

# Die virtuelle Poststelle → eine zentrale Security Plattform

**Prof. Dr. Norbert Pohlmann**

Institut für Internet-Sicherheit  
Fachhochschule Gelsenkirchen  
<http://www.internet-sicherheit.de>



if(is)  
internet-sicherheit.

- **Was ist eine virtuelle Poststelle?**
- **E-Mail Sicherheit**
- **Die Bedeutung der Sicherheitsfunktionen**
- **Zusammenfassung**

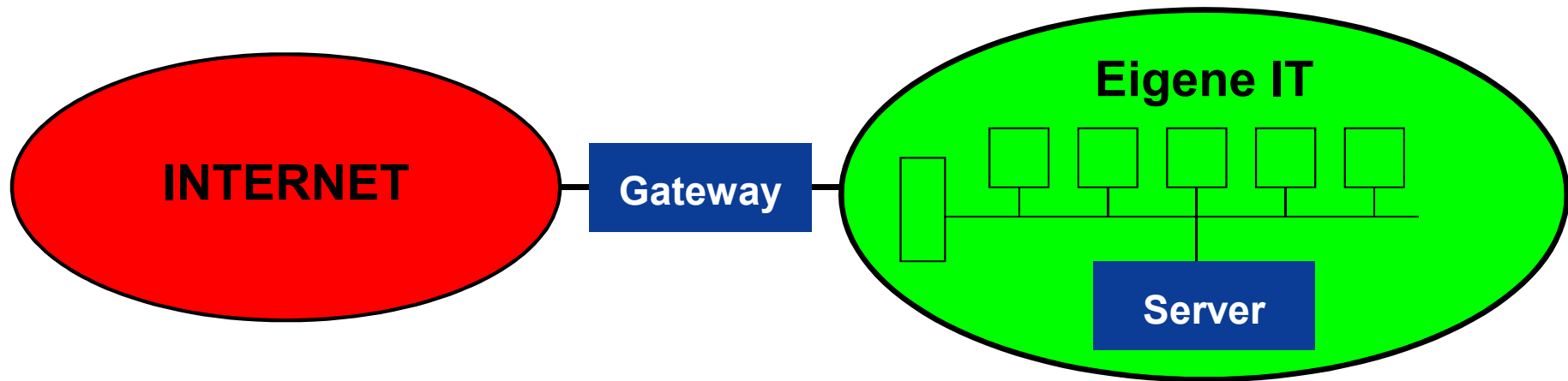
- **Was ist eine virtuelle Poststelle?**
- E-Mail Sicherheit
- Die Bedeutung der Sicherheitsfunktionen
- Zusammenfassung

# Was ist eine *virtuelle* Poststelle?

- **Zentrale Security Plattform**
  - **Sie stellt Sicherheitsdienste für eine gesicherte Kommunikation der vertrauenswürdigen elektronischen Prozesse zur Verfügung.**
- **Sicherheitsdienste der *virtuellen* Poststelle sind:**
  - **Vertraulichkeit** der übertragenen und gespeicherten Informationen
  - **Datenintegrität** der Mails, Dateien und sonstigen Informationen
  - **Authentikation** für die angebotenen Anwendungen (z.B. über Web)
  - **Verbindlichkeit** der ausgetauschten Informationen und Prozesse
  - **Protokollierung und Beweissicherung** der Aktionen, die über die *virtuelle* Poststelle durchgeführt wurden !

