

“We were impressed by the technology. It works immediately after the devices are switched on, i.e. even before they actually boot up.”

*Fredi Schmid,
Project Manager,
Swiss Re*



CUSTOMER NAME

Swiss Re

INDUSTRY

Reinsurance

CHECK POINT PRODUCTS

Pointsec® PC

Note: Pointsec Mobile Technologies was acquired by Check Point Software Technologies after this story was written

Swiss Re



www.swissre.com

Risk-free Travel

*By Jürgen Wasem-Gutensohn**

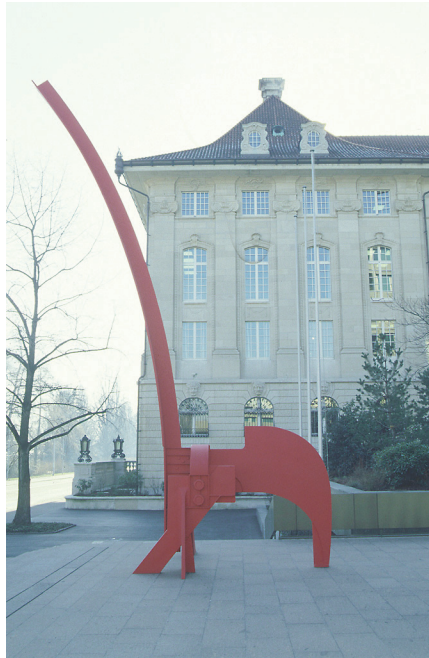
THE COMPANY

Swiss Re is one of the world's leading reinsurance companies and the biggest reinsurance company for life insurance and health insurance. With more than 70 group companies and agencies, the company is present in over 30 countries. Since its formation in 1863 in Zurich, the Group has been active in reinsurance. With its three Business Groups, Property & Casualty, Life & Health and Financial Services, Swiss Re offers a wide range of products for capital and risk management. Traditional reinsurance products such as miscellaneous property cover and liability, accident and motor vehicle cover, life and health insurance and associated services are supplemented by insurance-based corporate finance solutions and solutions for extensive risk management. Swiss Re is rated by Standard & Poor's with "AA", by Moody's with "Aa2" and by A.M. Best with "A+".

Critical data is best protected against misuse on business trips by complete encryption of notebook hard disks. If 4,500 notebooks are involved, as is the case for the Zurich firm Swiss Re, precise selection criteria and exact planning for the international rollout are important.

It's all in the name - for example "Enigma". An encryption machine bearing this name was designed back in the 1920s. The Enigma machine was used first in the civil commercial field and later by the military. Enigma is also the name chosen by Swiss Re for its IT project involving the encryption of 4,500 notebooks. The laptops are used by employees who travel a lot, commute between different locations or occasionally work in a home office. The reason behind the project is that the password protection in Windows XP was not adequate for those in charge at the reinsurance company. Notebooks protected in this way are open to any form of misuse within minutes with easily available hacking tools.

However, complete encryption of notebook hard disks, including the operating system and data, prevents unauthorized persons from reading the data. To find the right solution, the project team was asked to define selection criteria and to assess the products offered on the market on that basis.



The Swiss Re headquarters were built in 1913 and are located very close to Lake Zurich. (Source: Swiss Re)

“The essential requirement for an encryption solution for mobile terminals is that it must be compatible with the existing server infrastructure, the application components on the laptops and the software distribution mechanism. This also means that the software can be installed automatically during operation (i.e. without support employees on site) on the devices in use. The solution currently used, Pointsec for PC, meets these requirements.”

Fredi Schmid, Project Manager, Swiss Re

SELECTION CRITERIA SEPARATE THE WHEAT FROM THE CHAFF

“The essential requirement for an encryption solution for mobile terminals is that it must be compatible with the existing server infrastructure, the application components on the laptops and the software distribution mechanism,” stresses Fredi Schmid, the competent Project Manager at Swiss Re in Zurich. “This also means that the software can be installed automatically during operation (i.e. without support employees on site) on the devices in use. The solution currently used, Pointsec for PC, meets these requirements.” Installation should be as easy as possible for users. If complete encryption of notebook hard disks runs in the background, according to Schmid, the user can largely perform his daily work undisturbed.

The encryption of the entire notebook hard disk is binding on all notebook users. This means complete sector-by-sector encryption of the entire hard disk. This includes not only the storage areas in use but also areas with temporary or deleted files and the space not currently in use. For this reason, complete encryption is necessary.

The necessity of compliance with the encryption measures also means that even employees with administration rights on a notebook cannot disable or delete encryption software that has been installed. Measures are also necessary for cases in which users enter the wrong password repeatedly or have forgotten the combination of characters they chose. If a company has consciously decided against a central repository with all passwords, a challenge-response procedure between the user and the administrator helps in such cases. The user must first identify himself to the helpdesk. The user then generates a chain of characters (challenge). The administrator, who administers the user accounts but not the passwords, responds with the suitable response. The central administration software determines the response on the basis of the challenge. It is important that each response applies for only one access attempt. Therefore, the challenge-response procedure is superior to the transmission of encrypted passwords.

After a detailed evaluation of several quotations, Swiss Re decided on the Pointsec solution. “First of all, we were impressed by the technology. Another feature in its favor is the user authentication in addition to the actual encryption. This protection function works immediately after the devices are switched on, i.e. even before they actually boot up,” stresses Schmid. “Secondly, the international experience of Pointsec from the rollout of extensive installations also played an important role in the decision.”

