zertificon®
Easy. Secure. Encrypted.

White paper

Secure email in times of rising mobile communication

Applied cryptography: Certificates, Gateways and End-to-End Encryption

White paper

Secure email in times of rising mobile communication

Applied cryptography: Certificates, Gateways and End-to-End Encryption

Essentially, there are two driving forces that bring decision-makers to deal with the issue of encryption. First entrepreneurs have a vested interest in keeping certain information very secret. Customer, management, financial data, concepts and new developments have to be encrypted to protect them against industrial espionage and manipulation. Second, compliance conformity is required. For instance, certain jurisdictions legally define how personal data must be handled and make the company directors personally liable. Furthermore, large numbers of national, international or sector-specific regulations have to be considered, including the linking of a company's credit worthiness with its IT security capabilities. All regulations demand: encryption must meet the current industry standards. Encryption according to the current industry standards relates to the available products, industry standards and the economic viability of the solution. To understand the available solutions, let us consider general cryptology.

Modern cryptology was developed in the middle of the last century, and was based completely on mathematics. It replaced the previous security concept of "Security by obscurity" by which security was achieved by keeping the encryption method secret – a risky, proprietary method with high dependencies.

Common contemporary market solutions rely on known algorithms. The only parameter needed to turn plain information into secret – encrypted – data is a key which itself is the secret. Algorithms such as AES (Advanced Encryption Standard) are considered very secure. The necessary effort for a brute force attack in which every possible combination is calculated and tried, rises exponentially with length of the key. The NSA does not have the resources to break AES on a large scale. Besides enormous amounts of mere computer processing time, such an attack would need more energy than is used in the US in a complete year. Specialists have calculated that the size of the secret NSA power plants is not sufficient even to produce the amount of energy required.[1]

Key Symmetry

There are essentially two types of encryption: symmetric and asymmetric (see Fig. 1).

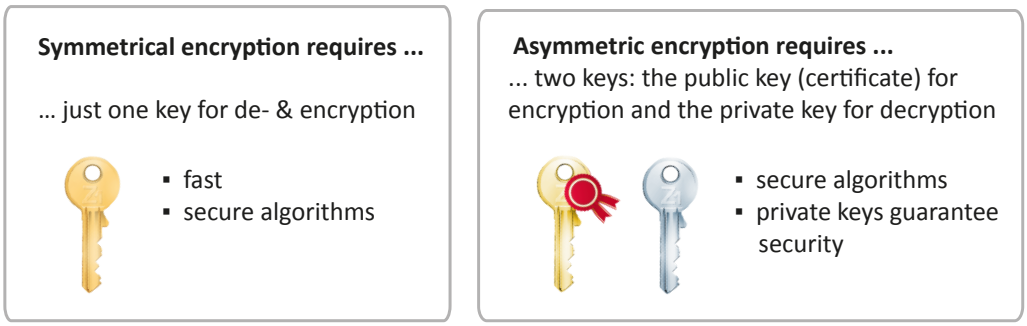


Fig 1: Symmetrical and asymmetrical encryption

In symmetric encryption, for example a defined in the AES standard, the same key is used for both encryption as well as decryption. Security of the encrypted data is inevitably linked to the secrecy of the key. A problem arises when communicating directly with another party: the key has to be initially shared between the parties, but subsequently kept secure.

In asymmetric encryption, two keys are used: a public key is used for encryption while a private key is used for decryption. Both keys are mathematically intertwined. However the private key cannot be derived from the public one. RSA encryption, named after its creators Ron Rivest, Adi Shamir and Leonard Adleman is a widely used standard for asymmetric encryption.

Private and public keys with identities

The initial problem of distributing keys and keeping them safe is solved with the separation of the key into public and private parts. Only the private key remains secret. The public key which is used for encryption is not secret: it can be found and used by anyone, similar to a telephone number. Only that under this number, only the owner of the private key can be reached.

Asymmetric key pairs are assigned to identities. This is the core principle of the Public Key Infrastructure (PKI) model – the basis of public key cryptology – which enables secure communication within an insecure network. Public keys are issued as certificates to known identities and disseminated. By checking the authenticity and validity of the certificates, identities can be established beyond doubt at any given time.

PKIs are used for secure email communication by encrypting messages with certificates. Only the owner of the private key for a particular certificate can decrypt the message. Moreover, the PKI model allows the creation of digital signatures which are also used for secure email communication.