# Ausprägungen der *virtuellen* Poststelle

## → Zentrale Security Plattform



### Security-Gateway

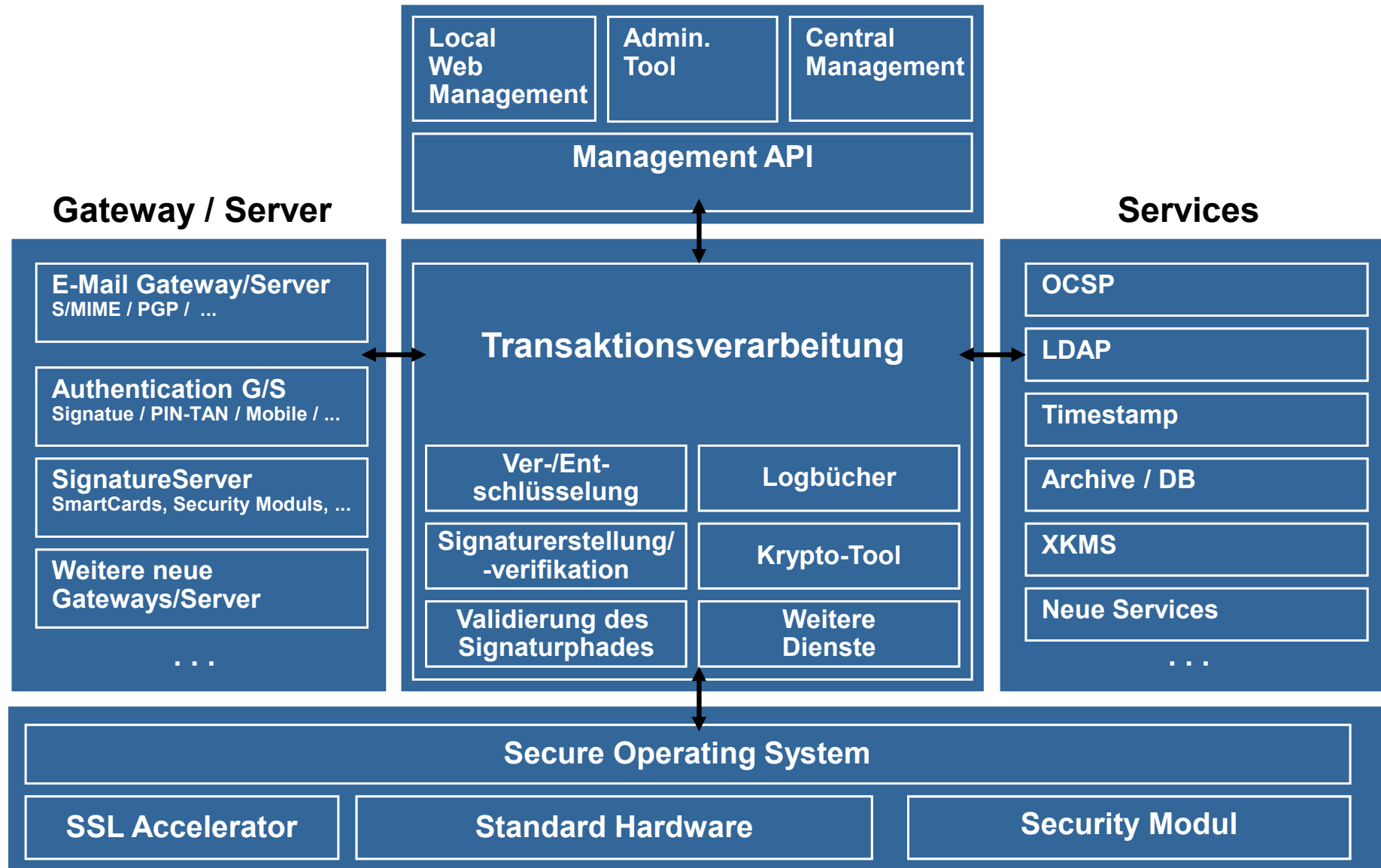
Einbindung von Sicherheitsfunktionen in die Kommunikation (SMTP-, oder HTTP-Proxy; wie eine Firewall)

### Security-Server

Sicherheitsdienstleistungen über definierte Schnittstellen  
z.B. Zeitstempel, Massensignaturen, ... aber auch E-Mail, Web, ...

### Gateway / Server

# Architektur der *virtuellen* Poststelle



# Warum eine zentrale Security Plattform?

## → Warum eine *virtuelle* Poststelle?

- **Pragmatischer Ansatz, weil ...**
  - die notwendigen Standards bei unterschiedlichen Herstellern nicht zustandekommen oder zu lange dauern
  - auch die virtuelle Welt nicht ideal ist
- **Eine zentrale Security Plattform, weil ...**
  - sie passgenau ist (Sicherheit umsetzbar machen)
  - sie als modulare Plattform für hohe Flexibilität sorgt
  - sie zukunftssicher ist (das Sicherheitssystem wächst mit den Anforderungen)
  - sehr gutes Kosten-/Nutzenverhältnis hat

- Was ist eine virtuelle Poststelle?
- **E-Mail Sicherheit**
- Die Bedeutung der Sicherheitsfunktionen
- Zusammenfassung



