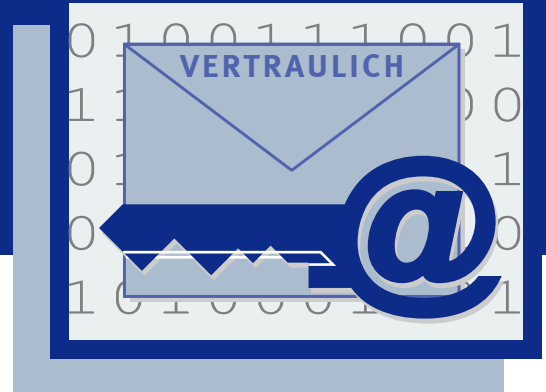


eMail-Sicherheit



Networkers

Networkers ist eines der in Deutschland führenden Unternehmen für die Planung, den Aufbau und den Betrieb von sicheren und leistungsfähigen Applikations- und Netzwerkinfrastrukturen.

Unternehmen und Organisationen bieten wir ein breites Spektrum an Services - zuverlässig, kompetent und herstellerneutral.

Strategischer Erfolgsfaktor Informationsschutz

Die eMail ist das inzwischen am häufigsten genutzte Kommunikationsmedium - insbesondere im gewerblichen Umfeld. Damit bildet sie die bedeutungsvollste Basis zum Austausch von Informationen.

Die Gründe für den rasanten Siegeszug der eMail liegen auf der Hand. Nie zuvor war eine Nachricht gleichermaßen so schnell, bequem und günstig an den Mann zu bringen. Und so wird vielerorts beinahe alles, was in elektronischer Form von A nach B übertragen werden kann, via eMail kommuniziert.

Doch Vorsicht: eMails sind alles andere als "sicher". Der Grad ihrer Vertraulichkeit, Authentizität und Integrität entspricht gerade mal dem Niveau mit Bleistift beschriebener Postkarten. Die Technik macht es möglich, dass sie recht einfach mitgelesen und verändert werden können, ohne dass dies nachweisbar wäre. Um große Schäden zu verhindern, sollten daher mindestens sensible Informationen niemals ungeschützt übertragen werden.

Einigen Konzernen und Unternehmen sowie auch immer mehr Verbänden, Kammern und Behörden geht dies nicht weit genug. Sie fordern von ihren Kommunikationspartnern die Umsetzung technisch-organisatorischer Sicherungsmaßnahmen als Voraussetzung für den weiteren Austausch geschäftlicher eMails.

Auch wohl aufgrund dessen ist die Bereitstellung von Lösungen zur eMail-Verschlüsselung und -Signierung in Unternehmen ein Thema mit stetig steigender Bedeutung. Und unabhängig davon eine sinnvolle Ergänzung der klassischen eMail-Sicherheitsmaßnahmen wie Virenschutz, Spam-Abwehr oder Mailsystem-Absicherung.

Grund genug also, eMail-Verschlüsselung und -Signierung etwas genauer zu beleuchten. Im Verlauf werden wir unter anderem den Fragen nachgehen, was konkret hinter diesen beiden Verfahren steckt, auf welchen Ideen und Hintergründen sie basieren, wie die Verfahren funktionieren und wie sie in IT-Infrastrukturen integriert werden können.

Das Zwei-Schlüssel-Verfahren (Public Key-Verfahren)

Die Verwendung kryptographischer Verfahren ist die einzige Möglichkeit um Vertraulichkeit, Integrität und Authentizität von elektronischen Dokumenten zu gewährleisten.

Man unterscheidet zwischen symmetrischen Verfahren, z.B.

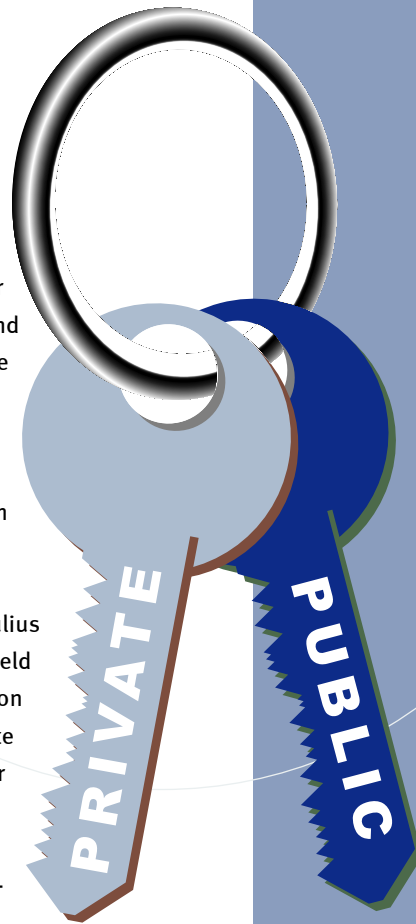
- DES/3DES (Data Encryption Standard)
- IDEA (International Data Encryption Standard)
- RC (Rivests Code)
- AES (Advanced Encryption Standard)

