

# Unsere Softwarelösungen

Die fideAS®-Produktfamilie



## fideAS® mail

**fideAS® mail macht Ihre E-Mails sicher –  
ohne Mehraufwand für den Empfänger**

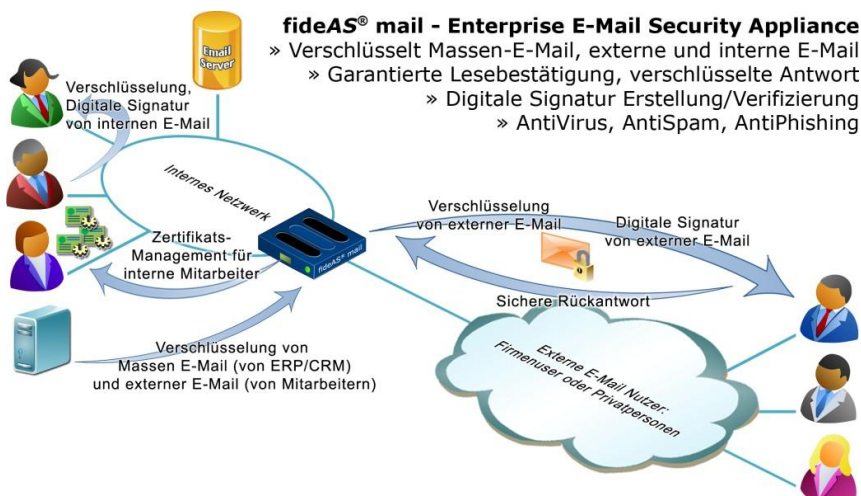
Der Versand von verschlüsselten E-Mails, die den hohen gesetzlichen Standards bezüglich Datenschutz genügen, war bisher ein teures und kompliziertes Unterfangen.

Für eine sichere Verschlüsselung brauchte es bisher auf beiden Seiten – also sowohl beim Versender als auch beim Empfänger – aufwändige Softwareinstallationen.

**Die fideAS® mail-Technologie schafft Abhilfe:**

Der Empfänger Ihrer E-Mails benötigt zur Entschlüsselung nichts weiter als sein gewohntes E-Mail-Programm.

Durch die patentierte Technologie ist auch ein Zwischenspeichern der versandten Mails – wie dies bei einer „sicheren Webmail“ der Fall ist – nicht nötig. Die Mails werden vollständig verschlüsselt an den Empfänger ausgeliefert.



**Die Vorteile der patentierten Push-Technologie in fideAS® mail**

Die fideAS® mail-Technologie beruht auf einem patentierten Push-Verfahren. Die E-Mails werden dabei in einem verschlüsselten HTML-Attachment an den Empfänger ausgeliefert. Um die Mail lesen zu können, braucht der Empfänger neben der empfangenen E-Mail ein Passwort, welches ihm einmalig per SMS, Telefon oder Fax übermittelt wird. Im Vergleich zu anderen Lösungen, bei denen eine „sichere Webmail“, „PDF-Verschlüsselung“ oder ähnliches eingesetzt wird, entstehen durch die fideAS® mail-Technologie folgende Vorteile:

**Zwei Faktoren Authentifizierung:** Eine „sichere Webmail“ ohne zusätzliche technische Sicherheitseinrichtungen wie OTP-Token ist in der Praxis weniger sicher als herkömmlicher, unverschlüsselter E-Mailverkehr, da es relativ einfach durch Phishing bzw. durch eine Mailspoofing-Attacke ausgehebelt werden kann. fideAS® mail bietet den Komfort einer „sicheren Webmail“ mit einer zwei Faktoren Authentifizierung (empfangene E-Mail und Passwort) auch ohne zusätzliche, teure Token.



Ihr Vertriebspartner:

**QKomm GmbH**  
In Gerderhahn 36a, D-41812 Erkelenz  
Tel.: 0 24 31/ 980 893, Fax: 0 24 31/ 980 894,  
e-mail: office@qkomm.de, www.qkomm.de

## fideAS® mail auf einen Blick

- Automatische Verschlüsselung und Entschlüsselung
- Verschlüsselungsstandards: OpenPGP, S/MIME, TLS, fideAS® mail
- Versenden und Empfangen von E-Mails im gewohnten E-Mail Client, kein Plugin nötig
- Der Empfänger benötigt keine Software zur Entschlüsselung
- Hochverfügbarkeit (integrierter Multimaster Cluster)
- Anpassung an Security Policy durch programmierbare Rule Engine
- Optionale Verschlüsselung interner E-Mails
- Anbindung an LDAP/ADS möglich
- Optionaler Schutz gegen Viren, Spam und Phishing
- Automatische Firmensignatur und Disclaimer
- Zentrale User- und Schlüsselverwaltung
- Übersichtliche Mail-Logs und Statistikfunktionen
- Garantierte Lesebestätigung bei fideAS® mail Nachrichten
- Geringer Administrationsaufwand
- Keine Softwareinstallation notwendig

# Unsere Softwarelösungen

## Die fideAS®-Produktfamilie

### Übersicht:

#### fideAS® mail small business

- Kleine Unternehmungen, bis zu 50 fideAS® mail Benutzer
- Appliance, Desktop Format

#### fideAS® mail medium business

- Kleine bis mittlere Unternehmungen, bis zu 500 fideAS® mail Benutzer
- Appliance, 19" Rack Format

#### fideAS® mail enterprise

- Unternehmungen mit über 500 fideAS® mail Benutzern
- Hochverfügbarkeit
- Appliance, 19" Rack Format

#### fideAS® mail VM

- für virtuelle Umgebungen und private Clouds

### Anwendungen:

- e-Statement
- e-Verträge
- e-Attestierung
- e-Banking
- e-Health / e-Government
- e-Reservierung
- ERP und CRM Integration
- Automatisiertes Reporting
- Eindeutige Sender Identifizierung
- Sichere Übermittlung vertraulicher Daten
- Übermittlung personenbezogener Daten konform zum BDSG

fideAS® mail powered by SEPPmail

**Interne Verschlüsselung:** Neben der externen E-Mail Verschlüsselung bietet fideAS® mail auch ein erweitertes Schlüsselmanagement für die interne E-Mail Verschlüsselung mit dem S/MIME-Standard. Die Generierung der Benutzer-Schlüssel und Zertifikate wird zentral gesteuert und die Zertifikate werden über das Active Directory oder einem eigenen Verzeichnisdienst verteilt.

**Digitale E-Mail Signatur:** Elektronische Signatur von ausgehenden E-Mails für eindeutige Identifikation des Senders durch beliebige E-Mail Empfänger. Vollautomatische Prüfung von eingehenden elektronisch signierten E-Mails mit Prüfbestätigung. Unterstützt werden die fortgeschrittene Signatur mit TrustCenter Zertifikaten oder die einfache Signatur.

**Clustering:** Bei fideAS® mail werden die gesendeten E-Mails nicht auf der Appliance gespeichert. Neben geringem Verwaltungsaufwand und höherer Sicherheit bietet dies den Vorteil, dass eine fideAS® mail-Appliance mit einem einfachen Backup File jederzeit wiederhergestellt werden kann und das Clustering standortunabhängig auch über langsame Verbindungen realisierbar ist.

Leistungsumfang	fideAS® mail small business	fideAS® mail medium business	fideAS® mail enterprise
Abmessungen (BxHxT)	325x88x200mm	19" Rack, 1HE ,T=356mm	19" Rack, 1HE, T=650mm
Leistungsaufnahme	250 Watt	260 Watt	450 Watt/Redundant
Netzwerkschnittstellen	2x100/1000 Mbits	2x10/100/1000 Mbits	2x10/100/1000 Mbits
Speicher	SSD Card	250 GB SATA HDD	2x73 GB SAS HDD (RAID 1)
Verschlüsselung	OpenPGP, S/MIME, TLS, fideAS® mail		
Asymmetrische Algorithmen	RSA, DSA, ElGamal, Diffie-Hellman u.a.		
Symmetrische Algorithmen	AES, 3DES, CAST5, Blowfish, Twofish u.a.		
Sprachen fideAS® mail-Viewer	DE, EN, FR, IT		
Zentrale Signaturprüfung	✓	✓	✓
Domainbasierte Verschlüsselung	✓	✓	✓
Backup/Restore	✓	✓	✓
Virus, Spam, Phishing Protection	Option	Option	Option
Empfohlen max. User	50	500 pro Appliance	unbegrenzt

### Sprechen Sie mit uns!

apsec bietet Ihnen umfassenden Service für alle Bereiche der Datensicherheit.

#### Beratung

- Erstellen von Sicherheitsrichtlinien,
- Gefährdungsanalysen, interne Netz-Sicherheit

#### Netzwerksicherheit

- Sicherheit im Internet/Intranet/Extranet,
- Zugangskontrolle zu Datenbanken, Firewalls, VPN, Virenschutz, Remote-Access

#### Softwaresicherheit

- kryptographische Funktionen in beliebigen Anwendungen, Aufbau von PKIs mit
- TrustCenter, sichere E-Mail, digitale Signatur, Verschlüsselung.