

Operations

Butler Group Subscription Services

Security

TECHNOLOGY AUDIT

Cryptomathic

Cryptomathic Signer 2.2

Abstract *Cryptomathic Signer is a server-centric solution for the creation, management, and use of private keys within a Public Key Infrastructure (PKI). The storage of a private key on a computer's hard disk not only presents a security risk but also reduces the use of this key to operations carried out only from this computer. Storing the user's signature key on a secure central server reduces security risk, and at the same time increases the use of the key as the user is now able to access and use the key from any Web browser. Butler Group thinks that the use of SMS offered by this product for two-factor authentication is a great use of pervasive technology, and highlights the flexibility and real-world value of the solution. A dominant player in Europe, Cryptomathic still has to make a big name for itself in the North American market. Large organisations, banks, and government departments would benefit from this product at a time when non-repudiation plays an increasingly significant part in corporate governance and compliance.*

KEY FINDINGS

- | | |
|---|---|
| ✓ Integrates with existing PKI solutions and end-user applications. | ✓ Supports a variety of authentication techniques. |
| i An alternative to a smartcard solution. | i Signs more than 4,000 signatures per minute on a single server. Scalable to multiple servers. |
| X Yet to be accredited as a Secure Signature Creation Device. | X Server-side, Microsoft Windows-only solution. |

Key: ✓ Product Strength X Product Weakness i Point of Information

LOOK AHEAD

The use of digital signatures has been slow to start, but as organisations, governments, and institutions look for solutions to reduce fraud and increase electronic security, so products like Cryptomathic Signer look set to become the next element of IT infrastructure. Cryptomathic's success will ultimately be linked with growth away from domestic markets.

► FUNCTIONALITY

Cryptography is essential for e-business, e-commerce and the secure exchange of data across Intranets, Extranets, and the Internet. Governments, individuals, businesses, and organisations of all kinds rely on cryptography to provide authentication, confidentiality, and integrity. Authentication assures the recipient of the message that the sender is who he claims to be. Confidentiality ensures that the data, information, or message can only be read by the intended or authorised recipient. Integrity assures the recipient (and the originator) that the data has not been altered in transit.

Product Analysis

Every company wants to be seen as easy to do business with, and as a result many more organisations are exchanging and providing access to information that would have been kept under lock and key in a metal filing cabinet in years gone by.

Clearly one of the most significant business challenges today is the preservation of data confidentiality, integrity, and availability. Confidentiality means ensuring that information is accessible only to those who have authorised access, while integrity means safeguarding the accuracy and completeness of information along with any associated processing methods. Availability ensures that authorised users have access to information and associated assets whenever and wherever required.

Butler Group believes that only through the ubiquitous deployment of Public Key Infrastructure (PKI) can the world trust the Internet (which is basically an insecure public network) in terms of confidentiality, integrity, and availability. Back in the mid-1990s, many industry commentators predicted that the smartcard would be the answer to all of our concerns, but several years on and smartcard readers are still something of a rarity – and this is despite the support of such devices by Microsoft Windows for several years.

While no one really knows why the smartcard reader never became a standard component of the PC in the way the CD-ROM drive did, the fact remains that organisations still require a method of ensuring strong authentication and privacy – and now increasingly in demand is non-repudiation as well.

To address these business issues, organisations are starting to consider – and in many cases deploy – public key encryption for digital signatures, yet in all too many usage scenarios, the option of storing the user's signature key on the desktop computer or on a smartcard is not an option. The vulnerability of desktop PCs, and the complexity and cost associated with hardware-based solutions, means that organisations are seeking alternative solutions for the management of users' private keys.

Cryptomathic Signer's (Signer) role in a PKI is to generate and then store the user's signature key in a high security environment, and then to generate digital signatures as and when required by the user. The most obvious business benefit of Cryptomathic's solution lays in the removal of those barriers often presented by traditional technologies. Signer does not require installation of client-side software – thereby enabling user roaming and greater mobility. The architecture of the solution is such that complete confidentiality is assured – no one, not even a systems administrator, will be able to learn the message that is to be signed by the private key.

While the solution has yet to be accredited as a Secure Signature Creation Device (under the European Electronic Signature Standardization Initiative), and a UNIX port has yet to appear, Cryptomathic Signer is relatively simple and cost effective to deploy, and easy to use. The system offers organisations easy key management, strong authentication and non-repudiation, and perhaps most important of all, end-user mobility.