Public keys are turned into PKI certificates

For PKI based email encryption, two standards have become established: S/MIME and OpenPGP. Both use basically the same cryptographic method. However, they differ in the certification of the public key and thus confidence in the models (see Fig. 2).

S/MIME stands for Secure/Multipurpose Internet Mail Extension and defines a standard using X.509 certificates. The certification of public keys is offered as a paid service by public certificate authorities (CAs). The trust model is hierarchical. Identities are verified through a certificates chain from the user certificate, to subCAs and eventually to the root CA-certificate of the issuing authority.

Fig 2: S/MIME and OpenPGP use different trust models.

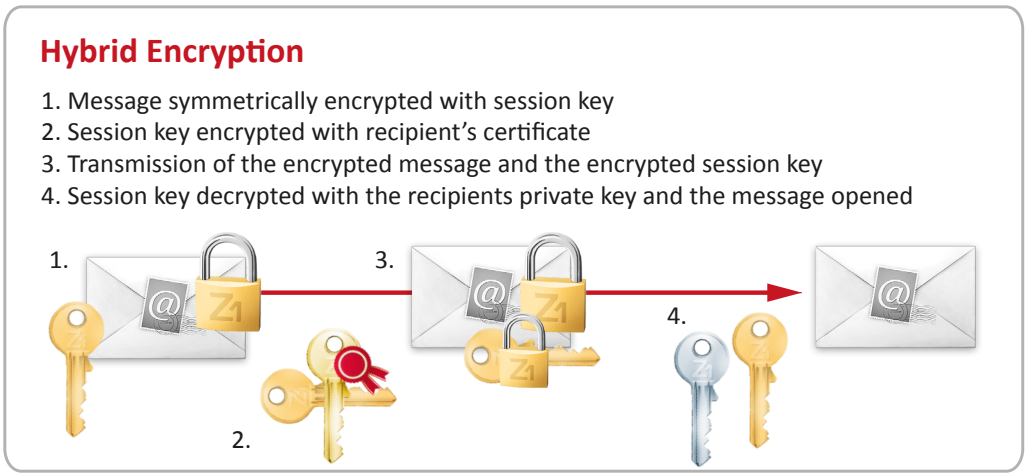


Fig. 3: Core functions of hybrid encryption.

During the enrollment process, the key pairs are generated. The private key remains with the owner while the public key is signed with this private key and then sent to the CA for certification. The CA adds its own signature to the key and sends back a signed public key. From this moment onwards, the public key is a certificate.

X.509 certificates have a limited lifetime and are divided into different classes. These classes however are not standardized. A class 1 certificate usually certifies that a public key and email address belong together. Higher classes can require notarial authentication. S/MIME is implemented as communication standard in most common email clients which also use the CA and subCA certificates of the common certificate authorities to validate user certificates.

OpenPGP (Pretty Good Privacy) is based upon the principle that participants reciprocally sign and thereby validate their keys. This generates a non-hierarchical "Web of Trust". Key pairs are generated autonomously and public keys certified by other users – for example at signing parties.

OpenPGP is not installed in common email clients, which means that users have to install a client program such as Enigmail for Thunderbird. The use of both PGP and S/MIME in webmail clients is not satisfactorily solved yet.

With regard to security aspects, OpenPGP is safer than S/MIME since some certificate authorities have already been compromised and forced to issue forged certificates by government agencies.

The encryption of a message

In the light of a PKI's complexity, the process of encryption itself seems almost trivial, as the following example demonstrates (see Fig. 3).

Alice wants to send an S/MIME encrypted message to Bob. The encryption software first generates a symmetric session key. This is used to encrypt the message. The session key will then be encrypted with Bob's certificate and attached to the message.

The encrypted message now contains the information about which certificate was used to encrypt the message, so that Bob's software may now use the private key related to the certificate to decrypt the message.

Bob receives the message. With his private key, he can now first decrypt the symmetrical session key generated by Alice's encryption program. The session key can then be used to decrypt the original message.

This mixture of symmetric and asymmetric techniques, called hybrid encryption is common practice and is mainly used for performance reasons. Asymmetric encryption of the original file would rapidly become inefficient due to the large amounts of computing effort it requires. Asymmetric encryption of a session key on the other hand is fast and is sufficient to guarantee the message security. Even when an email is sent to multiple recipients, the original information is encrypted only once with the session key, which in turn is then encrypted with each recipient's certificate.