# E-Mail Sicherheit

## → Lösungen

— Pivacy, Integrity, Non-repudiation  
— No security

- End to End Security



- End to Site Security



- Site to Site Security



- No Security



# E-Mail Sicherheit

## → Lösungen

— Privacy, Integrity, Non-repudiation  
— No security

### ■ End to End Security

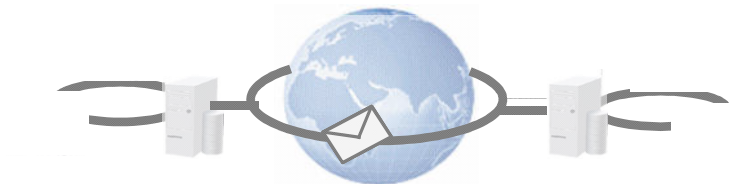
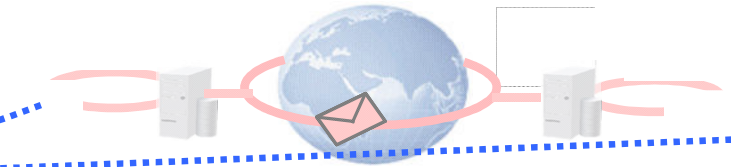
Client-Anwendung

### ■ End to Site Security

### ■ Site to Site Security

Virtuelle Poststelle

### ■ No Security



# E-Mail Sicherheit

## → Probleme bei End-to-End-Lösungen

- **Keine verbreitete Installationsbasis**
  - ↪ Kaum Einsatz von PKI (Zertifikat-Management)
  - ↪ Clients: Empfänger können nicht entschlüsseln/verifizieren
- **Hohe Kosten für Infrastruktur**
  - ↪ Alle SW-Clients mit E-Mail Security Applikation
  - ↪ Token (z.B. SmartCards), SmartCard-Reader
  - ↪ Rollout ist sehr aufwendig
  - ↪ Updates
  - ↪ Helpdesk ist notwendig
  - ↪ Schulung aller Mitarbeiter, Nutzung und Verwendung
  - ↪ Zertifikatsmanagement (PKI)
- **Alleinige Kontrolle bei Benutzer**
  - ↪ Verantwortung, wann verschlüsselt und signiert werden soll
  - ↪ Recovery Probleme (Mitarb. krank, verliert SmartCard (SC), SC defekt, ...)
  - ↪ Keine Vertreterregelung

## EU-Studie

- Laut EU-Studie lässt sich gut 2/3 der Kosten bei voller elektronischer Rechnungsverarbeitung einsparen.

Rechnungsart	Kosten
herkömmliche Rechnung	1,4 Euro
herkömmliche Rechnung + elektronische Rechnung (Medienbruch)	< 1,4 Euro
elektronische Rechnung	0,4 Euro