Product Operation Signer is designed to play a significant part in a PKI. The primary role of this product is as a key management system, generating and storing user digital signature keys for use as and when required.

Interaction with PKI

Signer interacts with a Certificate Authority (CA) as both Registration Authority (RA) and key owner. Signer initiates user registration with a CA, generates public and private keys, and then requests certification of the public key by the CA (the registration of users can also be handled from a third (RA) application, using Signer's administration API). Having certified the public key, the CA then takes care of certificate management.

Protection of Signature Keys

Having generated the keys, Signer stores the user's private key securely in a central database – rather than the user's computer hard disk – and so effectively reduces security risks, while at the same time extending the use of digital signatures to roaming users.

By providing the user with access to the private key at any time via a Web browser, e-mail client, or mobile device, Signer enables organisations to use digital signatures in many more ways and situations than would be the case if the key were stored on the user's computer hard drive.

Authentication and Key Usage

With the user's private key now stored on a highly secure central server, the only challenge now remaining is protection of key usage. Cryptomathic has opted for a well-known technique called two-factor authentication to protect key usage. There are many ways of proving one's identity, and these are divided into four categories:

- Something you *have*, e.g. smartcard, hardware token.
- Something you *know*, e.g. password, PIN.
- Something you *are*, or something intrinsic to your body, e.g. fingerprint or iris pattern.
- Something you *do*, e.g. the way one writes.

By authenticating something the user *knows* and something the user *has* through two independent channels, Signer is able to protect key usage.

Signer was developed to provide a transaction signing solution for a Danish Internet banking system and, as such, a primary requirement of the solution was the independence of the security mechanism from the core banking application.

Figure 1 shows a generic Signer usage scenario. In essence, the solution combines a static password *known* by the customer, together with a one-time password *held* by the customer, i.e. two-factor authentication. The one-time password can be delivered to the user's mobile phone via Short Messaging System (SMS), generated by a token, or printed on a scratch-card – alternative authentication options can be accommodated by the product's architecture. In order to access the signature key the customer has to prove that: (a) he *knows* the password; and (b) he *has* the mobile phone/token/scratch-card.

Here is how Signer works in an Internet banking scenario: the Internet banking customer logs on to the application using his computer via the Internet, and performs an operation that requires his digital signature.

1. The customer logs on to Signer using the static password and the one-time password received via SMS.
2. A secure tunnel is set up between server and client.
3. The hash of the transaction is sent to Signer.
4. Signer returns a digital signature and the customer's certificate.
5. The transaction, digital signature, and certificate are now sent to the Internet banking application.

The Internet banking application now validates the customer's signature. If the certificate was issued to the customer by a third-party then the Internet banking application validates the certificate.

The two important things to notice here are: (a) Signer never sees the transaction content – only its hash value; and (b) the customer's signature key never leaves the secure Signer environment.