Security in certificate and key management

Confidential communication between Alice and Bob as described above is merely an over simplified example. As a prerequisite to any encryption, the following questions have to be answered: Where does Alice gets Bob's certificate? Is this certificate real? Is it valid?

It is indispensable that Alice can find Bob's certificate. The verification of the certificate protects against so-called "man in the middle" attacks. In such an exploit, somebody with a forged certificate pretends to be Bob. He intercepts the message and then forwards it to Bob using Bob's real certificate. This could go on for weeks or months without neither Bob nor Alice being aware of it. Without a validation step, even a revoked certificate can be used by an attacker.

The complexity of a PKI and the volume of information required for authenticating and validating certificates makes a manual management of keys and certificates almost impossible. As a result, certificate servers have been developed for this purpose, automating key and certificate management, including their verification and validation (see Fig. 4).

Certificate servers are connected via diverse interfaces to certificate authorities and the CAs of large corporation. They check validity using Certificate Revocation Lists (CRLs) and conduct real time verification checks using Online Certificate Service Protocols (OCSPs). This mechanism retrieves data, checks integrity using check-sum comparison and keeps the local certificate repository constantly up-to-date. Z1 Global TrustPoint[2] is a freely available public certificate server which provides this functionality including certificate publication.

Besides their use in email encryption, the certificate servers can also be used by other PKI based applications. Instead of a natural person, a certificate owner can be a system – for example identified by its host name or IP address.

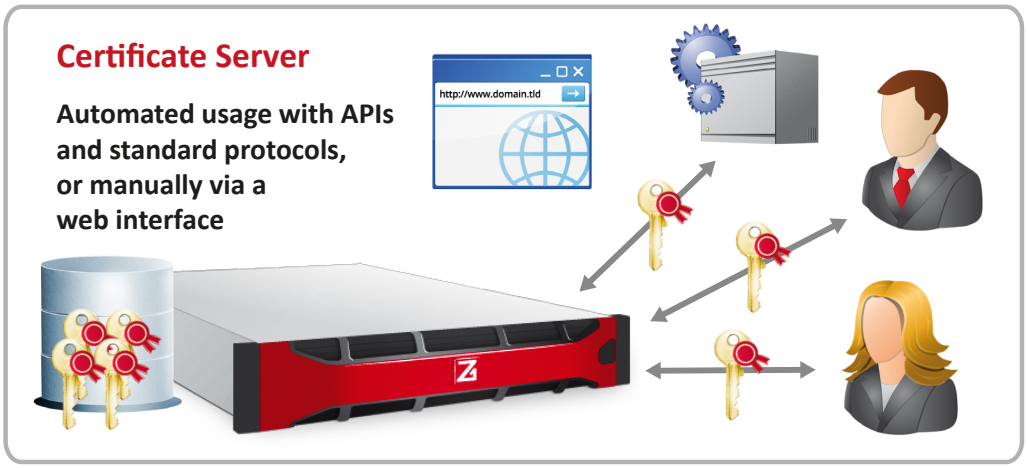


Fig 4: Certificate servers automate the management of keys and certificates.