und asymmetrischen Verfahren

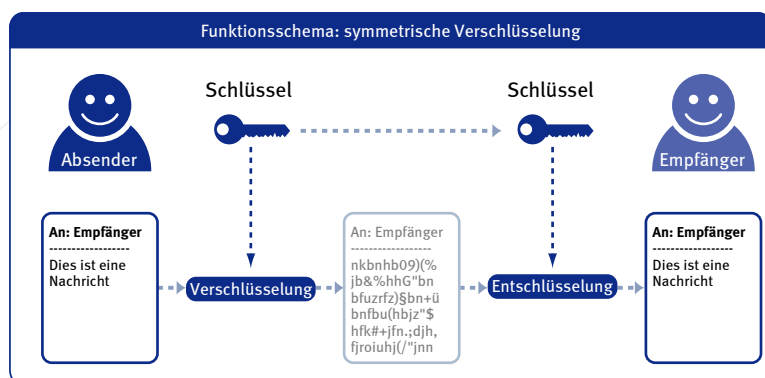
- Diffie-Hellman
- RSA (Rivest, Shamir, Adleman)
- DSA (Digital Signature Algorithm)
- ElGamal.

Beide Verfahren haben Stärken und Schwächen, vor allem hinsichtlich ihrer Verarbeitungsgeschwindigkeit und ihrer Widerstandsfähigkeit gegen Angriffe. Um die jeweiligen Vorteile konsequent zu nutzen, kommen in modernen kryptographischen Systemen zumeist hybride Verfahren - also eine Kombination aus symmetrischen und asymmetrischen Verfahren - zum Einsatz.

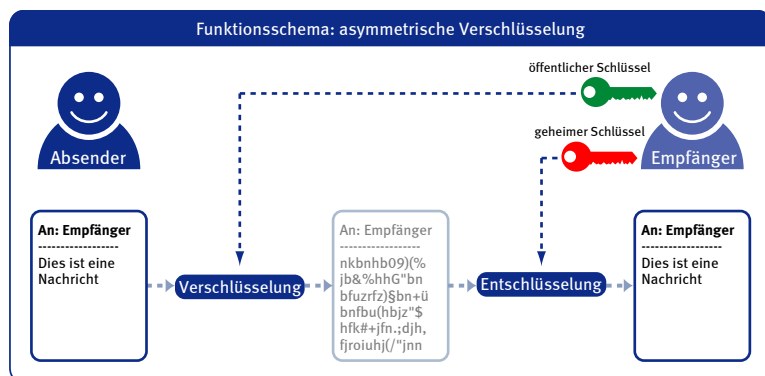
Während symmetrische Verfahren schon zu Zeiten Julius Cäsars eingesetzt wurden, stellt das 1976 von Whitfield Diffie und Martin Hellman entwickelte und 1978 von Rivest, Shamir, Adleman (RSA) in die Praxis umgesetzte Public Key-Verfahren einen echten Durchbruch in der Geschichte der Kryptographie dar. Denn durch die erstmals asymmetrische Codierung und Decodierung konnte das bis dato größte Problem der Kryptographie - der sichere Schlüsselaustausch - clever gelöst werden.



Die Methode: Bei symmetrischen Verfahren wird zur Codierung als auch zur Decodierung ein und derselbe Schlüssel verwendet. Zur Entschlüsselung muss dem Empfänger also neben der Nachricht ebenso der streng geheime Schlüssel zugeleitet werden. Das Problem: Jeder, der den Schlüssel kennt, kann die Nachricht ohne Aufwand entschlüsseln.



Asymmetrische Verfahren beruhen hingegen auf Schlüsselpaaren. Damit umgehen sie die Schwäche der symmetrischen Verfahren raffiniert: Denn eine mit dem einen Schlüssel codierte Nachricht kann nicht etwa mit demselben Schlüssel, sondern nur mit dem jeweils anderen Schlüssel (dem passenden "Bruderschlüssel") entschlüsselt werden. Der Clou bei diesem Verfahren ist, dass sowohl die verschlüsselte Nachricht als auch der zur Verschlüsselung notwendige Schlüssel über öffentliche Kanäle verteilt werden können, ohne dabei einen Verlust an Sicherheit in Kauf nehmen zu müssen.



Zwei dieser asymmetrischen Public Key-Verfahren haben sich inzwischen als de-facto Standards etabliert: PGP und S/MIME. Wie die Signierung und Verschlüsselung per PGP und S/MIME funktioniert, wird im Verlauf verdeutlicht.