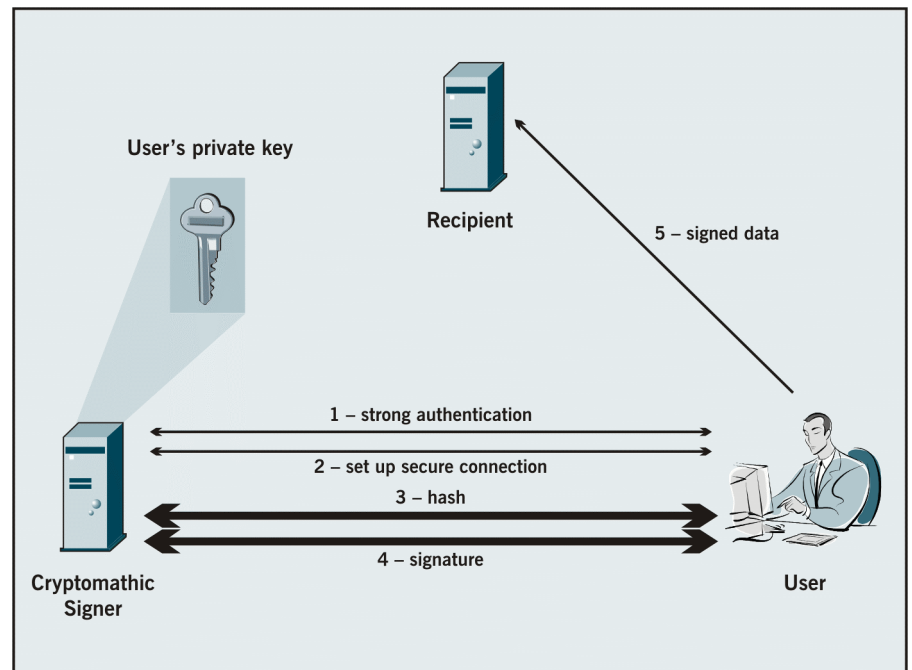


Figure 1: Generic Cryptomathic Signer Usage Scenario

Product Emphasis

Ease of use, low complexity, and optimum security are the key features of this system. Cryptomathic has to balance ease of use on the one hand with security on the other – not an easy thing to do well. In Butler Group's opinion, Cryptomathic has managed to develop a system that offers extremely high levels of security without presenting barriers to business.

The ability to accommodate a variety of authentication methods will enable organisations to tighten security without placing additional burden and risk on the shoulders of end-users. We like the fact that SMS – a technology familiar to most people these days – can play a part in the authentication process, as this avoids the need to deploy and manage yet more technology.

Because Signer comprises two physical servers, organisations deploying the product (in conjunction with an independent third party) can increase the integrity of the overall signing solution by removing the possibility of fraud committed by insiders – a significant differentiator for this type of signing solution.

Signer is built on the same crypto standards as other products on the market, but Signer's capabilities and architecture permit more implementation permutations, and an aggressive pricing model means that organisations looking to offer this solution to a very large user base can get the price down to £0.25 (25 pence) per user.

Cryptomathic has focused very much on the Danish domestic market to date – specifically the banking sector – but now the company is targeting its products and services at Telco's, governments, and large enterprises. Recent recognition by the World Economic Forum (Cryptomathic was designated as one of only 40 Technology Pioneers considered to be excelling in areas such as innovation, technology leadership, and growth) has provided the company with something of a springboard to launch its products into other regions.

► DEPLOYMENT

The operating environment supported by Cryptomathic Signer is currently restricted to Microsoft Windows NT/2000; therefore installation of the product will require Microsoft Windows platform expertise – especially if the separate server elements are to be clustered. Both Oracle and Microsoft databases are supported, so most organisations will already have the necessary database administrator skills required for Signer deployment.

Signer is likely to form only part of a PKI solution, and therefore successful deployment will also require knowledge of other PKI components. Cryptomathic offers consultancy services to those organisations having little or no in-house PKI expertise, and this, along with the company's other software products, could make Cryptomathic a one-stop-shop for many organisations.

A Signer deployment will typically consist of two physical servers (though a single server configuration is possible); these are the Cryptomathic Signature Server (CSS) and the Cryptomathic Authentication Server (CAS). To maximise the credibility of the solution, especially where Signer is deployed as an outward-facing service providing users with digital signatures for a variety of purposes, the CAS should preferably be located at a separate, independent organisation. This configuration separates the operation of the two servers, and as such protects the system from attacks by insiders.

Butler Group believes this to be an ideal service offer for systems management (outsourcing) companies, and Cryptomathic would do well to engage with the dominant players in this market.