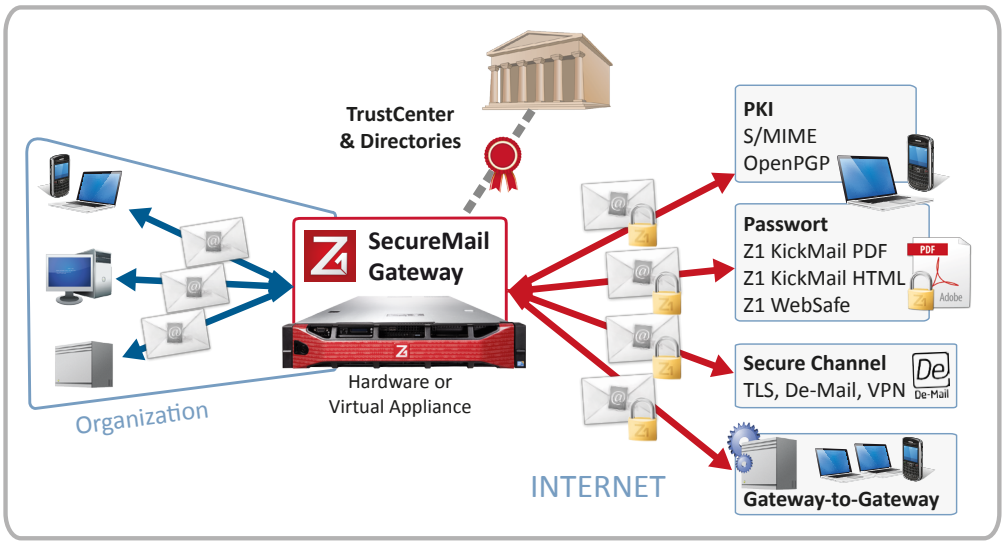


Fig. 5: Email encryption with Z1 SecureMail Gateway

Secure email gateways – server-based email encryption

In email encryption, so-called secure email gateways are widespread (see Fig. 5). These secure server-based systems handle the complete email traffic according to policies for users centrally and transparently. Compliance conformity and high user acceptance without the need for client-side software make the use of gateways efficient and profitable. Secure email gateways interact with certificate servers to implement PKI based encryption.

For communication partners without PKI, alternative secure delivery methods in which a password replaces the private key have been developed for secure email gateways. The security of password-based encryption is equal to PKI based encryption and represents a widely accepted and proven method of secure ad hoc encryption when PKI certificates are not available. In this case, the password is not saved as plain text in the system, but instead as an encrypted hash value. The only security challenge is the initial transmission of the password. To solve this problem different and practicable methods have been developed, including sending the password by SMS.

A secure email gateway can therefore not only provide S/MIME and OpenPGP email encryption, but also deliver password-encrypted PDF, HTML or ZIP files. Another popular alternative is the ad hoc creation of secure webmail accounts. De-Mail connectors, VPN and TLS support are also offered by some gateways.

Mobile communication demands end-to-end encryption

With a secure email gateway, one could relax and simply trust the state of the art security mechanisms. However, the gateways were originally conceived to provide encryption with external communication partners. Until a couple of years ago, it did not seem necessary to secure messages within a company's own internal network. The attacker came from outside and firewalls provided protection.

Besides the relatively new insights about government spying programs such as PRISM or Tempora, the rising use of mobile devices for email communication raises new challenges. Emails distributed via smart phone or notebook are sent in plain text within the internal communication network which in turn relies more and more on mobile communication channels or public WLAN infrastructures.

One possible solution to this problem can be found in end-to-end encryption. This approach is interpreted differently by each manufacturer and in its purest form carries a number of business risks. We will present the most general form of end-to-end encryption along with two different interpretations.

"Real" End-to-end encryption

In real end-to-end encryption, a message is encrypted immediately in the email client and can only be decrypted by the recipients email program (see Fig. 6). The message remains encrypted even in the email client's inbox. It is impossible for any system to view the message content during its transmission through the network. This means though that centralized content filters including virus/spam checkers, data loss prevention and archiving systems cannot be used, which increases the risks for the business.

This solution however, is not practical for spontaneous secure email communication even when a certificate server is used. The sender and recipient both need to use exactly the same standard: S/MIME or OpenPGP.

End-to-end encryption with X.509 certificates

When end-to-end encryption is required, but no certificate for the recipient can be found, the system itself can perform the certificate authority (CA) role.

In order to enforce ad hoc end-to-end encryption, Alice's dedicated certificate server issues Bob a key pair generated on the fly. Alice's system generates not only an X.509 certificate, but also a private key for Bob and sends both of them to him. Bob's private key however, needs to be protected somehow during transmission. By using the key pair generated in real time, Alice can now send an encrypted message to Bob. So far, so good.

The usage of the X.509 certificate will remain restricted to Alice and Bob, because it can neither be officially trusted, nor verified by certificate servers and other email clients. PKI security standards are not met, since Alice has access to Bob's private key. Moreover, such a certificate's rank of trust is very low – less than 1 since Bob's email address could not be confirmed.

