Deutscher Präventionstag –
der Jahreskongress seit 1995

Prävention durch Verschlüsselung – ökonomischer Wirtschaftsschutz

von

Hans-Joachim Giegerich

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Hans-Joachim Giegerich: Prävention durch Verschlüsselung – ökonomischer Wirtschaftsschutz, in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2015, www.praeventionstag.de/dokumentation.cms/3155

Giegerich & Partner

Prävention durch Verschlüsselung

- ökonomischer Wirtschaftsschutz

Präventionstag in Frankfurt am Main 08./09.06.2015

- Hajo Giegerich -

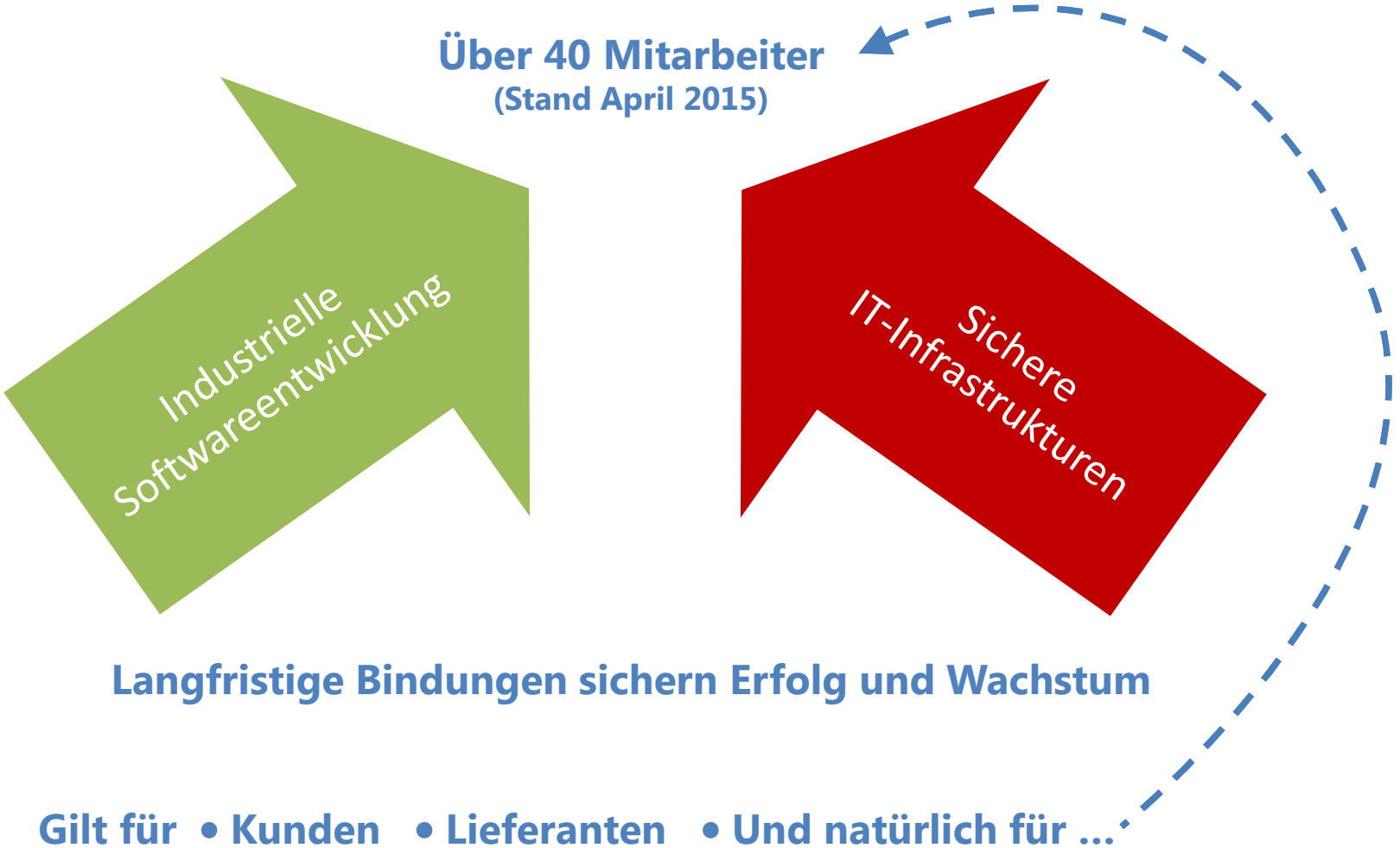
Agenda

1. Vorstellung
2. Warum sichere Datenkommunikation?
3. Analoge Welt – heile Welt?
4. Geheimnisse auf Postkarten?
5. Technologien für sicheren E-Mail-Verkehr
6. Fazit: Keine Einheitsgröße!

