is beginning to gain traction. In operational use the bank sends an OTP in an SMS form to the customer's registered mobile number before authenticating specific financial transactions.
- Transaction Authentication Number (TAN) Lists – a low-cost authentication mechanism where banks provide customers with an indexed paper-based list of OTPs. In order to authorise a transaction, the customer must key in the OTP corresponding to the specific index as requested by the bank.
- Matrix cards – a random grid of numbers printed on a matrix; customers may either use a pattern-based approach or can be prompted to key in specific contents within the matrix in order to authenticate a transaction.
- Static/Partial Passwords – this is often a legacy authentication step based on the end user's knowledge of a secret password.
- OATH – Cryptomathic also supports the use of Open AUTHentication (OATH) approaches, an industry initiative for providing a standards-based reference architecture that is aimed at the provision of strong authentication across all users and devices.

Use of the Cryptomathic solution lends itself well to the provision of a strong tie-in with a Hardware Security Module (HSM) for the secure storage of information that a customer knows or has knowledge of but other parties should not. HSMs are basically hardened black-box devices that provide absolute protection for the information that they hold, be it a token key, a public key, a static password or other sensitive data. Cryptomathic's own hardware team writes the firmware for the supported HSMs to ensure that all processing of secure data happens inside the secure HSM and not in the server environment, therefore providing the highest levels of data security.

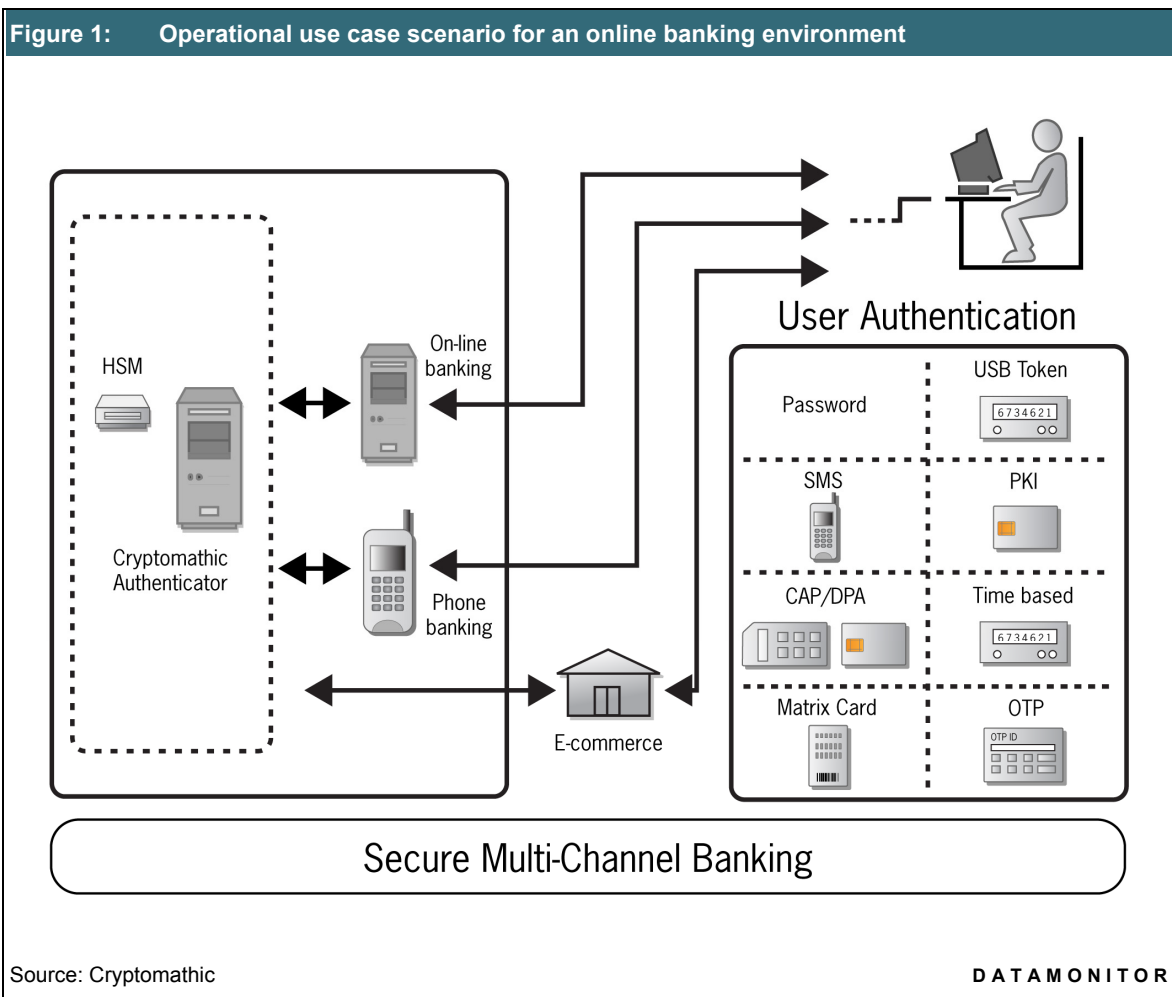
Cryptomathic's vendor-independent support for HSMs further enhances its applicability in scenarios where banks/organisations can select their own HSM during a two-factor authentication roll-out. Supported HSMs include SafeNet/Eracom ProtectServer Orange (validated to FIPS 140-1 level 3), SafeNet/Eracom ProtectServer Gold (validated to FIPS 140-2 level 3), nCipher nShield F3 (validated to FIPS 140-2 level 3), nCipher netHSM (validated to FIPS 140-2 level 3), and IBM 4764 (validated to FIPS 140-2 level 4). FIPS 140 is the current Federal Information Processing Standard for cryptography modules specified by the US Government, and the following levels (1 through 4) are the levels of security, with 1 being the lowest and 4 the highest.