Der Einsatz von Public Key-Verfahren für eMail-Signierung und eMail-Verschlüsselung

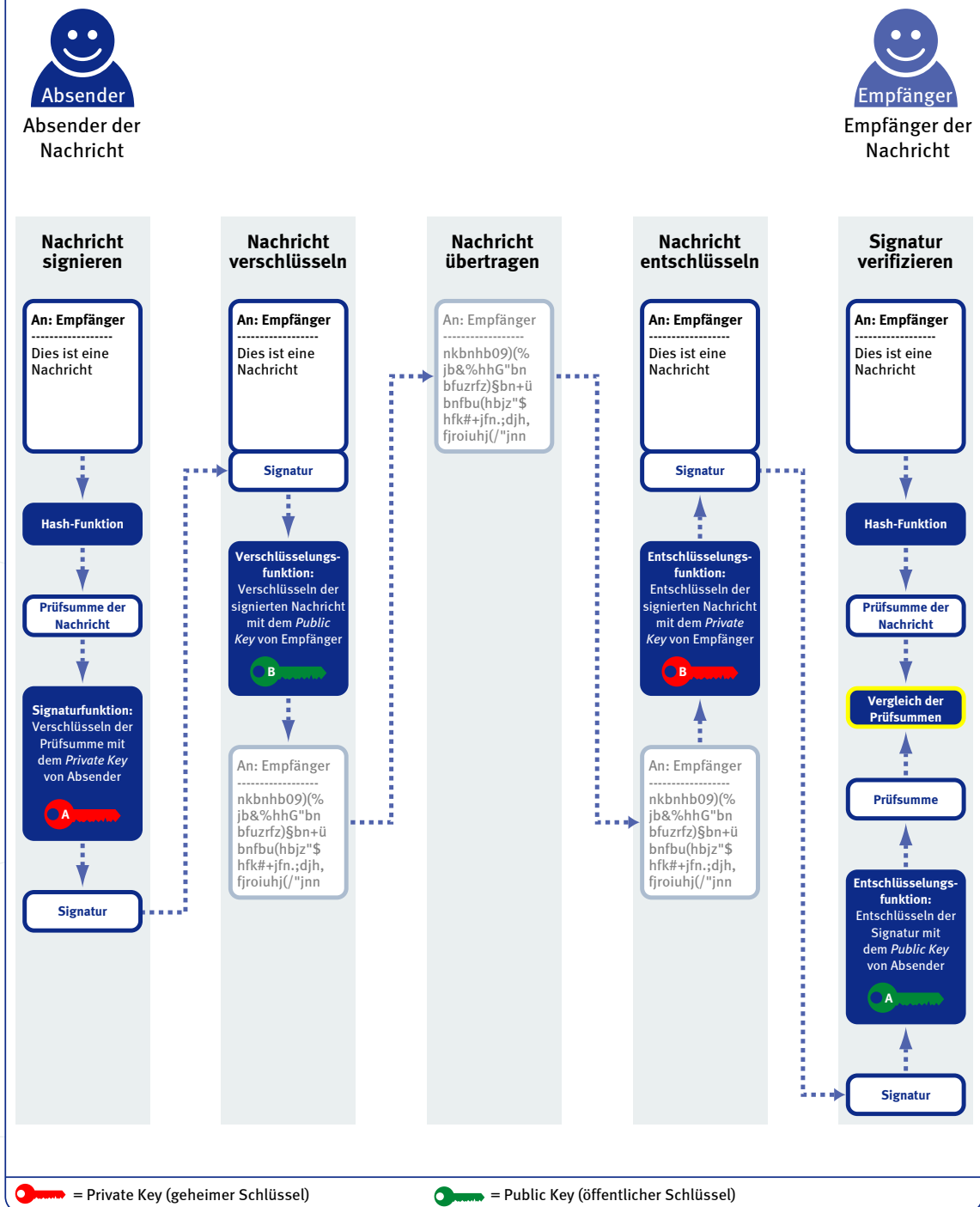
Auf welchen wesentlichen Verfahrensschritten die Signierung und Verschlüsselung von eMails beruht, ist Bestandteil dieses Kapitels.

Vorab sei darauf hingewiesen, dass die Verfahrensschritte je nach eingesetzter Software größtenteils automatisiert durchgeführt werden. Manuelle Eingaben sind - wenn überhaupt - in nur sehr geringem Umfang notwendig. Das Gros an Prozeduren wird vom Anwender vollkommen unbemerkt im Hintergrund abgewickelt.