Wer spricht denn hier?

Unternehmen und Person

Das Unternehmen



Engagement für (IT-) Sicherheit

H.-J. Giegerich

- Netzwerk-, Internet- und IT-Sicherheit seit 1989
- Geschäftsführer Giegerich & Partner seit 1993
- Aufklärung/Awareness
- Consulting sichere Datenkommunikation
- Lösungen zur sicheren Datenkommunikation
- Stv. Vorsitzender d. ITK-Ausschusses beim DIHK und Leiter der Expertengruppe IT-Sicherheit
- Mitglied im Beirat d. Allianz für Cybersicherheit
- Zahlreiche Veröffentlichungen, z.B.
  - Co-Autor IT-Management Handbuch 2011
  - Co-Autor FAZ Security Kompendium 2011 u. 2012
  - Zeitschrift Controlling 2014
  - iX Sonderausgabe zu IT-Sicherheit 2015
  - U.v.m.

Engagement für Prävention (Auswahl)

H.-J. Giegerich

- Awareness-Veranstaltungen und Schulungen für Verantwortliche sowie Mitarbeiter in Unternehmen seit 2002
- Veranstaltungsreihe „Jugend sicher im Netz“ 2011 (10 Veranstaltungen an Schulen im Kreis Offenbach
- Vortragsreihe „Sichere Datenkommunikation 2012-2014“ an verschiedenen Anlässen
- Veranstaltungsreihe für Auszubildende in Stadt und Kreis Offenbach (Initiative der IHK Offenbach mit Unterstützung des PPSOH, 6 Veranstaltungen an berufl. Schulen) in 2014
- Bitkom Webinar „E-Mailverschlüsselung“ 2015
- Internet Medien Coach seit 2015

Warum Verschlüsselung?

GESTOHLENE E-MAIL-ADRESSEN

Dropbox bestätigt Datenklau

Dropbox sind die E-Mail-Adressen einiger Nutzer gestohlen worden, entsprechende Vermutungen bestätigte das Unternehmen jetzt. Betroffen ist aber nur eine kleine Zahl von Nutzern. Es gab keinen Einbruch in das eigentliche Dropbox-System.

Datenklau im großen Stil

Chinesische Hacker spähen High-Tech-Konzern aus

Dienstag, 14.02.2012, 11:51

ZUM THEMA

Telekommunikation
Apple und Microsoft kaufen Nortel-Patentschatz

Dank gestohlener Passwörter haben vermutlich aus China stammende Hacker jahrelang den inzwischen insolventen Nortel-Konzern ausspioniert. Sie hätten „Zugang zu allem gehabt“, offenbarte nun ein Manager.

Mitgliederdaten der CDU geklaut UPDATE

vorlesen / MP3-Download

Wie erst jetzt bekannt wurde, ist das Mitgliedernetz der CDU schon im August 2009 Opfer eines Angriffs geworden. Darüber informierte die Partei an diesem Freitag betroffene Mitglieder per E-Mail. Es habe sich herausgestellt, dass die Einbrecher beim Angriff Zugriff auf Mitgliederdaten hatten und diese dann am 12.08.2011 im Internet veröffentlichten. Dabei handele es sich um den Nachnamen, eine interne Kennnummer und die E-Mail Adresse.

02.08.2012 16:06

heise Security « Vorige | Nächste »

Kundendaten bei Online-Brillenladen Mister Spex geklaut UPDATE

vorlesen / MP3-Download

Unbekannte konnten bei einem Hackerangriff auf den Internetoptiker Mister Spex auf die Kundendatenbank zugreifen. Laut dem Berliner Unternehmen hatten die Angreifer dabei Zugriff auf Adressdaten und Passwörter und habe diese möglicherweise auch kopiert. Gehasht waren die Passwörter demnach nicht. Zahlungsinformationen seien nicht betroffen, da diese laut Mister Spex nicht gespeichert werden.

Erneuter Datenklau

Hacker knacken 93 000 Konten bei Sony

Mittwoch, 12.10.2011, 10:15

Erneut sind bei Sony Userkonten geknackt worden. Diesmal sind fast Hunderttausend Kunden betroffen. dpa

Erst im April hatten sich Hacker Zugriff auf Millionen Userkonten bei Sony verschafft. Nun ist der Elektronikriese erneut ins Visier von Cyberkriminellen geraten: Daten von fast Hunderttausend Kunden wurden gestohlen.