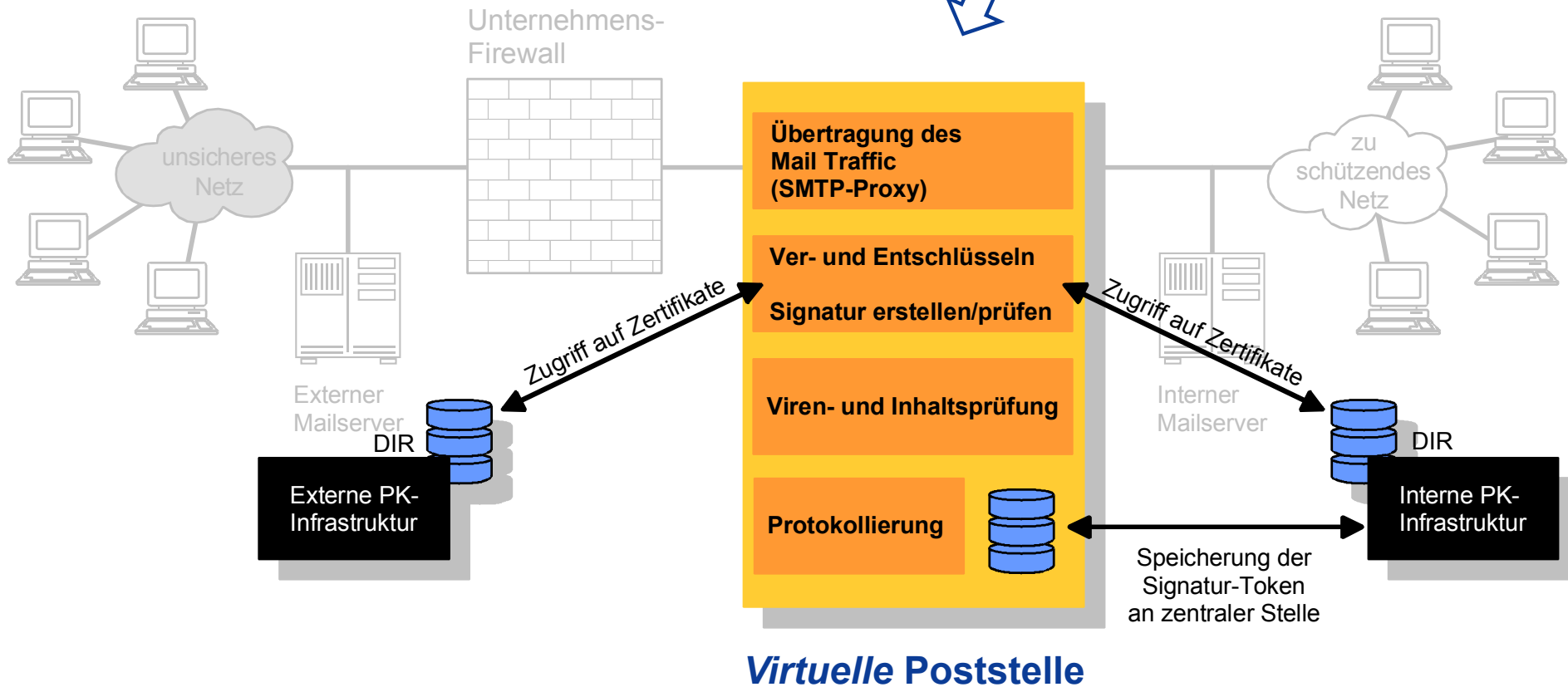


Quelle : Studie im Auftrag der EU Kommission

# Die virtuelle Poststelle (E-Mail Sicherheit)

## → Pragmatisches Technologie-Konzept

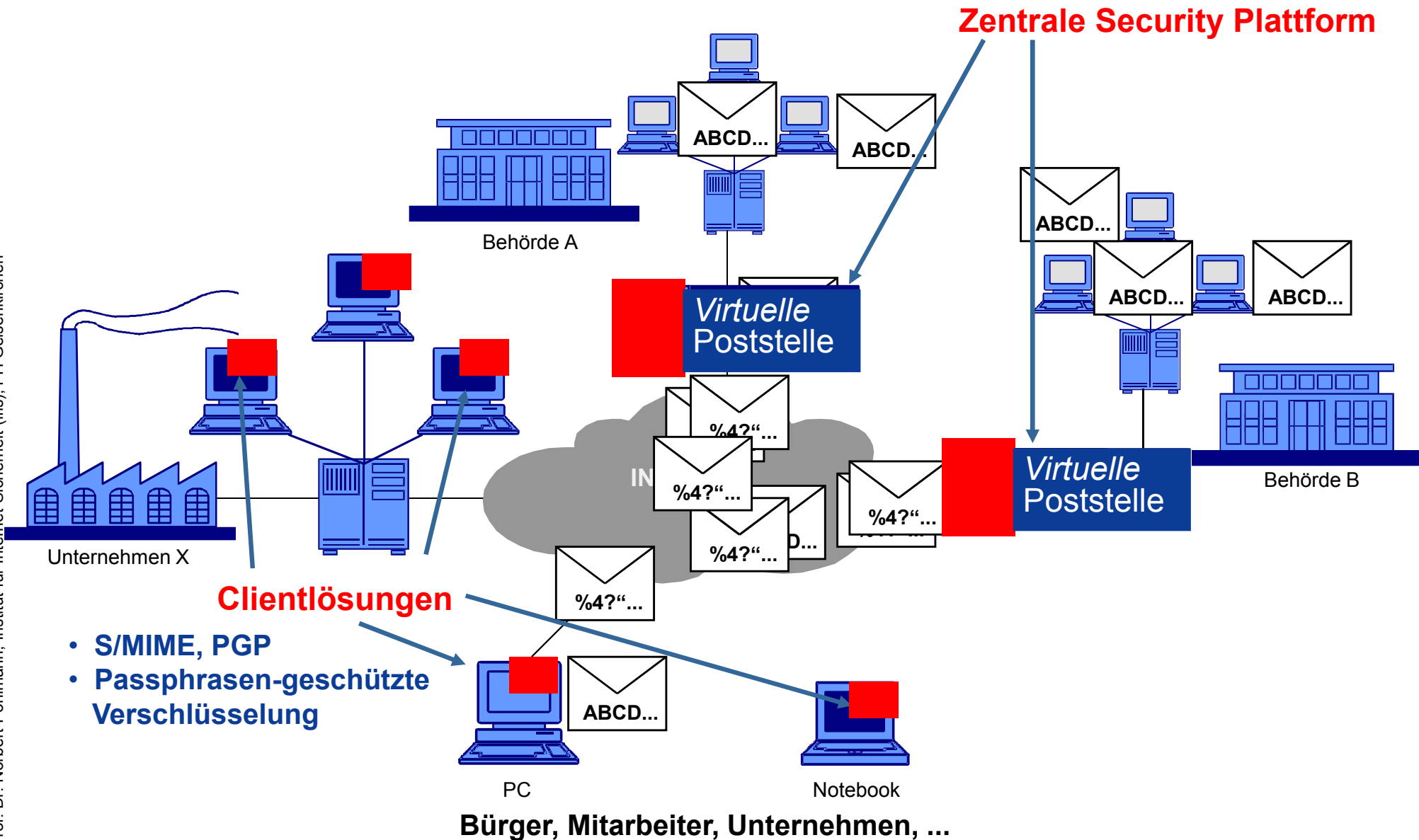
Einfache Integration in die vorhandene Einsatzumgebung



