vSEC:MAIL Server

Secure Email – a Cornerstone for Secure Communications

Digital signatures and encryption is the industry standard for securing email communication and has been for many years, even to the point that it is now in many regions legally binding. The most widely used standard for adopting digitally signed and encrypted email is S/MIME – all email clients available on the market support this standard – this means that everybody has the capability to receive an email that has been digitally signed according to S/MIME and they can also verify that it has a valid signature. To send a signed email, the sender has to acquire a certificate and hold his/her associated private key. When the user has a certificate, the user is ready to receive encrypted emails from other users (that has been provided with this certificate). The standards are there and the applications can use them, but the infrastructure and the processes to make email signing/encryption used for all communication has been complex for many organizations, vSEC:MAIL Server addresses this issue and automates the procedure.

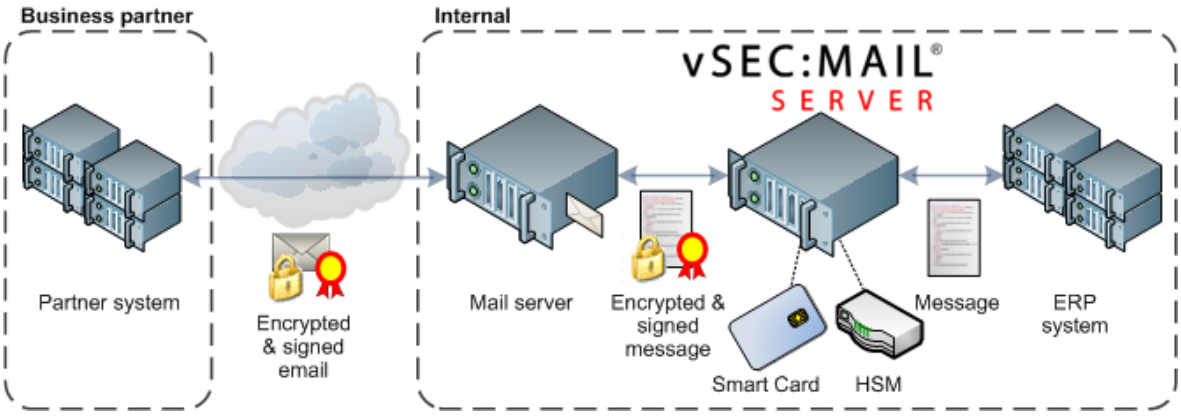

Figure 1: vSEC:MAIL Server – Example Use Case

vSEC:MAIL Server Features

Using vSEC:MAIL Server from Versatile Security legacy systems can transparently use S/MIME email communication. vSEC:MAIL Server supports all the most widely used email protocols (SMTP, POP3 and IMAP4, also in the context of EDI standard AS1) and other protocols common in B2B communication (HTTP/AS2, FTP/AS3). The vSEC:MAIL Server runs in a fully transparent proxy mode at a central location to generate and/or handle S/MIME secured communication. It is a proven stable and scalable .NET based solution and runs as a Windows Service. It uses X.509 certificates and private keys provided by Microsoft Windows crypto capabilities (CAPI/CNG) - smart card support is also available.

Certificate revocation checks are available using CRLs or OCSP. The vSEC:MAIL Server is customizable in several ways, for example by dynamically loaded filters for email manipulation and dynamically loaded connectors for system integration. The product consists of the vSEC:MAIL Server (the core service) and the vSEC Server Console (the administration console). It can easily be integrated into an existing IT infrastructure. It is a PKI-enabled email server component that supports several interfaces. It supports all the S/MIME cryptographic tasks: encryption, decryption, signing and verification.

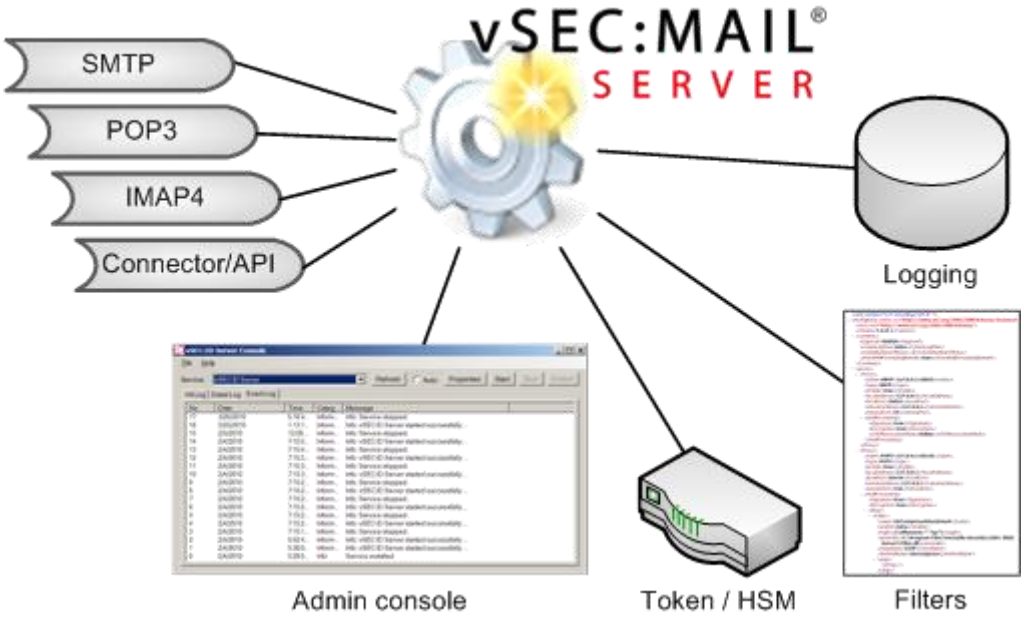

Figure 2: vSEC:MAIL Server - Interfaces

Technical Specifications

Operating Systems

- MS Windows
  - XP, Vista, 7, 8, 2003, 2008, 2012,
  - 32bit, 64bit
  - .NET 2.0

Functionality

- S/MIME email
- Client and proxy mode for SMTP, POP3 and IMAP4 (unlimited number of instances/threads)
- Client mode for FTP
- Server mode SMTP, POP3 and IMAP4
- EDI protocols AS1, AS2, AS3
- Verify, sign, encrypt, decrypt on PKCS#7 based signatures and envelopes (S/MIME)
- Contact based S/MIME behavior
- X.509 certificates and private keys provided by Microsoft CSPs
- Certificate revocation checks: CRL, OCSP
- TLS, STARTTLS and IPv6 for all protocols
- Windows Service
- Management and configuration console
- Hit log and Audit log
- Customizable: Dynamically loaded Filters for email manipulation and Connectors for integration
- Archiving integration
- Highly scalable, multi-threaded

Standards Compliancy

- RFC5312: Simple Mail Transfer Protocol (SMTP)
- RFC1939: Post Office Protocol - Version 3 (POP3)
- RFC3501: Internet Message Access Protocol - Version 4rev1 (IMAP4)
- RFC3851: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- RFC1847: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
- RFC2560: Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- RFC5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
- RFC5652: Cryptographic Message Syntax (CMS)
- Public Key Cryptography Standards (PKCS) (important are: PKCS#1, PKCS#7)

Cryptography

- .NET access to Microsoft CSPs