Die Angreifer hätten auf breiter Front versucht, in Nutzerkonten bei Sonys Online Diensten einzudringen, teilte der japanische Elektronikriese mit. In 93 000 Fällen sei es Eindringlingen gelungen, Kundennummern

Datenklau bei der Citibank gelang durch simple URL-Manipulation

citi

Laut einem Bericht der New York Times gelang der Diebstahl von rund 200.000 Kundendaten durch einen äußerst simplen Angriff.

Kundendaten bei der Citibank entwendet

citi

Bei dem Einbruch wurden laut der US-Bank die persönlichen Daten von etwa 200.000 Kreditkartenkunden entwendet. Der Vorfall wurde bei einer Routinekontrolle entdeckt.

Gute Gründe

- Wahrung von Geschäftsinteressen
- Verhinderung von unfreundlichem Informationsabfluß (Wirtschaftsspionage)
- Wettbewerbsvorteile ausbauen und halten
- Erfüllung gesetzlicher Vorschriften (z.B. Datenschutz)

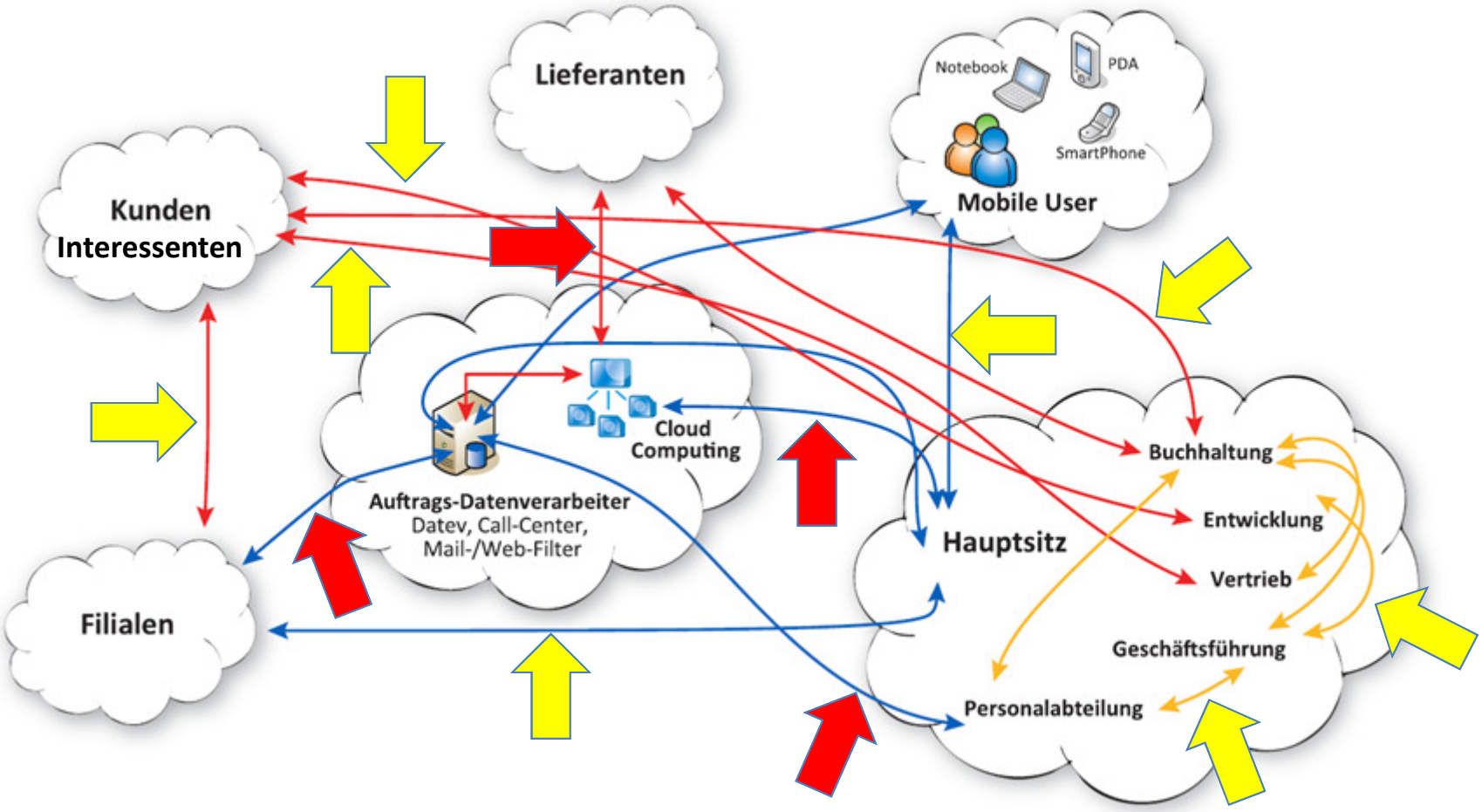
Was verschlüsseln?