- Behörden und Unternehmen treffen auf die unterschiedlichsten Voraussetzungen in Bezug auf E-Mail Sicherheit bei ihren Kommunikationspartnern
  - Der Kommunikationspartner hat ebenfalls eine *Virtuelle Poststelle*  
→ **z.B. eine andere Behörde, Unternehmen, ...**
  - Der Kommunikationspartner nutzt eine Security Client-Lösung (S/MIME, PGP, ...)  
→ **z.B. Bürger, Mitarbeiter, Unternehmen, ...**
  - Der Kommunikationspartner hat lediglich Mail-Clients ohne integrierte Security (AOL, usw.)  
→ **z.B. Bürger, ...**

# E-Mail Sicherheit in der Praxis

→ Virtuelle Poststelle und E-Mail Clients



- S/MIME, PGP
- Passphrasen-geschützte Verschlüsselung

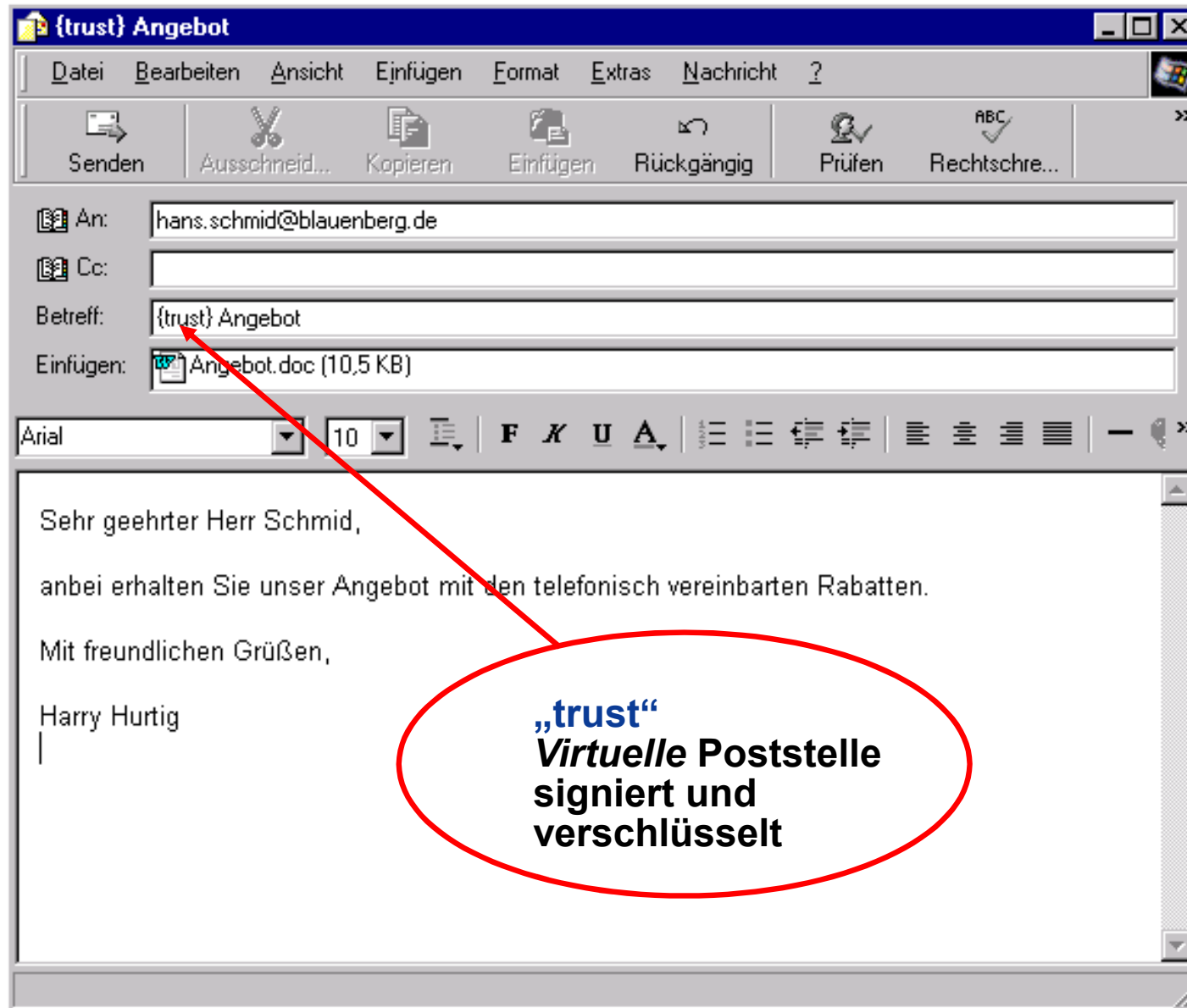
- **Unterschiedliche Methoden**
  - S/MIME (ISIS-MTT)
  - PGP
  - Passphrasen-geschützte Verschlüsselung
- **Ablauf beim Versenden von E-Mails**
  - „Regelbasiert“
    - **In der virtuellen Poststelle wird definiert**, bei welcher E-Mail-Adresse, die E-Mail durch die *virtuelle* Poststelle digital signiert und/oder verschlüsselt werden soll (z.B. „\*@fh-gelsenkirchen.de“).
  - „Benutzergesteuert“
    - **Der Benutzer steuert** z.B. über das Betreff-Feld, ob die E-Mail durch die *virtuelle* Poststelle digital signiert und/oder verschlüsselt werden soll.