Product Operation

Figure 1, below, provides an illustration of an operational use case where Cryptomathic Authenticator is being used in an online banking environment. As highlighted, the solution supports multiple authentication mechanisms, tokens, and smart cards, etc., and through the use of its best-practice key management facilities by leveraging an HSM within the same operation, the solution provides strong external, as well as internal, security for banking customers.

Typically, strong authentication systems can utilise several distinct categories of protection that incorporate:

1. Something the customer has – for example, an OTP or USB token, matrix card, CAP/DPA, etc.
2. Something the customer knows – a password or other checkable information.
3. Something that the customer is – a biometric authentication approach perhaps.



The use of a biometric authenticator is typically not viable in an online banking application because of the costs and complexities involved in its roll-out to customers. Hence, the most practical way forward is normally to couple the something that a customer has with the something that a customer knows in order to provide reasonable two-factor authentication.

In normal operational use the Cryptomathic Authenticator solution is invisible to the customer. Each time they wish to access their online banking facilities, they are presented with a log-on page from the bank's Web access control system. The customer then typically enters their on-line banking customer ID, together with a static password or entry code, and the one-time key that has been generated from a bank-provided token. The collected account access keys are received and verified by the Web access control system, which then validates the customer's identity and their credentials. If these checks are successfully completed, the Web access control system then accesses the customer database to map the customer ID to their credentials and calls the Cryptomathic Authenticator and passes on the token's unique identity and one-time key to the Authenticator.

The Cryptomathic Authenticator responds by using its databases to look up the customer keys for that particular token ID. It then links to the HSM that is being used to process the request and formally validates the requestors keys; to complete the process, the response from the HSM of 'access is allowed' or 'access is denied' is passed back to the bank's Web access control system by the Cryptomathic Authentication server.

Each generated key is received by the Cryptomathic Authenticator system on a one-time basis. Functionally, from a security position, this means that the same code cannot be used again to authenticate systems access, and, most importantly, even if the code was intercepted or given out freely by a customer to a third party it could not be reused. Under such circumstances, threats from Trojans, Spyware, and key logger attacks (where a virus or program installs itself in a customer's PC, reporting back on password and system access details), Phishing and Pharming attacks (where fraudsters try to trick customers into revealing password details), Man-in-the-Middle attacks (where information is intercepted whilst the customer is online), and Insider Attacks (where a bank employee exploits the security system 'in-house') can all be significantly reduced, or indeed eradicated.

With respect to the use of specific token management systems, organisations can integrate their existing token management solution through the use of Cryptomathic Authenticator's management API, or integrate with third-party customer management solutions (for example Identity and Access Management suites), or alternatively use the solution's native token management capabilities. The Cryptomathic Token Manager is basically a wrapper to the management API and provides an interface, along with a configurable workflow to token management tasks.