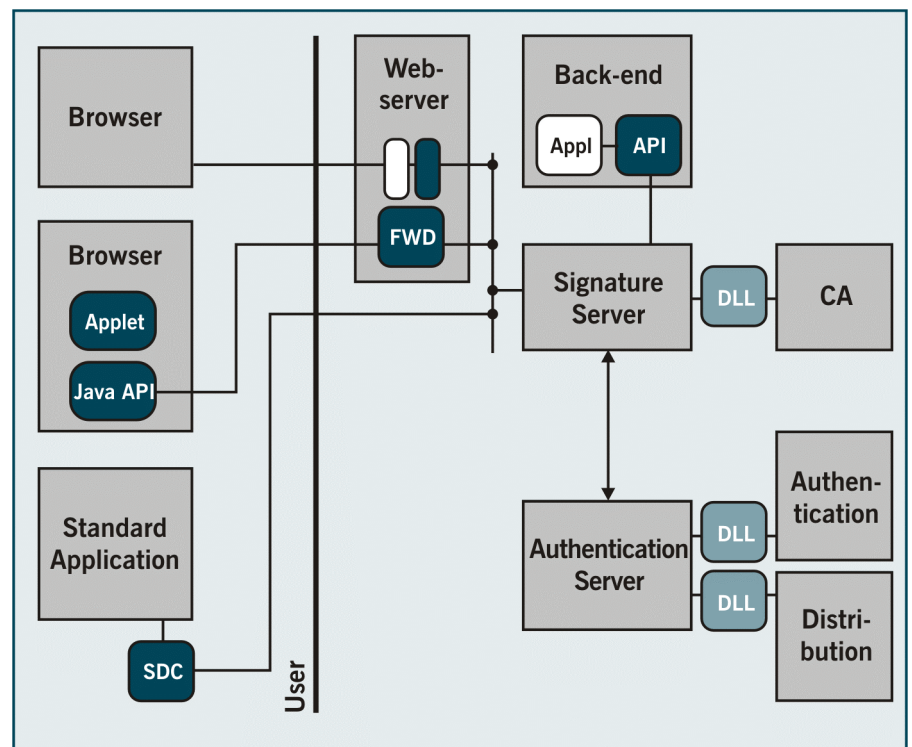


Figure 2: Cryptomathic Integration Overview

Typical planning issues to be considered before deployment of Signer include clustering topology, type of hardware to be used (including tamper-resistant hardware security modules), and location of servers (including back-end database servers). Implementing Signer with a third party will also introduce additional planning issues – many of which are likely to be non-technical.

Signer's well-documented deployment process is as follows:

- Install and configure the database for use by CSS and CAS (the product ships with database scripts for Microsoft SQL Server (7 and 2000) and Oracle (8 and 9) databases).
- Install CSS and CAS server software.
- CSS and CAS to exchange keys.
- Install Initialisation Wizard and Administration Client.
- Initialise system using Initialisation Wizard.
- Upload of Policy Definition File and System Configuration File by Security Officer (the administrator role entitled to create other administrators or to perform security-related management).

The product documentation provides complete guidance as to the installation, configuration, and maintenance of Signer, including a section on Disaster Recovery – something more vendors should provide.

Cryptomathic provides a comprehensive Administration Guide (although Signer comes with two different administration clients, one for CSS and one for CAS). Signer administration is typically split between two roles: the Security Officer and the Clerk. The latter is entitled to manage user accounts and very little else, while the former has complete control over the system – assuming of course both CSS and CAS are deployed within the same organisation, and even then separate CSS and CAS administrators would be preferable.

According to Cryptomathic, installation and configuration of Signer takes just a few of days, but as with all major infrastructure projects, overall project duration is likely to be significantly longer.

Cryptomathic offers a range of support options ranging from an 8-hour response Monday – Friday, 8.30am – 4.30pm (GMT+1), to 365x24 4-hour response. No end-user training is required as such, but Cryptomathic does offer one and two day courses for system operators and security officers.

As stated earlier, Signer only runs on Microsoft Windows NT and Microsoft Windows 2000; however, the company states that a UNIX port is possible. Database support extends to Oracle 8 and 9, as well as Microsoft SQL Server 7 and 2000. Administration clients require a Java 2 SE Runtime Environment – Windows 2000 is the preferred administration platform.

Signer supports cryptographic hardware processors from IBM (the 4578) and nCipher (nForce and nShield). By using these tamper-resistant products, Signer provides true non-repudiation digital signatures.

Signer generates RSA signatures with key lengths from 512 to 2048 bits. Signed formats are ISO9796, PKCS#1, and PKCS#7. Signer uses X509v3 certificates as public-key certificates – these can be appended to signed messages (ISO9796 and PKCS#1) or embedded into the message (PKCS#7).

PKCS#10 “issue” and PKIX-CMP “revoke” protocols are used for issuing and revoking certificates with the CA; certificate renewal and update are not used. According to Cryptomathic, the registration protocol is the only protocol not standardised, and so Signer must be tailored to handle new CAs – although one would expect popular CAs to be accommodated out-of-the-box.

On the client side, the end-user can use Signer either through a browser, e.g. for form signing, or through such applications as Microsoft Outlook, Microsoft Outlook Express, and Netscape Messenger. This client-side integration can be achieved through various means: PKCS#11, Microsoft CryptoAPI (integrates as a Crypto Service Provider), a 30KB applet, Java API, ANSI C API, Windows DLL, or Signer Desktop Client (SDC).

A wide-range of authentication devices are supported, including RSA SecureID and Vasco DigiPass authentication tokens, one-time passwords delivered by SMS, and EMV (Europay, MasterCard, and Visa) smartcard-based authentication from Xiring.