Was darf / sollte verschlüsselt werden

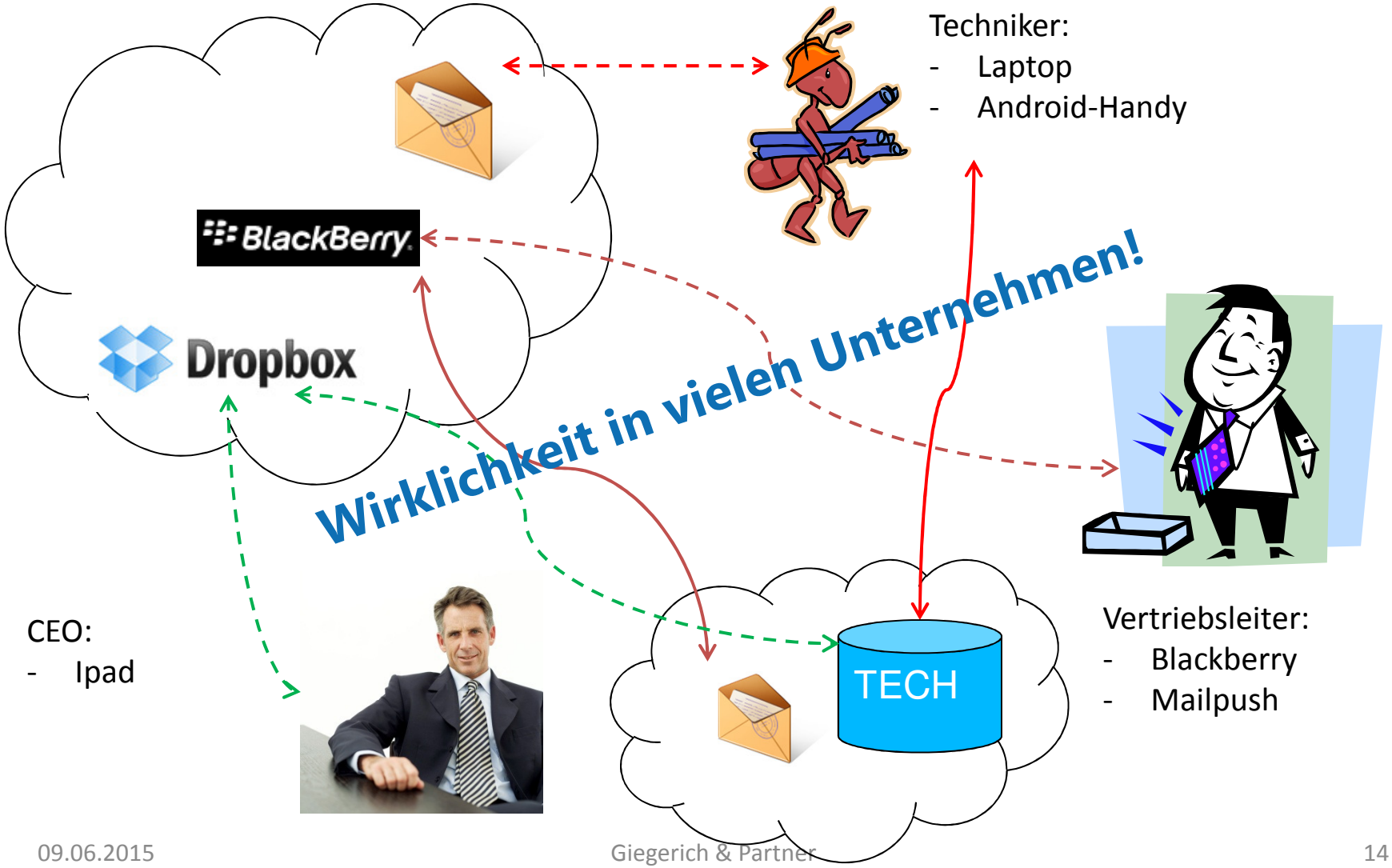
- Innovationen, Forschungs- und Entwicklungsergebnisse
- Personenbezogene Daten
  - Datenschutz
  - Arbeitnehmerdatenschutz
- Weitere Informationen, welche nicht für jedermanns Augen bestimmt sind
  - Mailarchive
  - Informationen für spezielle Interessengruppen (z.B. Geschäftsleitung)

Schwerpunkt Mailverschlüsslung?

Vielfalt der Kommunikationsbeziehungen

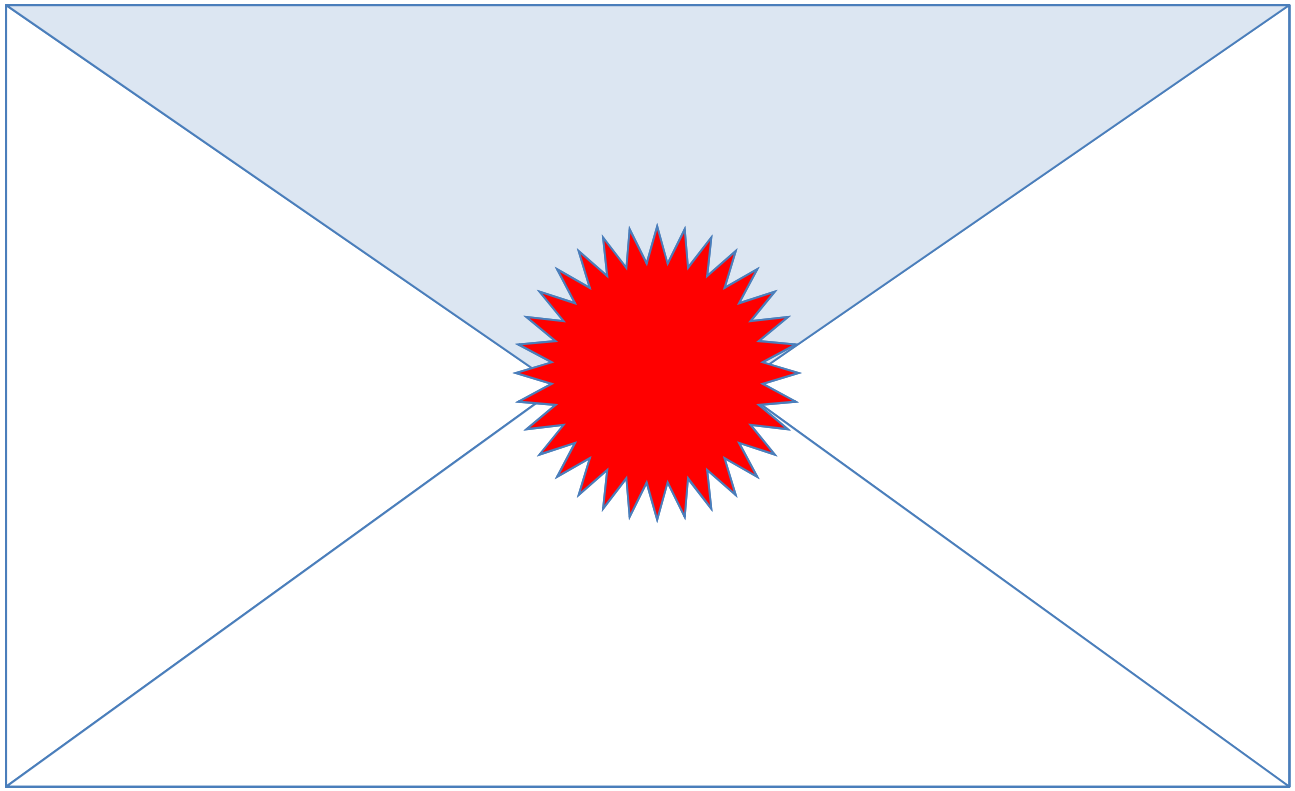


Vielfalt der Kommunikationsarten/Akteure



Analoge Welt – heile Welt?

Ein Ausflug zur „guten alten Post“



Kennzeichen des Briefes

- Geschlossen – Inhalt nicht unmittelbar einsehbar
- Durch das Briefgeheimnis geschützt
- Nachweis der Zustellung möglich

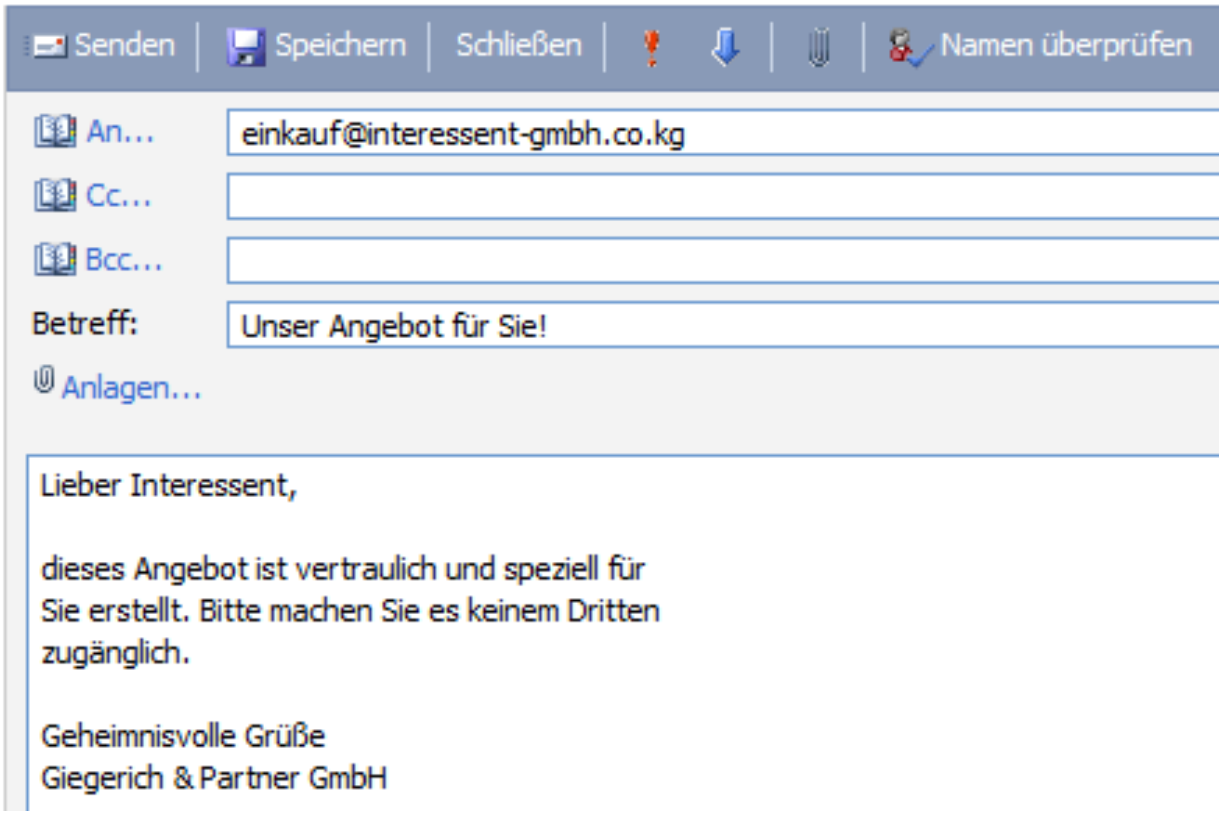
Aber: Inhalt im Klartext lesbar, wenn geöffnet

Geheimnisse auf Postkarten?

Wir tun es doch!

E-Mail – die digitale „Postkarte“

Ihr vertraut man vieles (vertrauliche) an…



Müssen wir alles im Klartext schreiben?

Geheimnisse verschlüsselt auf die Postkarte!

Giegerich & Partner GmbH
Robert-Bosch-Str. 18
63303 Dreieich

```
hQEMAwruW21QpvMwAQf/WZif/yrWout6ZHnUPuCn
L6RW+KMRNRLPBJDGR8g2TaQOuSXPG5hOmrNuyxhp
Ykj7kbwlSCHCW/AEbfTmAH9OyBHheU28UN4WCw/B
hXsTkoDYSBCar3itVxipDCCAROnRqbHv8uilbGxv
4I873fKXIAHD46vklKBdS26GWGw8cWMEk2yi2tNb
PgiS6qoblP7dZntKajY69x3tnSTPtykU2EpNVkwf
7T+G6c0HY2b0BfzRDj2nSTYErra5VIGMn97Y1bLp
adWDKxHM5LtYjitPnq97w1gpuJTVEerACaxe9c7h
RRRYWqzlUR90emQqNiEB9v00yeps+m9Kl6cm1yTr
TCfi9sI7iJ/N995ypzmizk0ZGRCQlZWo9OOj0oIX
CbhpBZqzuwmBIpb2EZr9mIzrknatllC+AKadyHkv
```

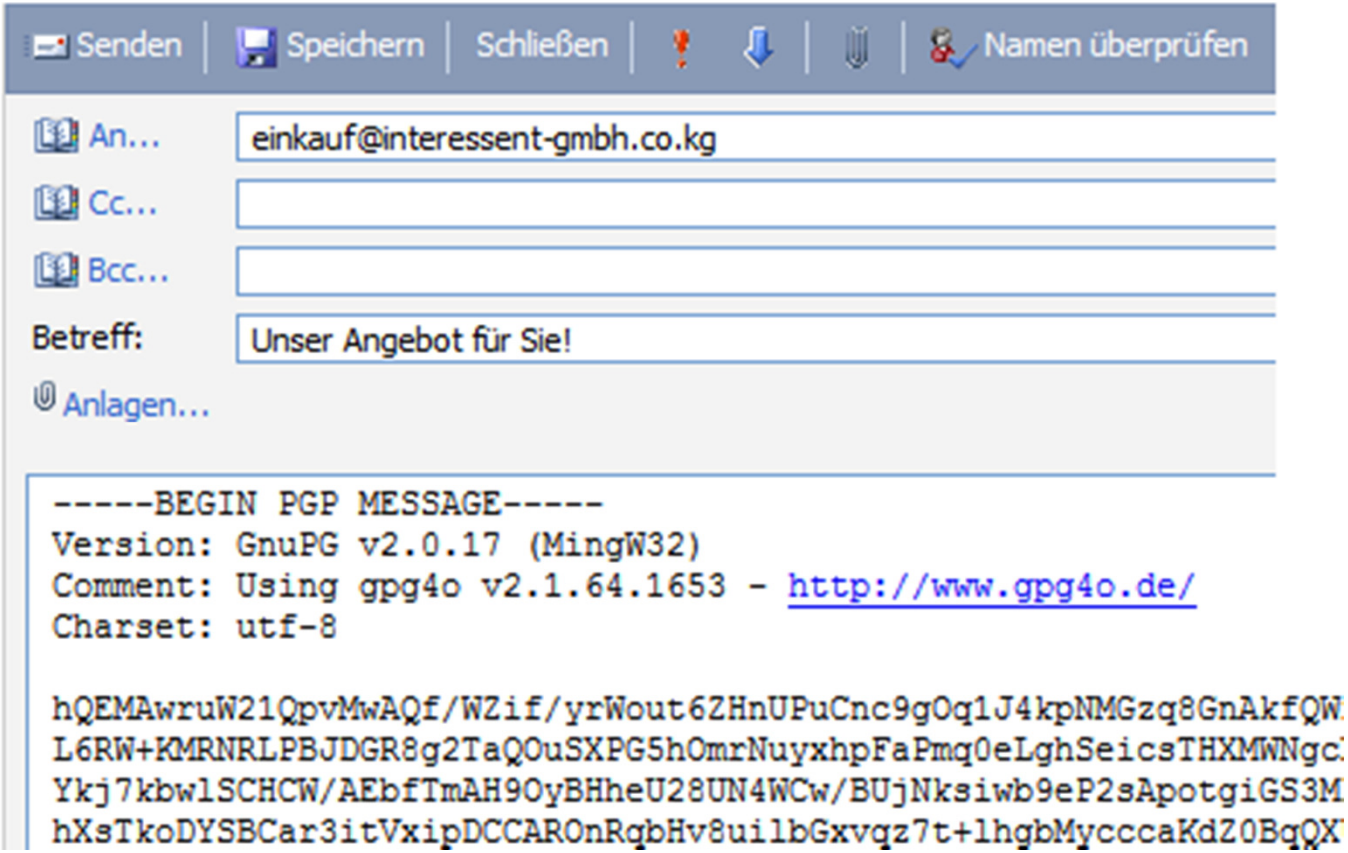
Arbeitskreis Forum
Hessen IT

Postkarte
- verschlüsselt -

Interessent GmbH & Co. KG
Strasse des Einkaufs 47
0815 Alleshabenwillingen

Müssen wir alles im Klartext schreiben?

Geheimnisse verschlüsselt auf die E-Mail!



Sinnvolle Anwendungsszenarien

Bei vertraulichem Inhalt

Verwenden Sie E-Mailverschlüsselung immer dann, wenn vertrauliche Informationen eine vertrauenswürdige Umgebung verlassen:

- **Nachrichten an Personen außerhalb des Unternehmens**
  z.B. Kunden, Lieferanten, Auftragsdatenverarbeiter
- **Nachrichten innerhalb des Unternehmens, sofern besondere Schutzwürdigkeit gegeben ist**
  z.B. Personaldaten, Forschungsergebnisse, Konzepte etc.
- **Nachrichten an Personen innerhalb des Unternehmens, wenn diese über nicht vertrauenswürdige Netze kommunizieren**
  z.B. im Ausland befindlich und VPN unterbunden

Technologien für sicheren E-Mail-Verkehr

Für unterschiedliche Anwendungszwecke

- **(Passwort)-Verschlüsselte Archive als Anhang zur E-Mail**
  z.B. RAR-Archive
- **OpenPGP basierte Nachrichtenverschlüsselung**
  für verschiedene Plattformen verfügbar
- **S/MIME basierte Nachrichtenverschlüsselung**
  für verschiedene Plattformen verfügbar
- **DE-Mail**
  vom Bund initiierte und lizenzierte Plattform zur sicheren Nachrichtenkommunikation
- **Andere**
  ePostbrief, E-Mail made in Germany