The solution offers strong security functionality at both the HSM and the database level. As a result it provides customers and financial institutions with a hardened and protected environment for the processing and security of critical data and financial processes. The Cryptomathic Authenticator offers configurable thresholds where users are automatically denied access after a certain number of failed attempts and can also offer a time window, after which any means to gain access would be blocked. By encrypting critical fields within the database and by offering hardened protection to security keys that reside within the HSM, the solution ensures that customer-sensitive data remains protected and is never exposed.

Product Emphasis

Cryptomathic Authenticator delivers strong business and user protection on two specific levels: for financial institutions it provides a proven, secure, and cost-efficient authentication vehicle that can be deployed without disrupting existing banking and customer management systems by virtue of its support for multiple authentication tools and a variety of HSM products; for customers it provides the ability to deliver a secure, easy to use, one-time authentication approach that cannot be wilfully or accidentally undermined by malicious identity-theft activities.

DEPLOYMENT

The Cryptomathic Authenticator solution is normally deployed in line with and alongside a financial organisation's own banking protection systems, to deliver an extra sealed layer of customer protection, although where necessary it can also operate independently. At its point of deployment the solution requires the availability of a range of basic systems and server management and installation skills. These include some knowledge of HTTP to cover basic integration requirements, and integration with management interfaces, which may be optional in some installations. It also requires a level of expertise in the use of Web services and Simple Object Access Protocol (SOAP).

Installers need to have a working understanding of standard operational systems concepts, and administration and set-up elements need to be supported by a good knowledge of industry-standard security principles. In addition, some database management knowledge is required which, dependent upon systems complexity, can range from basic installation and administration skills, up to expert database knowledge to deal with clustering, hot failover, and real-time backup requirements. Average deployment timescales are impacted by systems complexity issues, but can start from as little as two hours for the installation and integration of a very basic system with no customer management requirements.

Following installation very little in the way of systems administration is normally required. Even where the system has been deployed alongside, and integrated with, an organisation's customer management system, normal token management and customer management activities are external to the Cryptomathic solution and are delivered through standard back-office systems channels.

Cryptomathic provides training that covers the requirements of systems integrators (only occasionally requested), systems administrators, and company auditors. Such training can be provided on the customer's site and is supported by a comprehensive range of integration, installation, administration, and maintenance manuals. Systems support and maintenance is also provided by Cryptomathic, and is available on a level to suit the needs of the customer – weekday office hours, weekday 24-hour, and on a 24x7 basis.

The key platform used when deploying Cryptomathic Authenticator is currently Microsoft Windows Server2003, although the product can be ported to various UNIX platforms if required. The system operating framework is Microsoft.NET, and the supporting databases can be run on either Microsoft SQL or Oracle platforms. Supported HSMs include: IBM, nCipher, and Eracom. Other additional requirements, dependent upon the financial services organisation's authentication tool of choice, may include smartcard readers (normally GEMplus), and a systems toolkit for the integration of certain cryptographic functions.

Once deployed, some changes will need to be made to operational procedures within the end-user organisation as Cryptomathic Authenticator adds an additional layer of security. However, this should have only a very small impact on day-to-day operations and the main changes will be seen by the organisation's customers if they do not already make use of a one-time token or smartcard for authentication purposes when they sign in to the system; this will be an identifiable extra security layer.

Across the overall solution Cryptomathic Authenticator normally involves the use of an authentication server and database, with one or more selected HSM products attached. A chosen form of authentication token or smartcard will be required to drive user authentication, but the selection and deployment is seen as external to the core Cryptomathic system.

PRODUCT STRATEGY

The target market for Cryptomathic Authenticator is banks and financial institutions that provide their customers with self-service, Internet, and telephone access to account and financial information. The company also targets government systems with its Authenticator solution. In terms of organisation size, Cryptomathic claims that its solution is suitable for use within small and medium, as well as large organisations.

The primary ROI drivers for using Cryptomathic Authenticator are the cost savings that can be realised by preventing fraudulent attacks on banking systems. Such savings manifest themselves as financial and reputational losses that have been prevented. In addition, a further argument in favour of the solution is that the visible availability of associated protection (strong two-factor token use) encourages customers to continue to use cost-effective, online, self-service facilities, rather than reverting to other more-expensive-to-the-business communications channels.

Because Cryptomathic Authenticator supports a wide range of authentication schemes, it avoids both technology-mandated solutions and vendor lock-in to a particular authentication scheme. The product can be brought to market via reseller and partner channels, although its primary sales channel is direct. Key business partners and technology partners include: nCipher (Thales), Eracom, Vasco, Xiring, Mastercard, and Visa.

Cryptomathic states that the release strategy for Cryptomathic Authenticator is governed by business needs. The priority requirements of all existing customers, which are gathered annually at the Cryptomathic Authenticator user group meeting, are the main release drivers. Major functional releases happen either once or twice a year and are available free of charge to all existing customers with a valid maintenance and support agreement.

For each deployment there is a one-off licensing cost. This is based on the number of potential users, and the organisation's requirements for failover, redundancy, and scalability. Annual support costs are based on the company's three-tier support infrastructure (weekday office hours, weekday 24 hour, and 24x7 cover). Typical project costs are based on project size, but may be as wide ranging as UK£20,000 to over UK£1 million. Other major systems releases, which are covered by the systems maintenance contract, are made on a bi-annual basis.

COMPANY PROFILE

Cryptomathic was founded as a university spin-off back in 1986 by Professor Peter Landrock. The company, which remains in private ownership, has its headquarters in Aarhus, Denmark, and also has major offices in Munich, Germany; Cambridge in the UK; Copenhagen, Denmark; and Montreal, Canada. Cryptomathic is known as a leading provider of strong security solutions that are used across a wide range of business and industry sectors including: Finance and Banking, Government, and the Digital Rights Management and Smart Card sectors. The company prides itself on its strength of technical expertise, employing some of the world's leading cryptographers, including Vincent Rijmen and Ivan Damgaard.

Today the company employs 55 staff, with 50 deployed across its European operations. The breakdown by functional area is 60% employed in Research and Development (R&D) activities, 20% in Sales and Marketing (S&M), 10% in support services, and 10% in administrative roles. Using this base it continues to focus on the development and provision of industry-focused, high-quality protection solutions.

As a privately held security company Cryptomathic does not make public either its revenue figures or its list of existing customers. However, it was prepared to confirm that its revenue split by region was US 20%, Europe 70%, and elsewhere 10%. Its customer base, across the company's product portfolio, extends to over 500 customers worldwide, and 20 of these (mainly high street banks) are already using its Cryptomathic Authenticator product.

SUMMARY

Butler Group believes that putting in place a strong, provable, multi-factor authentication foundation is crucial to ensuring that only users with legitimate access rights are allowed to successfully gain entry to the online banking services of our financial institutions. Doing so offers the twin benefits of (a) increasing customer confidence in the secure nature of online banking, and (b) making financial institutions more secure and less susceptible to socially engineered security breaches. Butler Group strongly recommends the use of strong business- and user-protection solutions such as Cryptomathic Authenticator, especially where its use can be linked to the secure use of authentication tools that are appropriate to the risk profile of the organisation and its customer base.

Also, today's economically uncertain climate, which has seen a raft of mergers and acquisitions within the banking fraternity, has made the task of integrating and managing the roll-out of multiple technologies for user authentication and systems access into an evermore challenging task. In Butler Group's opinion, such a scenario presents Cryptomathic with a clear-cut opportunity to offer an integrated and secure authentication solution platform that can work openly with a wide variety of front-end authentication devices and back-end HSMS through its vendor-independent approach.

Table 1: Contact Details	
Cryptomathic Ltd. (Europe) 329 Cambridge Science Park Milton Road Cambridge CB4 0WG UK Tel: +44 (0)1223 225 350 Fax: +44 (0)1223 225 351 www.cryptomathic.com	Cryptomathic Security Corp. (Americas) 420, Rue McGill Bureau 300 Montreal Quebec, H2Y 2G1 Canada Tel: +1 (514) 871 9398 ext. 229 Fax: +1 (514) 937 6140
Source: Cryptomathic	DATAMONITOR

Headquarters

Shirethorn House,
37/43 Prospect Street,
Kingston upon Hull,
HU2 8PX, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.

Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

Butler Group

245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

For more information on Butler Group's Subscription Services please contact one of the local offices above.

