



s/mail

Email encryption and digital signature

cryptovision's s/mail is a solution for encrypting and signing emails. s/mail is realized as a plug-in for standard email systems. It is client-based and integrates into Microsoft Outlook and IBM Notes, which means that a mail is secured from end to end (in contrast to a gateway solution). It supports smart cards and a large number of special features.

Functions	All functionalities for end-to-end security in email communication: <ul style="list-style-type: none"> • Signing and verification of emails • Encryption and decryption of emails • modules to manage keys and certificates
Features	<ul style="list-style-type: none"> • Supports smart cards / USB tokens / soft keys • Generation of self-signed certificates / certificate requests • Generation of standard keys • PIN cache mechanisms • Watchdog function (automated smart card import) • Message recovery mechanisms • Centralized administration and distribution of policies via group policies • Multi Trust Center compatible • LDAP / OCSP / HTTP support / HTTP Proxy • TeleSec & eTrust certificate verification (certificate chain model) • X.509 version 3 certificates + CRL
Scope of Supply	<ul style="list-style-type: none"> • s/mail plugin for Microsoft Outlook • s/mail plugin for IBM Notes • Watchdog daemon service • Management Component and Administrative Templates
Supported Standards	<ul style="list-style-type: none"> • S/MIME version 3.2 including ECC • PKCS#11 • PKIX • Mailtrust • CDSA security architecture • PRNG following TR2101-1 / random from smart card

Evaluations and Certifications	<ul style="list-style-type: none"> • SPHINX certificated (S/MIME interoperability) • Approved for "VS – Nur für den Dienstgebrauch", NATO Restricted, and EU Restricted by the German authorities
Supported Algorithms	<p>Asymmetric algorithms:</p> <ul style="list-style-type: none"> • RSA (up to 16384 bit, up to PKCS1#v2 incl. PSS/OAEP) • DSA/DH (up to 2048 bit) • ECC (up to 571 bit): NIST and Brainpool curves <p>Symmetric algorithms:</p> <ul style="list-style-type: none"> • DES (56 bit) • Triple-DES (168 bit) • RC2 (40 bit, 64 bit, 128 bit) • AES (128 bit, 196 bit, 256 bit) <p>Hash algorithms:</p> <ul style="list-style-type: none"> • SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 • RIPEMD-128, RIPEMD-140, RIPEMD-160 • MD2, MD4, MD5
Supported Platforms	<ul style="list-style-type: none"> • Microsoft Outlook 2007 / 2010 / 2013 • IBM Notes 8.0.x / 8.5.x / 9.0.x
System Requirements	<p>Workstation operating system:</p> <ul style="list-style-type: none"> • Windows 7 / 8.1 / 10 <p>Works with:</p> <ul style="list-style-type: none"> • IBM Domino 7.x or higher • Microsoft Exchange 2000 or higher • IMAP POP3 SMTP