256-BIT DATA ENCRYPTION

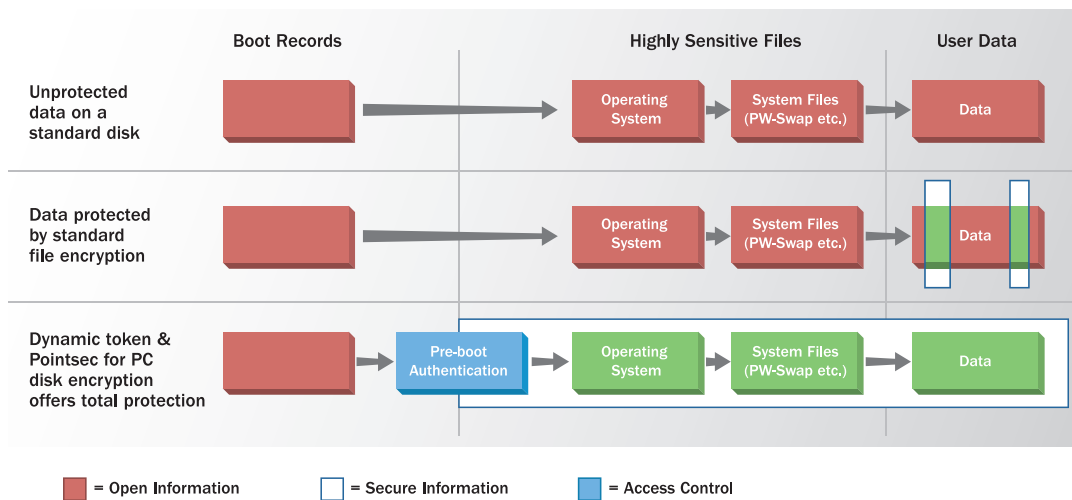
The encryption algorithm used in the Pointsec solution for Swiss Re is AES (Advanced Encryption Standard), a symmetrical procedure proclaimed by the National Institute of Standards and Technology in the USA as the successor of the Data Encryption Standard (DES). Named by its developers, the Belgians Joan Daemen and Vincent Rijmen, AES offers variable key lengths up to 256 bits. The algorithm also supports the challenge-response authentication required by the Swiss.

An extensive test in a staging area preceded the actual roll-out. The test involved around 100 employees, including some from the IT Department, members of the Security Committee and selected power users in regional branches. One aim of the test, for example, was to assess whether the encryption solution worked correctly in the existing IT infrastructure environment. Another aim was to test the reaction ability of the helpdesk in the event of challenge-response authentication. An intended side-effect of this was to train the support personnel “on the job”.

Users are supported today by a three-level service organization in which third-level support is provided by system administrators specially certified by Pointsec. They define security profiles centrally from Zurich and thus ensure general, uniform authentication and encryption guidelines. Three Pointsec administrators work at the headquarters. The administrators, none of whom is exclusively responsible for the encryption solution, look after the 4,500 notebooks in use worldwide. Purely arithmetically, the total administration cost amounts to one full-time position per annum.



Critical data stored on notebook hard disks is best protected against misuse by complete encryption of the hard disks.



While file encryption only securely encrypts data, with its solution Pointsec offers secure encryption of the operating system, system files and user data.



WORLDWIDE ROLLOUT

The actual rollout phase of the solution lasted almost six months. Every week, the encryption software was distributed to an average of 150 users as a normal software update. Just over half of all 4,500 users work in Europe. In Zurich, Fredi Schmid organized the distribution himself. There were a further six regional Rollout Managers.

After installation from a server, Pointsec for PC first encrypts the entire notebook hard disk. The actual user authentication takes place before the boot process (pre-boot authentication). Although initial encryption takes several hours, it runs in the background and users can use their notebooks normally. However, the notebook reacts slightly more slowly than normal during initial encryption.

The single sign-on procedure ensures that users subsequently only log on with their Windows user name and their Pointsec password. It is also possible to transfer the notebook to a colleague. To do this, the user logs off without restarting the notebook and his colleague can then log on.

During the evaluation phase, Swiss Re had already planned the second step. In addition to notebook hard disks, the removable media such as memory cards or USB sticks used in conjunction with the laptops are also to be encrypted with Pointsec products in the near future.

PENETRATION TEST

In the search for a security loophole, companies leave well-trodden paths. Instead of trying themselves to break encryption algorithms and encryption solutions, they commission experts, i.e. security companies, who specialize in testing security software thoroughly for customers. This is also true of Swiss Re, which had its encryption solution for notebook hard disks examined by experts. The result was clear. The experts confirmed that, supplemented by specific organizational measures, the solution offers the reinsurance company an extremely high degree of security.

SUMMARY OF THE SOLUTION

Employees who frequently travel, commute between different locations or occasionally work at their home office are provided with a notebook by Swiss Re in Zurich. Before the detailed analysis of individual security solutions, precise decision-making criteria were defined. Complete encryption of the notebook hard disks was required. The solution also had to be purely software-based and run under Windows XP.

**Jürgen Wasem-Gutensohn is editor with Beratungsgesellschaft für strategische Kommunikation PR-COM in Munich.*

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-575-9256 | Email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, Check Point Pointsec Protector, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.