► PRODUCT STRATEGY

Cryptomathic aims to ship a new release of the product every 12 months, with particular focus on adding support for new authentication devices and schemes. The company plans to enhance the product's management features over the coming months, ensuring that total cost of ownership for the product remains low. Accreditation as a Secure Signature Creation Device is sought from the European Telecommunications Standards Institute (under the European Electronic Signature Standardisation Initiative) in 2004 – a move likely to raise the profile of Cryptomathic's products in this sector.

Target markets remain on-line banking, e-Government, and identity and access management within large organisations. Cryptomathic is keen to leverage its strong track record in the Danish banking sector in to other countries, and recent selection by a UK high-street bank shows the company to be making significant progress in this direction.

In the e-Government space, Cryptomathic has recently teamed up with AEP Systems and Bull to provide IT solutions for criminal justice, police, and government agencies. In Butler Group's opinion, this is likely to be a very lucrative market under the current political world climate – as demonstrated earlier this year when the British Government announced a £330 million counter-terrorism initiative to enhance UK security.

Cryptomathic continues to extend its partnerships with vendors offering complimentary products and services: nCipher and IBM in the crypto-processor market; and Vasco and Xiring in the authentication market. The company has also linked up with French IT security firm AVENCIS, a move likely to enhance both party's offerings. Other partners include Bull, iSecure, Nexus, Eracom, and Aladdin Knowledge Systems.

Signer licensing fees comprise of a one-time low-entry software fee and user fees (one-off or yearly). According to Cryptomathic, a typical project will be in the region of €500k, with licenses and services split roughly 50/50. The company charges an annual maintenance fee (20% of software list price at the time of purchase) to cover upgrades, and patches.

There is a great deal of activity in the electronic security market (most of it still fuelled by e-commerce); however, PKI is still something many organisations have not yet committed to. Butler Group believes that corporate governance, regulation, and general security concerns will drive the adoption of digital signatures in the coming months, and companies like Cryptomathic will be ready and waiting to provide a whole range of different products and services to meet this demand.

The key to success in this market will be visibility; there are already a number of companies with high profiles in this area, and for Cryptomathic to succeed it will have to partner with some major players – most likely outsourcing companies and System Integrators.

Telco's, mobile phone companies, and IT industry heavy weights are all vying for a piece of the action, and as a result this sector is likely to be the scene of a significant amount of merger and acquisition activity – typical of a ripening market.

Although Europe appears to be leading the way on digital signature thought and usage, the North American market cannot be ignored. Cryptomathic must establish presence and visibility in this region quickly in order to gain a foothold in this rapidly growing market.

► COMPANY PROFILE

Cryptomathic was founded by Professor Peter Landrock and two fellow cryptographers in 1986 as a university spin-off from the University of Aarhus, Denmark. The company was one of the first in the world to commercialise cryptographic algorithms and has since become one of the world's leading providers of security solutions. The company employs around 70 people in offices throughout Europe (Denmark, UK, Belgium, France, Italy, and Germany).

Cryptomathic is a privately owned company, and has reported growth of 74% and 86% for 2001 and 2002 respectively. The company has backing from Infineon Technologies and Maersk Data.

Companies listed on the Cryptomathic Web site include: British Telecom, SDC (Datacentre of Danish Savings Bank), NHS, and the Danish Government. Products are sold on 5 continents, with Europe being seen as the most important.

► SUMMARY

Cryptomathic Signer is an Internet-centric solution for the secure generation, storage, and use of digital signatures. By maintaining the user's digital signature in a secure environment, rather than on a desktop computer's hard disk, Signer enables organisations to reduce risk while at the same time increasing flexibility. In a growing market for digital signature solutions, Signer offers a well-architected product at a reasonable price – backed by world-class experience and expertise.

Cryptomathic offers a range of products and services for organisations, governments, and institutions seeking digital signature solutions. The company has a deservedly strong reputation in Europe, and continues to develop innovative electronic security solutions.

► CONTACT DETAILS

Cryptomathic A/S
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark
Tel: +45 8676 2288
Fax: +45 8620 2975
www.cryptomathic.com

Cryptomathic Ltd.
329 Cambridge Science Park
Milton Road, Cambridge
CB4 0WS, UK
Tel: +44 (0)1223 225350
Fax: +44 (0)1223 225351

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.

Europa House, 184 Ferensway, Hull, East Yorkshire, HU1 3UT, UK
Tel: +44 (0)1482 586149 Fax: +44 (0)1482 323577 www.butlergroup.com

For more information on Butler Group's
Subscription Services, contact: