s/mail

Approved email encryption and signature

s/mail provides encryption and digital signatures for emails on the highest security level currently available on the market. The German Armed Forces and several other military organisations in other countries use s/mail together with Microsoft Outlook or IBM Notes to assure strict confidentiality.

MANAGEMENT SUMMARY

Email is not only the most popular internet application, but also a very security-critical one. It is not very difficult to forge an email, and there are always persons (administrators, service staff, . . .), who can read other people's messages. For these reasons encrypting and digitally signing emails are important.

s/mail is a program that protects emails from these threats. It provides email encryption and digital signature assuring the highest security level that is available on the market.

Other ways to gain email security, like gateway-based encryption or built-in crypto functions of mail clients are only good enough for low- or medium-level security. For instance, if an email is encrypted at the gateway, everyone having access to the email on its way from the client to the gateway can read it, which is normally not the intention of the author. Built-in protection functions are usually not designed (and not evaluated) to meet high security needs.

As the only product of its kind, s/mail has an approval for „VS - Nur für den Dienstgebrauch", NATO Restricted, and EU Restricted data issued by the Germal Federal IT Security Agency (BSI). s/mail is used, among others, by the German armed forces (Bundeswehr).

s/mail is available as a plugin for Microsoft Outlook and IBM Notes. Convenience for both users and administrators have been important design-goals in the development process of s/mail. User interaction is kept to a minimum, encryption and signing are performed with a minimum of user input. The user-interface is seamlessly integrated into the respective email client. Flexible group policies allow for easy administration and preconfiguration.

BACKGROUND

Email Encryption And Signature

In spite of the World Wide Web, email is still the most popular internet application. As secret information are exchanged by email, it is crucial to observe security requirements. An email can be secured by encryption or by digital signature (the two techniques can be combined). Encryption is used to ensure confidentiality, while digital signatures assure non-repudiation. The most common way to encrypt and sign emails is based on the S/MIME standard and digital certificates, which are provided by a Public Key Infrastructure (PKI).

Emails can be secured at two locations: either on the client, where the email is written, or on a gateway. For low and medium security requirements it is often sufficient to operate a gateway.

However, an email protection gateway neither provides end-to-end security nor personal digital signatures. For enterprises requiring a high security level client-based email protection is therefore a must. In theory, the native crypto functionality provided by the popular email clients can be used for this purpose, but usually these tools don’t have the security evaluations required by organizations with high security needs. Instead, evaluated add-ons (plug-ins) have to be used. Such a plug-in may be seamlessly integrated into the email client.

PKI Support

The digital certificates used by s/mail are typically provided by a Public Key Infrastructure (PKI). s/mail supports a wide range of functionality for PKI interoperation. Among others, s/mail supports X.509 certificate handling, revocation lists, OCSP validity checks, PKCS#10 requests and PKCS#12 import/export.

Elliptic Curves

s/mail supports Elliptic Curve Cryptography (ECC). ECC algorithms, which are gaining more and more popularity, are more performant than conventional cryptographic methods. Therefore they enable the use of cheaper smart card chips with the same level of security. Several national information security authorities (for instance the German BSI) have committed to Elliptic Curve Cryptography as the preferred technology of its kind. Among others, Windows Vista and Windows 7 support ECC.

THE BASICS

s/mail

s/mail is one of the most powerful and secure client-based email encryption solutions on the market. As a plug-in for Microsoft Outlook or IBM Notes it integrates seamlessly into the respective email client and encapsulates crypto functionality from the rest of the system.

Security Approval

As the only solution of its kind, s/mail has an approval for VS-NfD, NATO Restricted, and EU Restricted data by the German authorities.

Powerful Administration

s/mail includes administration via group policies. It can be determined, which functionality and options are available for the users. An administrator can even define which level of security a user has to meet.

Standardized Cryptography

s/mail uses symmetric and asymmetric cryptography based on standards (S/MIME, PKIX, X.509, and PKCS#1). The digital certificates used are usually provided by the Certification Authority (CA) of a Public Key Infrastructure (PKI). As one of the first email plug-ins s/mail fully supports the RSA algorithm according to the PKCS1v2.2 standard, which provides especially robust and provably secure padding schemes.

Smart Card Support

s/mail includes a powerful smart card and token support. Digital certificates on a card chip are automatically detected and registered. Upon removal of the smart card automatic deregistration can be configured. Smart cards are utilized either native or through the standardized PKCS#11 interface.

Digital Signatures

s/mail supports digital signatures created by a smart card. Such signatures and the corresponding certificates are validated according to PKIX with certificate status information provided by LDAP, HTTP or OCSP.

Integration

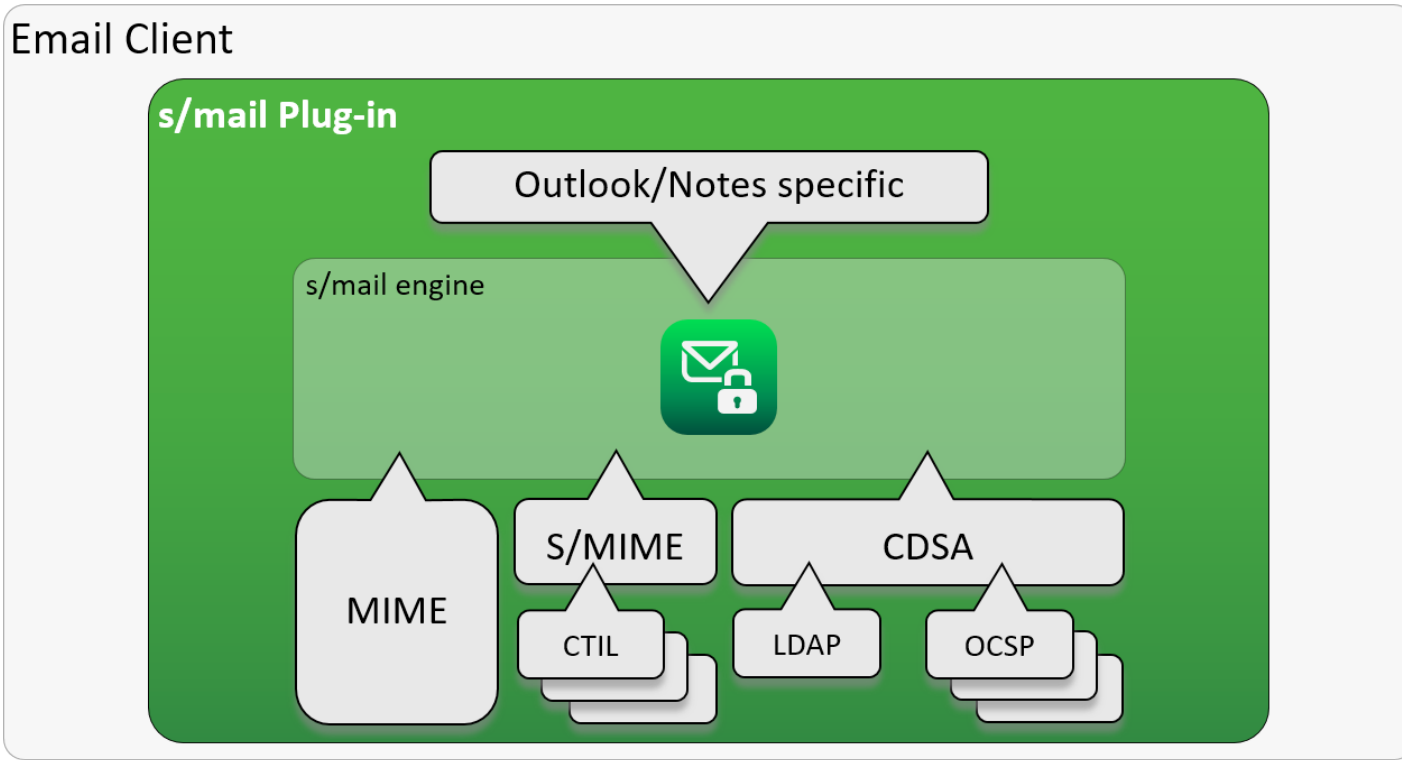
As s/mail works as a plug-in, users have to adjust themselves only to minimal changes during their work with emails. Most of the cryptographic processes are computed without any user interaction. In some cases a user has to provide a PIN or a passphrase.