Die Verfahrensschritte der eMail-Signierung und -Verschlüsselung

- **Erzeugen einer Prüfsumme:**
Für den Nachrichtentext wird eine eindeutige Prüfsumme erzeugt, z.B. mit einer so genannten Hash-Funktion.
- **Erzeugen der digitalen Signatur:**
Die Prüfsumme wird mit dem (streng geheimen) Private Key des Absenders verschlüsselt und damit gegen Manipulation geschützt. Das Resultat (die verschlüsselte Prüfsumme) ist die digitale Signatur dieser eMail.
- **Anhängen der digitalen Signatur:**
Die digitale Signatur wird der eigentlichen Nachricht angehängt.
- **Verschlüsselung der eMail:**
Die Nachricht und die Signatur werden zusammen mit dem Public Key des Empfängers verschlüsselt. Nun sind sowohl Text als auch Signatur gegen Einsichtnahme geschützt.
- **Versand/Zustellung:**
Versand/Zustellung der verschlüsselten und signierten eMail wird vorgenommen. Der Versand erfolgt übrigens genauso, wie bei einer unverschlüsselten und unsignierten eMail.
- **Entschlüsselung der eMail:**
Weil die Nachricht mit dem Public Key des Empfängers chiffriert worden ist, kann auch nur der angegebene Empfänger die ihm zugestellte Nachricht entschlüsseln. Und zwar mit Hilfe seines (streng geheimen) Private Keys. Nach der Entschlüsselung sieht er die Nachricht im Klartext. Ebenso sieht er auch, dass eine digitale Signatur angehängt ist.
- **Entschlüsselung der digitalen Signatur:**
Um die digitale Signatur überprüfen zu können, muss sie zunächst entschlüsselt werden. Und weil diese mit dem Private Key des Absenders verschlüsselt worden ist, entschlüsselt der Empfänger diese mit dem Public Key des Absenders.
- **Verifizierung der Prüfsumme:**
Der Empfänger erstellt durch die Anwendung der Hash-Funktion eine Prüfsumme von der zugestellten Nachricht. "Seine" Prüfsumme vergleicht er mit der, die der eMail angehängt war. Unterscheiden sich die Summen, so ist die Nachricht eindeutig manipuliert worden. Sind die Werte identisch, so ist die Nachricht eindeutig nicht manipuliert worden. Der Empfänger der eMail kann in dem Fall sehr sicher sein, dass die Nachricht verlässlich vom Absender stammt und dass sie auf dem Übertragungswege nicht verändert wurde.

Die Verfahrensschritte der eMail-Signierung und -Verschlüsselung



Auf den Seiten 6 und 7 wurden die einzelnen Verfahrensschritte der eMail-Signierung und -verschlüsselung verdeutlicht. Offen blieb jedoch eine der elementarsten Fragen, nämlich, was letztlich "die Sicherheit" bei diesen Verfahren ausmacht.

Der Beitrag der Signierung zur eMail-Sicherheit

Die Signierung garantiert die Wahrung der Authentizität und der Integrität einer eMail, da die verschlüsselte Prüfsumme "quasi unfälschbar" ist. Ohne Besitz des privaten Keys des Absenders ist es für einen Angreifer nahezu unmöglich, die verschlüsselte Prüfsumme nachzubilden. Dass dieses Verfahren verlässlich und einwandfrei funktioniert, kommt insbesondere dadurch zum Ausdruck, dass die digitale Signatur durch die Verabschiedung und Umsetzung des Signaturgesetzes in Deutschland inzwischen rechtsverbindlichen Charakter besitzt. Im Gesetz wird insbesondere exakt dargelegt, welche Einzelheiten wie zu beachten sind, um den gesetzlichen Anforderungen Rechnung zu tragen.

Der Beitrag der Verschlüsselung zur eMail-Sicherheit

Die Verschlüsselungen sichern die "Privatheit" von eMails. Die Sicherheit kommt dabei durch die "quasi Irreversibilität" der Verschlüsselung zustande. Das bedeutet: Die Entschlüsselung ist ohne Kenntnis des privaten Schlüssels fast unmöglich bzw. nicht mit vertretbarem Aufwand realisierbar.

Soweit zu den Verfahrensschritten und der durch Verschlüsselung und Signierung zu erzielenden Sicherheit. Wie eingangs dieses Kapitels schon kurz angerissen, können Public Key-Verfahren auf unterschiedliche Arten und Weisen in Netzwerke integriert werden. Welche Möglichkeiten zum Einsatz kommen können, ist Bestandteil des folgenden Kapitels.



```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Version: PGP 8.0.2  
mQENBD6qxVkBcADV3l4Jdfwmu6SWqTEmNWjigl  
DAxtAsBzlMcGRWZ+rVdM4vkWDBbDOysFXaHnFx  
v8LD5RksKeLd6cjYlTjqeUGUkLiVnciLDNafOn  
F+AVYqZobjfORd8MfbtUDrGOjU9+oJW88QUQrm  
bEIKzAtRzaxzd+zumXPibYc7GaKMWQdyCiI/sD  
F/aKA2B8cibPpuq+F7aLyyBab1k8M8U3fYmIq+  
7LJkx/+N5VMeBTeSc+B229fKE01WU5y3cK8emE
```

"Wenn alle PCs weltweit - d. h. 260 Millionen Computer - an einer einzigen von PGP verschlüsselten Nachricht arbeiten würden, würde es im Schnitt immer noch ungefähr 12 Millionen mal das Alter des Universums dauern, bis eine einzige Nachricht decodiert werden könnte."

William Crowell, stellvertretender Direktor des Nationalen Sicherheitsdienstes der USA (NSA), 1997

```
PibYc7GaKMWQdyCiI/sDU0S7qwx5CNvfRypTkn  
LpvsE399701h32Y5GDds5QwahOc8YECL6RsLp6  
gildUUO/oAwO2Vr9YhTT9P3EzYPc3auRxn/fJS  
DVlkwWnQyBkm2OnDop2VJ6cRrDMNS/ifw9ZT1+  
zKdfjSOrHdbVEJu8U1mIJUP68Kur6rRt07ABEB  
AAG0IkRpcmsgS3VlcHBlciA8ZGlyay5rdWVwcG  
VyQG1zaC5kZT6JAS4EEAECABgFAj6qxVkICwED  
QgHAgocGQEFgwMAAAAACgkQXyTp4csB5Mz3ywf  
+MNuj7l+QdPyTJ4f6hgKhrGOjU9+oJW88QUQrm  
bEIKzAtRzaxzd+zumXPibY4DQje2Pf10bKfkNn  
-----END PGP PUBLIC KEY BLOCK-----
```

eMail-Sicherheit

Verschlüsselungen / Signierungen: Umsetzungskonzepte

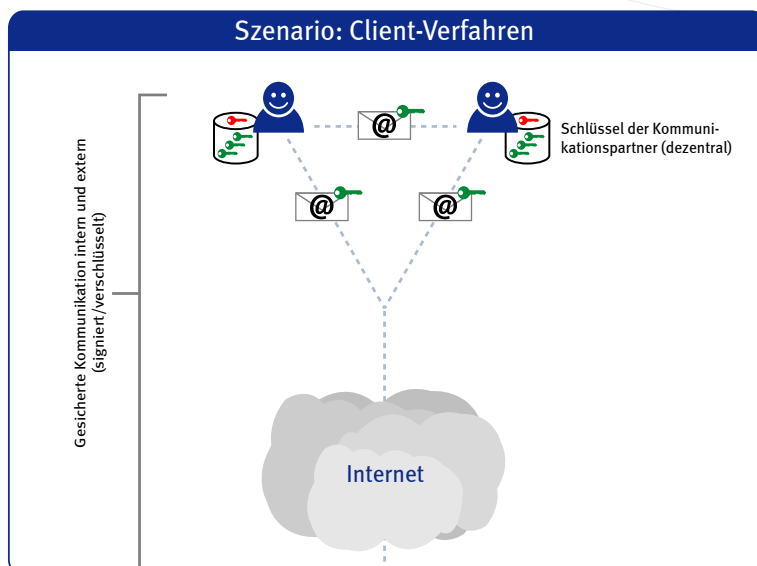
Hinsichtlich möglicher Umsetzungskonzepte (Topologien) unterscheidet man i.d.R. nach "Client-Verfahren" sowie nach "Gateway-Verfahren".

Das Client-Verfahren

Bei Client-Verfahren, auch dezentrale Lösung genannt, erfolgen eMail-Signierung und Verschlüsselung direkt am Arbeitsplatz (end-to-end). Und genau darin besteht der große Vorteil. Deshalb werden Client-Verfahren häufig dort eingesetzt, wo hochvertrauliche eMails auch intern zwischen Personen versendet werden. Anwender können (müssen) individuell entscheiden, welche eMails sie verschlüsseln bzw. signieren wollen.

Nachteilig wirkt sich jedoch der im Vergleich zum Gateway-Verfahren (siehe Seite 10) höhere Aufwand aus, der sich durch die dezentrale Installation (Roll-Out), Konfiguration und Wartung auf jedem einzelnen Arbeitsplatzrechner ergibt. Und um sicher zu stellen, dass die Lösung auch korrekt bedient wird, lassen sich Anwender-Schulungen zudem wohl nicht vermeiden. Ein weiteres nicht zu unterschätzendes Problem besteht in der Akzeptanz der Lösung. Denn häufig klagen Anwender über die hohe Komplexität, der sie sich mit der Ver- und Entschlüsselung bzw. der Signierung und Signaturprüfung von eMails ausgesetzt fühlen.

In der Praxis sind Client-Verfahren zunehmend häufiger auch in Kombination mit Public Key Infrastructures (PKI) vorzufinden, wobei PKI's als eine Art technische und organisatorische Plattformen die Verwaltung und die Distribution der kryptographischen Schlüssel und Zertifikate übernehmen. Da PKI's auch in vielen anderen Unternehmensbereichen sinnvolle Dienste übernehmen können, beschränkt sich ihr Einsatz selten ausschließlich auf das Schlüssel-Management im Bereich der eMail-Sicherheit.



Das Gateway-Verfahren

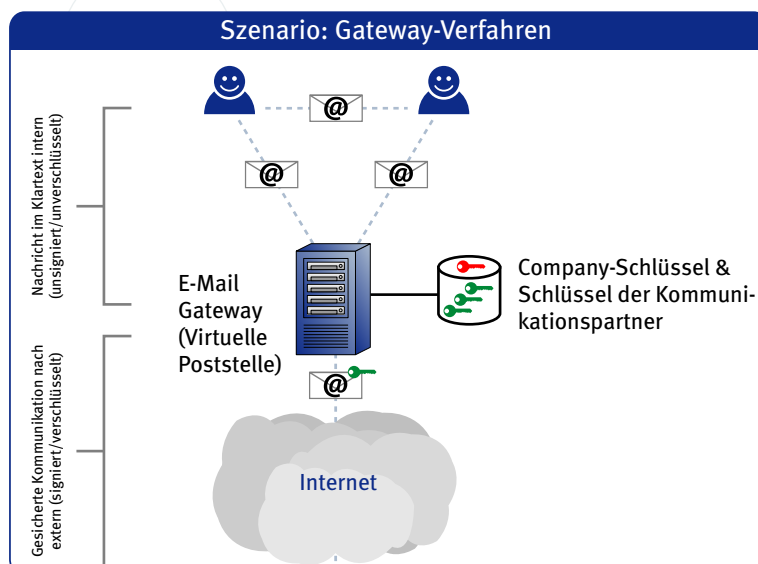
Bei Gateway-Verfahren, auch virtuelle Poststelle genannt, wird die Verschlüsselung/Entschlüsselung und Signierung/Signaturprüfung von eMails automatisiert am Gateway vorgenommen - also nicht auf Arbeitsplatzrechnern. Damit stellen die Verfahren eine verschlüsselte Datenübertragungen von einem Gateway zu a) einem Client oder zu b) einem anderen Gateway sicher - je nach dem, welche Lösung empfängerseitig integriert ist. Anwender können ihre elektronische Post wie gewohnt erhalten und absenden, ohne dass sie dazu irgendwelche zusätzlichen Tätigkeiten ausüben müssen.

Gateway-Verfahren "verwalten" Keys - insbesondere die Public Keys aller externen Kommunikationspartner - in einer internen Key-Datenbank, wobei die Einpflege der Keys in die Datenbank i.d.R. automatisiert erfolgt.

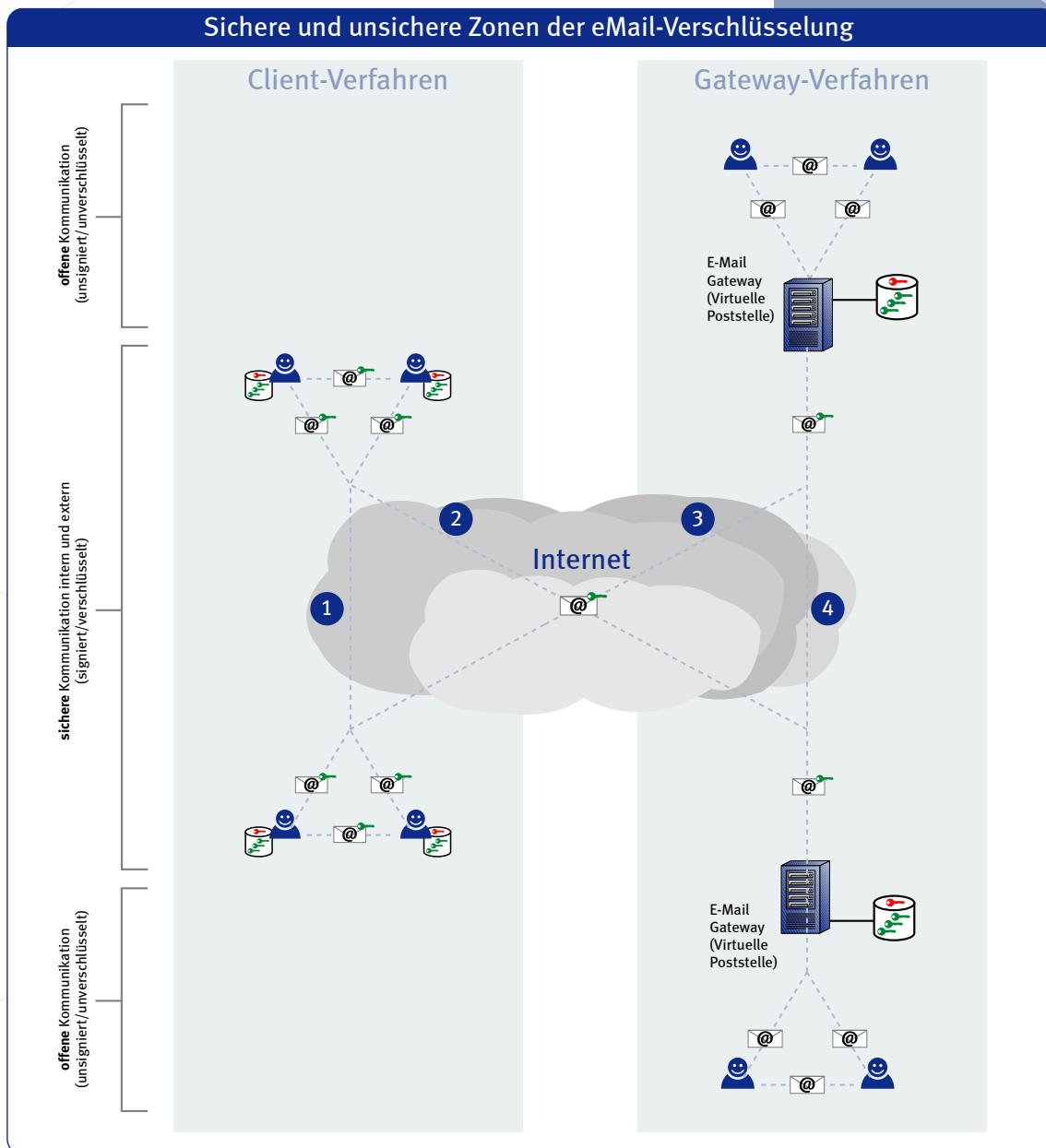
Da Entschlüsselungen eingehender eMails bereits am Gateway vorgenommen werden, kann bereits dort eine Kontrolle der eMails auf schadhafte Inhalte (z.B. Viren, Würmer, Trojaner etc.) erfolgen und nicht "erst" wie bei dezentralen Verfahren frühestens auf den Clients. Einige Gateway-Verfahren bieten zudem weitere nützliche Zusatzfunktionalitäten, wie z.B. Contentprüfungen, Weiterleitungen mit Vertretungsregelung, virtuelle Posteingangsbücher, Zeitstempel- u. Quittungsmechanismen, etc.

Die wichtigsten Eigenschaften zentraler Verfahren sind:

- Kein Roll-Out, keine Anwender-Schulungen und hohe Transparenz
- Entlastung der Mitarbeiter von komplexen Sicherheitsthemen
- automatisierte Ver-/Entschlüsselung bzw. Signierung/Signaturprüfung
- Content-Prüfung z.B. auf Malicious Codes schon am Gateway möglich
- Kostenvorteil durch Zentralisierung und zentrale Administration



eMail-Sicherheit








Im Schaubild werden 4 verschiedene Kombinationsmöglichkeiten einer verschlüsselten/signierten eMailkorrespondenz dargestellt.

- 1 Client-zu-Client-Verschlüsselung
- 2 Client-zu-Gateway-Verschlüsselung
- 3 Gateway-zu-Client-Verschlüsselung
- 4 Gateway-zu-Gateway-Verschlüsselung

Werkzeuge und Tools

Inzwischen ist eine Vielzahl verschiedener eMail-Verschlüsselungs-Tools am Markt erhältlich. Aber nur wenige nutzen Verschlüsselungsalgorithmen, die ernsthaften Entschlüsselungsversuchen standhalten. Ebenso bieten nur wenige Tools Features, die einen rundum professionellen Einsatz ermöglichen. Diese "Schmalspur-Varianten" haben im gewerblichen Umfeld jedoch nichts zu suchen. Denn hier gilt "halbe Sicherheit ist keine Sicherheit" und "der Betrieb muss jederzeit handhabbar sein". Daher greift Networkers im Projekteinsatz ausschließlich auf praxisbewährte Standardtools marktführender Hersteller zurück.

Exemplarisch seien hier die CryptoEx-Lösungen des Herstellers GlückKanja, SecurE Mail Gateway und Werkzeuge aus der SafeGuard SignCrypt- und PKI-Linie des Herstellers Utimaco Safeware und die Produkte Julia von ICC sowie PGP Corporate Desktop vom gleichnamigen Hersteller genannt. Unter Verwendung z.B. dieser Produkte kann Networkers sämtliche konzeptionell unterschiedlichen Ansätze von eMail-verschlüsselungs- und -signierungsverfahren auf nahezu allen etablierten Betriebssystem-Plattformen und unter Berücksichtigung gewünschter Standards zuverlässig aufsetzen.

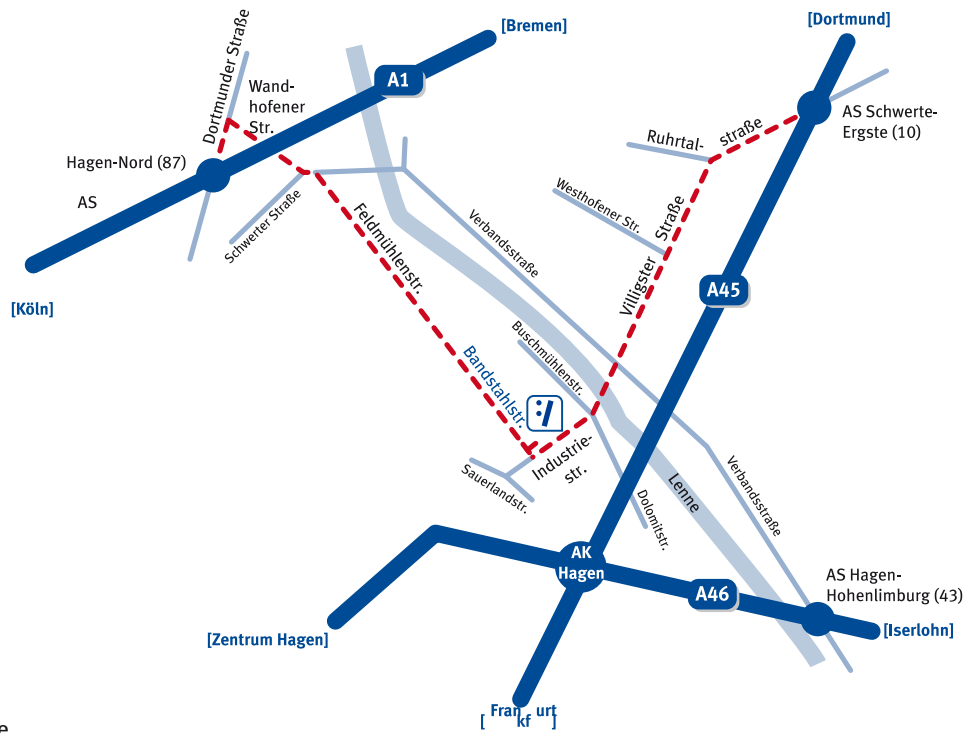
		Ort der Verschlüsselung	
		zentral	dezentral
Ort des Schlüsselmanagements	zentral	Virtuelle Poststelle: Glück Kanja <i>CryptoEx Business Gateway</i>  <i>SecurE Mail Gateway</i>  <i>Julia</i>	Client-Verfahren mit Public Key Infrastructure: Glück Kanja <i>CryptoEx Enterprise PKI Server / CryptoEx Business Server</i>  <i>SafeGuard PKI Enterprise / SafeGuard PKI Light</i>
	dezentral		Client-Verfahren ohne Public Key Infrastructure: Glück Kanja <i>CryptoEx Client</i>  <i>SafeGuard Sign&Crypt</i>  <i>PGP Corporate Desktop</i>