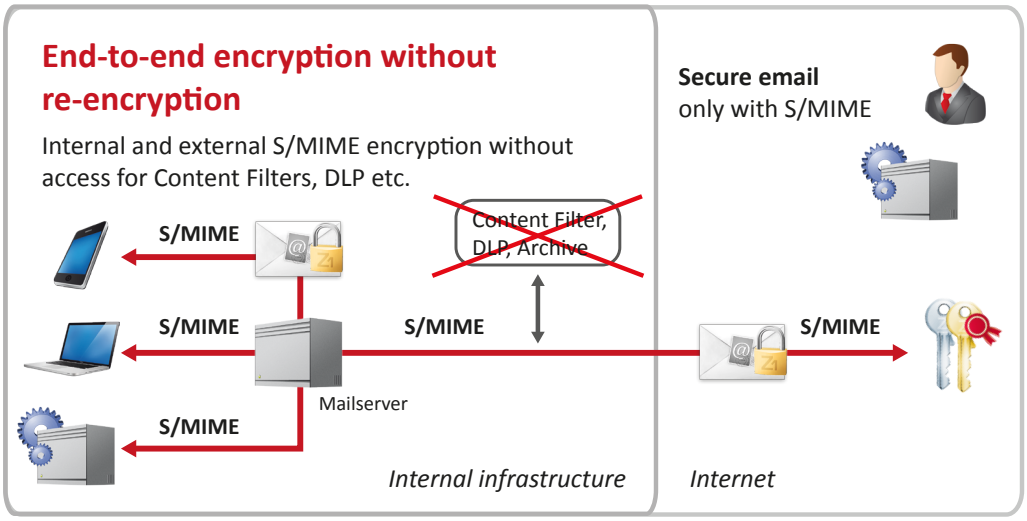


Fig. 6: "Real" End-to-end encryption

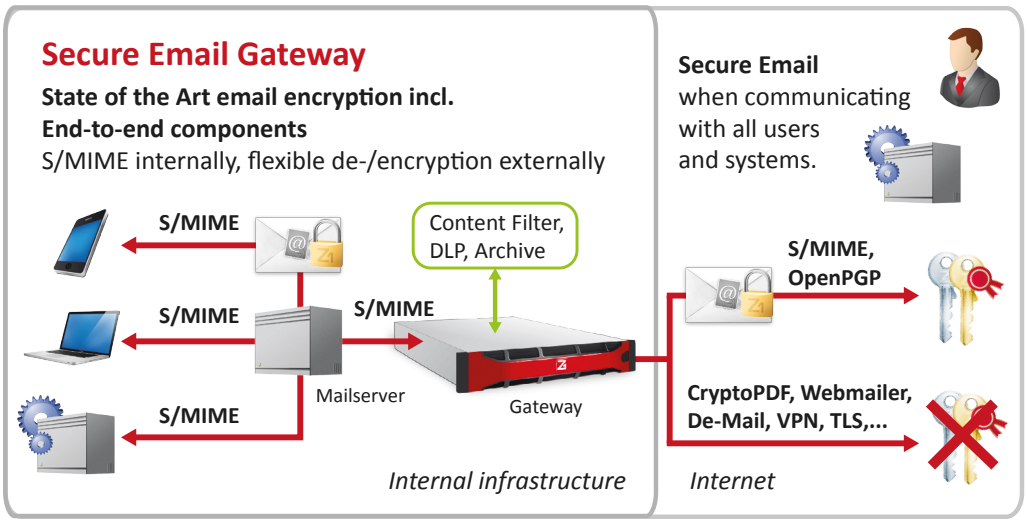


Fig. 7: End-to-end encryption with flexible re-encryption on the gateway.

In the meantime, a Public Key Infrastructure has been forced upon Bob. If he can use the certificate or not, depends on the administration rights in his email client. The solution is restricted to S/MIME, and even Bob's publicly available OpenPGP key is not any help. If Bob has contact with lots of companies he will quickly have a large collection of certificates. An explanation of the limited use of the pseudo-certificates is therefore essential.

The solution remains a compromise if there is not any access to the mail server.

End-to-end encryption with flexible re-encryption

Modern secure email gateways with extensions enable a connection between internal and external email encryption, so that messages are encrypted not only when they are sent over the Internet but also when transmitted within the company network (see Fig 7). To achieve this, an encapsulated internal PKI is set up, implementing S/MIME encryption directly on the client. The dedicated X.509 certificates issued exclusively for this purpose will never be published outside the company, so that the problem of trust on external certificate servers and email clients will never arise.

Outgoing emails are encrypted on the client with the S/MIME certificate of the gateway – email clients support S/MIME, while for mobile devices several easily installed Apps are available. The secure email gateway decrypts the message and queries the recipient's certificate. Depending on the availability of external communication partner's certificates, a re-encryption into S/MIME, OpenPGP, CryptoPDF, De-Mail, TLS, etc. is performed.