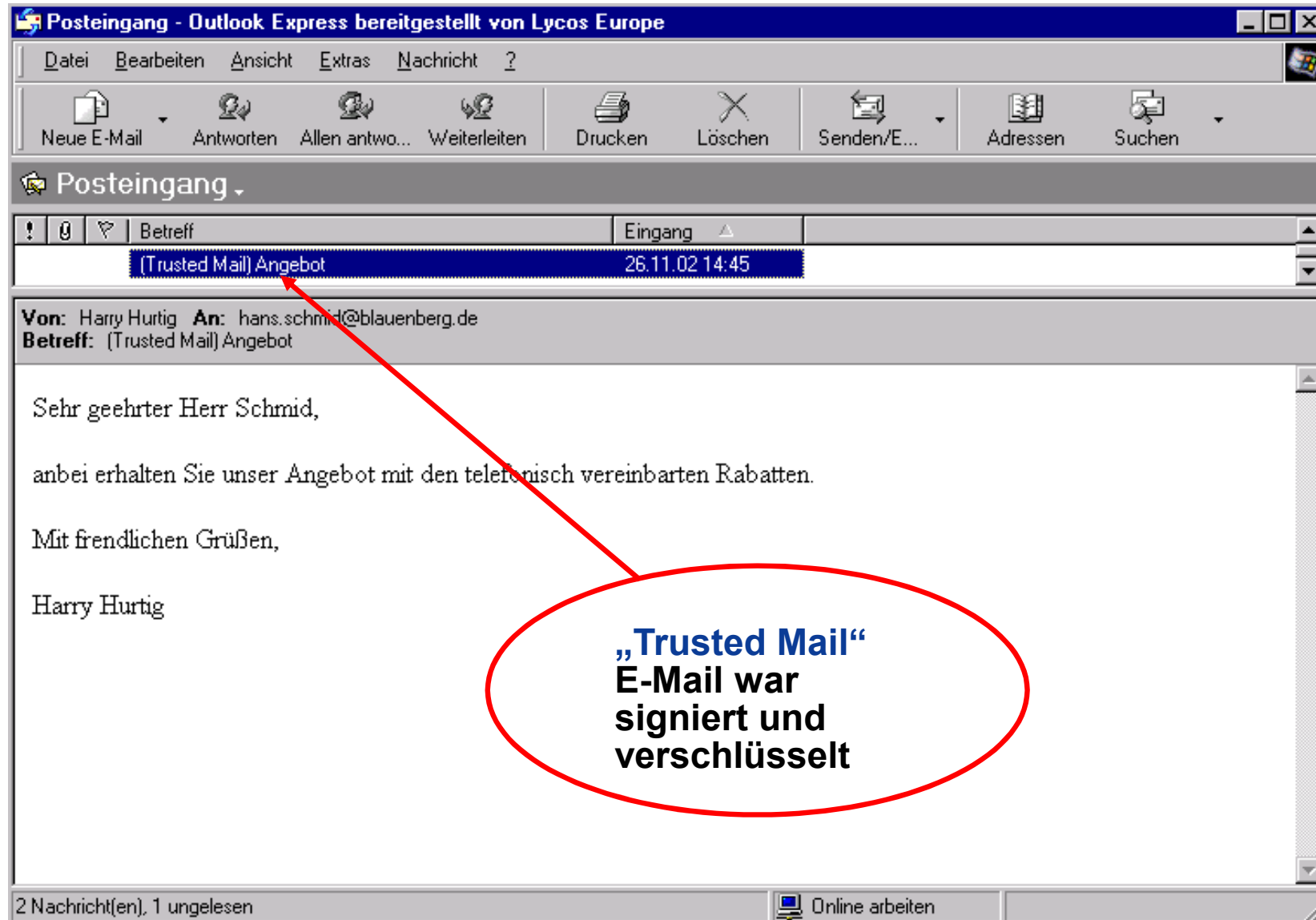
# Aktionen kontrolliert mittels E-Mail-Subject

- {sign}** Die Mail wird signiert.
- {crypt}** Die Mail wird verschlüsselt.
- {trust}** Die Mail wird signiert und verschlüsselt.
- {private}** Die Mail wird einem Passphrasen-geschützte System verschlüsselt.

# Senden einer E-Mail → Benutzergesteuert



# Empfangen einer vertrauenswürdigen E-Mail



# Empfangen einer Klartext E-Mail





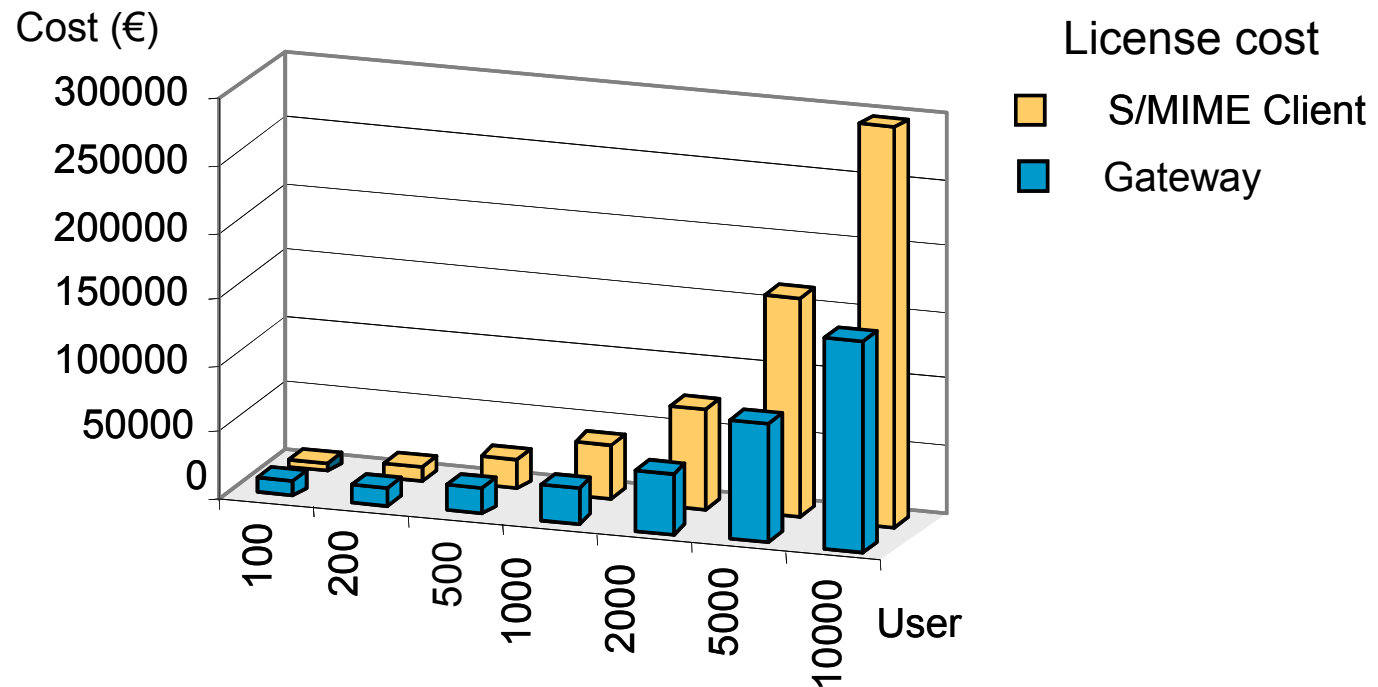
# Vorteile der *virtuellen* Poststelle

## → E-Mail Security

- Anwenderfreundlich
- Vertretungsregelung möglich
- „Maximale Sicherheit“ bei reduzierten Kosten
- Zentrale Viren- und Inhaltsprüfung
- Unterstützung mehrerer Standards und Methoden
- Sichere Basis: Firewall-Plattform
- PKI-"ready"
- Unternehmen/Organisationen sind in der Lage:
  - E-Mail-Sicherheit flexibel, schnell und **bedarfsgerecht** zu erzielen
  - E-Mail-Sicherheit **ohne ein hohes Investment in die benötigte Infrastruktur zu tätigen**