eMail-Verschlüsselungs-Services von Networkers

Als Full Service-Dienstleister insbesondere im Bereich der eMailsicherheit begleiten wir unsere Kunden über sämtliche Projektphasen - von der strategischen Beratung, der sachgerechten Konzeption und Planung über die kompetente Integration und Konfiguration als auch über die Durchführung von Schulungen und Workshops bis hin zur technisch versierten Betreuung in der Betriebsphase.

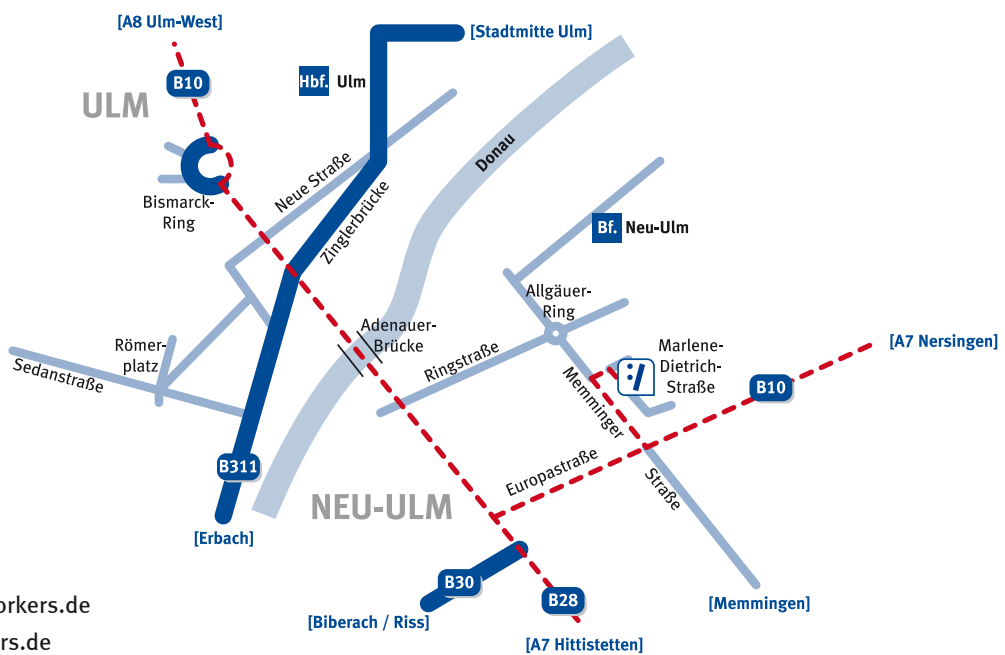
Ob dezentrales Verfahren, zentrales Verfahren, mit oder ohne PKI-Lösung: Wir beraten Sie umfassend und ausführlich und stellen Ihnen sämtliche in Frage kommende Verfahren mitsamt Ihren Besonderheiten detailliert vor. Dabei helfen wir Ihnen z.B. auch bei der Auswahl des für Sie sinnvollen Verschlüsselungsverfahrens (PGP, S/MIME), bei der eMail-Datenstromintegration, der Hersteller- und Betriebssystemauswahl, Entwicklung von Regelsätzen für Kommunikationsbeziehungen (zentrale Policy), etc.

Zentrale



Networkers AG
 Bandstahlstraße 2
 58093 Hagen
 fon: 02331 . 8095 0
 fax: 02331 . 8095 499
 email: info@networkers.de
 web: http://www.networkers.de

Niederlassung Neu-Ulm



Networkers AG
 Niederlassung Neu-Ulm
 Marlene-Dietrich-Straße 5
 89231 Neu-Ulm
 fon: 0731 . 98588 870
 fax: 0731 . 98588 874
 email: info@neu-ulm.networkers.de
 web: http://www.networkers.de



Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: www.networkers.de

Networkers AG Niederlassung Neu-Ulm
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

fon: 07 31 . 98 58 88 70
fax: 07 31 . 98 58 88 74

email: info@neu-ulm.networkers.de
web: www.networkers.de