zertificon

Success Story

Hannover Re Insures
Email Security

Compliance is a core business principle and has the highest priority at Hannover Re. IT security is a key driver and led the globally active re-insurer to choose the email encryption solution Z1 SecureMail Gateway with the Z1 SecureMail Messenger component from Zertificon Solutions. All incoming and outgoing messages are protected by a central system which guarantees legal compliance as well as the highest level of integrity when communicating with clients, partners and suppliers.

Central Gateway Solution contra Desktop Deployment

The network infrastructure requires a centralized email encryption system which is uncomplicated and able to secure all email traffic with diverse communication partners. Previously, Hannover Re deployed PGP based desktop solutions which generated a lot of work for IT administrators and had complex key management. The fact that the end users themselves had to decide which emails required encryption and which could be sent as plain text increased the security risks. Using password protected ZIP archives was an unsatisfactory compromise due to the fact that many client email systems blocked ZIP archives. Standard virus scanners cannot analyze ZIP archives which means common viruses can be hidden in them.

PKI- & Password-based Encryption

The consultants michael-wessel.de Information Technology GmbH presented the solutions PGP Universal Server, Utimaco SecureMail Gateway, ICC Julia MailOffice and Z1 SecureMail Gateway and after comparing and evaluating the various products, selected the solution from Zertificon Solutions. Z1 SecureMail Gateway is deployed as an SMTP proxy and automatically de-/encrypts, signs and validates signatures. It is compliant with the international email security standards S/MIME and OpenPGP.

*Wolfgang Lindner
Hannover Re*

A central feature of the Z1 SecureMail Messenger component is the possibility to send confidential messages using a password protected PDF email attachment and without the need for PKI (Public Key Infrastructure) or certificates as are required by conventional solutions. This significantly simplifies the secure email exchange.

A further advantage is the fact the solution is not only suited to securing communication with external partners, but can also be used to secure internal email communication. Due to the fact that Hannover Re communicates with partners who prefer PKI technologies as well as partners without PKI, the decision for Z1 SecureMail Gateway with the Z1 Messenger component was taken.

Wolfgang Lindner, responsible for Hannover Re IT-Network-Management explains:

"At the end of the day, the price/performance ratio as well as the constructive cooperation with the supplier convinced us. Any necessary patches were provided promptly and the development team was open to customizing suggestions. The system is highly flexible and powerful – but not overloaded with unnecessary functions."

hannover re®

Hannover Re transacts all lines of property, casualty and life/health reinsurance and maintains business relationships to over 5000 insurance companies in about 150 countries. It has a worldwide network of more than 100 subsidiaries, affiliates & local representatives on all five continents with approximately 2000 employees. The subsidiary E+S Rück is responsible for the German market.

Effortless Security

The installation and commissioning was performed without any interruption to the day-to-day operation and this has been true for all updates and upgrades since. Due to organizational reasons, the bedding-in phase lasted several months although the system was configured and ready-to-run within a few days. Worldwide, roughly 2000 users within the corporation benefit from secure email communication.

The decision to go with Zertificon was based upon the product features which guarantee high flexibility. The open platform enables rights-management for an unlimited number of administrators.

In addition, the solution offers flexible policies for a granular configuration of the security settings for each policy or communication partner. A key factor for selecting the solution was the multi-tenant architecture which supports the large number of domains and subsidiaries within the organization. The distinct separation of client-data, user interface and configuration parameters is supported, which ensures that each client can only see and modify his data.

Securing the emails is performed centrally and the end users are shielded from the complexity and effort associated with such a complex topic. The users no longer require any special knowledge and are free to concentrate on their core activities. In addition, confidential data (e.g. insurance or invoices) which were previously sent using CDs by post, can now be sent via email which avoids copying data and increases reaction times.

User Friendly Compliance

Wolfgang Lindner summarizes:

"*The requirements for secure information exchange within the context of global security projects can now be fulfilled, without emails losing their attractiveness for users – the usability is transparent and remains unchanged for internal users.*"

The Future

Hannover Re is considering rolling out the service – including customization of the user frontends etc. to a large subsidiary as well as the option of providing Z1 SecureMail Station to communication partners in order to facilitate secure email communication. In contrast to the Gateway, the Station looks up public keys from central providers such as Z1 Global TrustPoint which takes care of the management and validation of external keys. This variation is simple to administer and has low resource requirements.

Administration Building Hannover