Additional Functionality

s/mail supports a powerful message recovery function, advanced role handling including substitution rules, and many other advanced features.

THE TECHNICAL PART

s/mail realizes email encryption and email signatures as a plug-in for Microsoft Outlook and IBM Notes. Because of a deep integration only little user interaction is required.



THE MODULES

Architecture

The architecture of s/mail is strictly modular. During development much effort was spent on flexible core components, which minimize platform dependencies. In s/mail's architecture, these core components take center stage. They implement all cryptographic functions including encryption and digital signatures, decryption and signature verification. The core components also handle certificate verification including chain building. Both certificate revocation lists (via LDAP or HTTP) and OCSP are supported.

s/mail uses its own certificate database, which follows the CDSA architectural guidelines invented by Intel. The core components access private keys, e. g. on a smart card. They also include cryptographic libraries that are responsible for creating emails according to the S/ MIME standard. In addition a MIME library is included in the core components to compute the body of an email.

Beside the core components s/mail also includes a platform specific part. This component is responsible for handling the communication between the email client and the core components. It accepts the email to be S/MIME-encoded and passes it to the core components. In the other direction it passes the S/MIME email to the email client that sends the now S/MIME-encoded email out.

High Security Level

s/mail is designed to meet even the highest security requirements. It separates the crypto functionality from the rest of the system and provides security features including smart card support.

SUPPORTED SYSTEMS

- Windows Vista, Windows 8 / 8.1 or Windows 10
- IBM Notes or Microsoft Outlook
- Smart card reader or USB port

Success story

The German Armed Forces (Bundeswehr) is the biggest IBM Notes user in Germany and also uses Microsoft Outlook. Encryption is essential for such an organization. However, the native encryption functions of Notes and Outlook neither had an appropriate security evaluation nor provided all the required functionality. s/mail turned out to be the only alternative. It is client-based, available for both Notes and Outlook, provides high security, and has a number of practical features.

In a process of several years the Bundeswehr evaluated s/mail. As a consequence, cryptovision implemented several additional features and improvements, which made s/mail an even more powerful solution. s/mail became evaluated for national military use by the German authorities (meanwhile it even has a VS-NfD, NATO Restricted and EU Restricted approval). There is no other crypto product with these certifications on the market. In 2007 the Bundeswehr purchased an enterprise license.

Customers

s/mail is used (among others) by the following customers:

- Armed Forces: Apart from the German Armed Forces several military organizations in other countries use s/mail.
- German defense corporation: As a supplier of the German Armed Forces this corporation uses s/mail.
- IT company: An international IT company, which is active in the military sector, uses s/mail for their communication with the German Armed Forces.

About cryptovision

cryptovision is a leading supplier of innovative cryptographic IT security solutions. Based on its two decades of market experience and broad background in modern cryptographic techniques, such as Elliptic Curve Cryptography, all cryptovision products provide the most state-of-the-art and future-proof technologies. The company specializes in lean add-on components which can be integrated into nearly any IT system to gain more security in a both convenient and cost-effective way.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 500 million people worldwide make use of cryptovision products every day in such diverse sectors as defense, automotive, financial, government, retails and industry.

cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

T: +49 (209) 16724-50
F: +49 (209) 16724-61

cv cryptovision
100 Park Avenue / Suite 1600
New York, NY 10017, USA

T: +1 (212) 984 0750
F: +1 (212) 880 6499

www.cryptovision.com