In the other direction, every encrypted incoming message will reach the internal end user as S/MIME encrypted email. During re-encryption, virus and spam checking as well as DLP and archiving can be performed.

Some secure email gateways can be combined with real end-to-end encryption which may be required for a limited number of recipients.

Criteria for a solid trust base

Strict laws on privacy protection, government agencies who do not practice industrial espionage and governments who do not influence internet and IT service providers – such ideal conditions are not available all over the world. In Germany however, IT security can be developed without having to include secret back doors.

In proprietary IT security solutions, not only the trust in the suppliers plays a decisive role, but also the trust in the suppliers country. Furthermore, it has to be remembered that the sender and receiver must use the same solution and are then limited to the devices on which the software is installed.

Made in Germany: The future of Secure Email Gateways is safe

The Gateway concept is future-proofed with the combination of internal and external encryption techniques. Some manufacturers provide extra extensions that integrate the secure transfer of large files alongside message encryption features.

When considering an investment in an encryption solution, it is important to consider not only the suppliers geographical location but also whether the primary motivation is security or compliance. In addition it is important to consider the size and diversity of the potential communication partners.

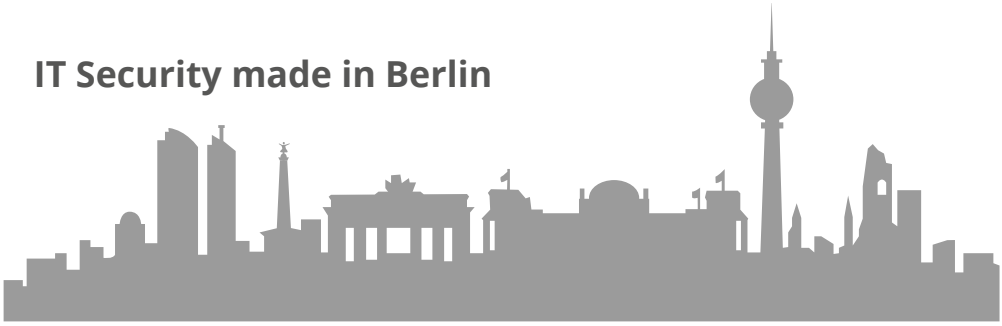
List of references:

(1) http://www.golem.de/news/verschluesselung-was-noch-sicher-ist-1309-101457-3.html
(2) https://www.globaltrustpoint.com

This white paper is also published in:
IT-Sicherheit 2/2014, Datakontext, Verlagsgruppe Hüthig Jehle Rehm, p. 41-45

Zertificon Solutions GmbH

Zertificon is a leading software manufacturer for IT security located in Berlin, Germany. An independent, founder-led company, Zertificon currently has more than 50 employees in its in-house development, sales and support departments. The award winning Z1 SecureMail Gateway has established Zertificon as a pioneer in the market for server-based email encryption for more than ten years. Through ground-breaking developments, Zertificon remains one of today's driving forces in email encryption solutions.



The focus is on delivering user friendly and economical turn-key solutions for secure email and data exchange. The popular **Z1 SecureMail Gateway** and **Z1 CertServer** for email encryption, digital signing and certificate management are complemented by Zertificon's **Z1 SecureHub** for secure web-based exchange of data files in any size and format.

The latest innovation from Zertificon – **Z1 SecureMail End2End** – provides state of the art end-to-end email encryption for organizations when combined with Z1 SecureMail Gateway. The organizational end-to-end mode allows immediate end-to-end encryption – all that is required is a recipient email address. Clients are able to connect seamlessly using the Z1 MyCrypt add-in for MS-Outlook and Lotus Notes or mobile app for iOS & Android. Z1 MyCrypt Mail supports end-to-end encryption alongside security features for server-based encryption whilst Z1 MyCrypt BigAttach integrates the web-based Z1 SecureHub into mail clients. Z1 MyCrypt integrate closely with all Z1 Server products. These new developments reliably meet the unique security demands of increased mobile communication via smart phones, tablets etc. in corporate environments.

For a simple, efficient and smooth operation of Z1 products, Zertificon offers its **Z1 Appliances** – as hardware or virtualized – optimized platforms for a full integration into existing IT infrastructures. Additionally, Zertificon's renowned support service offers rapid and personalized help for all product-related questions.

Accordingly, Zertificon enables companies and institutions of all branches and sizes to easily fulfill the highest security and compliance demands.