# Kostenvergleich E-Mail Security

Kosten	Zentral/Gateway 	Client 
Lizenzen	niedrig bis mittel	niedrig bis sehr hoch
Rollout	niedrig	mittel bis hoch
Helpdesk	niedrig bis mittel	mittel bis hoch
Migration	niedrig	mittel bis sehr hoch



- Was ist eine virtuelle Poststelle?
- E-Mail Sicherheit
- **Die Bedeutung der Sicherheitsfunktionen**
- Zusammenfassung

# Was bedeuten die Sicherheitsfunktionen für die E-Mail Sicherheit?

- **Verschlüsselung**
  - Die E-Mails können während der Übertragung im Internet **nicht im Klartext gelesen** werden
  - Es sind **keine gezielten Manipulationen** möglich
- **Elektronische Signatur**
  - Wie Behörden oder Firmenpapier bietet sie eine **höhere Vertrauenswürdigkeit**
  - Gewährleistung der **Datenunversehrtheit** und der **Verbindlichkeit**
  - Elektronische Signatur nach dem **Signaturgesetz**
  - Haftung nach Vereinbarung, z.B.
    - Kommunikationsvertrag mit Kunden, Lieferanten, Partnern
    - Betriebsvereinbarung
    - AGBs



# Anwendungsvergleich E-Mail Sicherheit

Anwendung	Zentral/Gateway	Client
Benutzerfreundlichkeit	+	-
Signatur und Verschlüsselung großer Mailvolumina	+	-
Elektronische Signatur	+	+
Qualifizierte Signatur	- (evtl. auch +)	+
Umsetzung der Organisationsspolicy	+	o (Vertrauen auf Anwender)
Vertreterregelung	+	-
Recovery	+	o (Nur wenn Anwender mit Organisationskey mitverschlüsselt)
Mails mit hoher interner Vertraulichkeit	-	+
Virenschanning, Inhaltsprüfung	+	-

**!Hybrid Lösung ist der Königsweg! (VP+Clients)**

- **Virtuelle Poststelle**
  - **Grundsätzliche Sicherheit** aller E-Mails
- **Client-Security in der eigenen Organisation**
  - **Höhere End-to-End-Vertraulichkeit** (z.B. Beihilfe) und
  - persönliche Digitale Signatur (qualifizierte Signatur)
  - **Weniger als 5%** der Personen müssen eine qualifizierte Signatur durchführen / brauchen End-to-End Vertraulichkeit
    - Sachbearbeiter für Fachanwendungen, z.B. Steuer
    - Vorstand/Geschäftsführer/Prokuristen/Einkäufer
    - ...

- Was ist eine virtuelle Poststelle?
- E-Mail Sicherheit
- Die Bedeutung der Sicherheitsfunktionen
- **Zusammenfassung**

# Zusammenfassung

## → Die *virtuelle* Poststelle

- Die *virtuelle* Poststelle ist ein **pragmatischer** Ansatz zur Absicherung der Kommunikationsdaten und Prozesse
- Vorteile dargestellt am Beispiel der E-Mail Sicherheit
- Die *virtuelle* Poststelle ist **flexibel**, da verschiedene Verfahren und Methoden parallel angeboten werden können.
- Die *virtuelle* Poststelle ist **zukunftsicher**, leicht erweiterbar für neue Prozesse, da sie einen modularen Aufbau hat und sich an der Infrastruktur orientiert.
- Die *virtuelle* Poststelle hat ein **sehr gutes Kosten-/Nutzenverhältnis.**
- Die *virtuelle* Poststelle hat sich **in der Praxis sehr gut bewährt.**

# Die virtuelle Poststelle → eine zentrale Security Plattform

Vielen Dank für Ihre Aufmerksamkeit  
Fragen ?

**Prof. Dr. Norbert Pohlmann**

Institut für Internet-Sicherheit  
Fachhochschule Gelsenkirchen  
<http://www.internet-sicherheit.de>



if(is)  
internet-sicherheit.