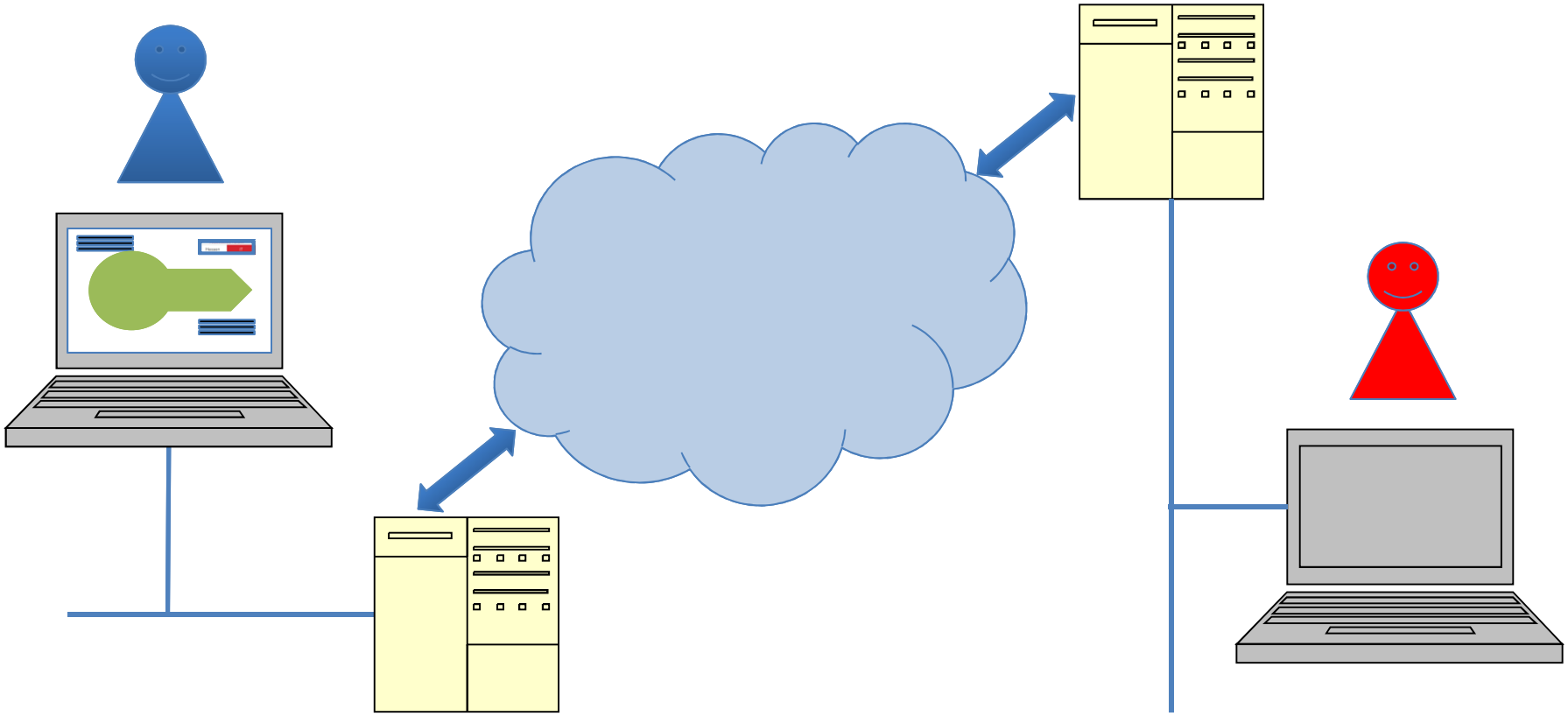
Technologien für sicheren E-Mail-Verkehr

Wer verschlüsselt hier – Client oder Server?

Clientbasierte Verschlüsselungsmethoden

- Gewährleisten eine durchgehende (Ende-zu-Ende) Verschlüsselung zwischen Sender und Empfänger
- Bieten maximale Vertraulichkeit
- Sind auf jedem Client separat einzurichten
- Fordern (in größeren Organisationen) erhöhten administrativen Aufwand
- Zur Erfüllung ges. Vorschriften (z.B. GdPdU) sind ggf. zusätzliche Maßnahmen erforderlich
  (z.B. ADK = additional decryption key)

Clientbasierte Verschlüsselungsmethoden

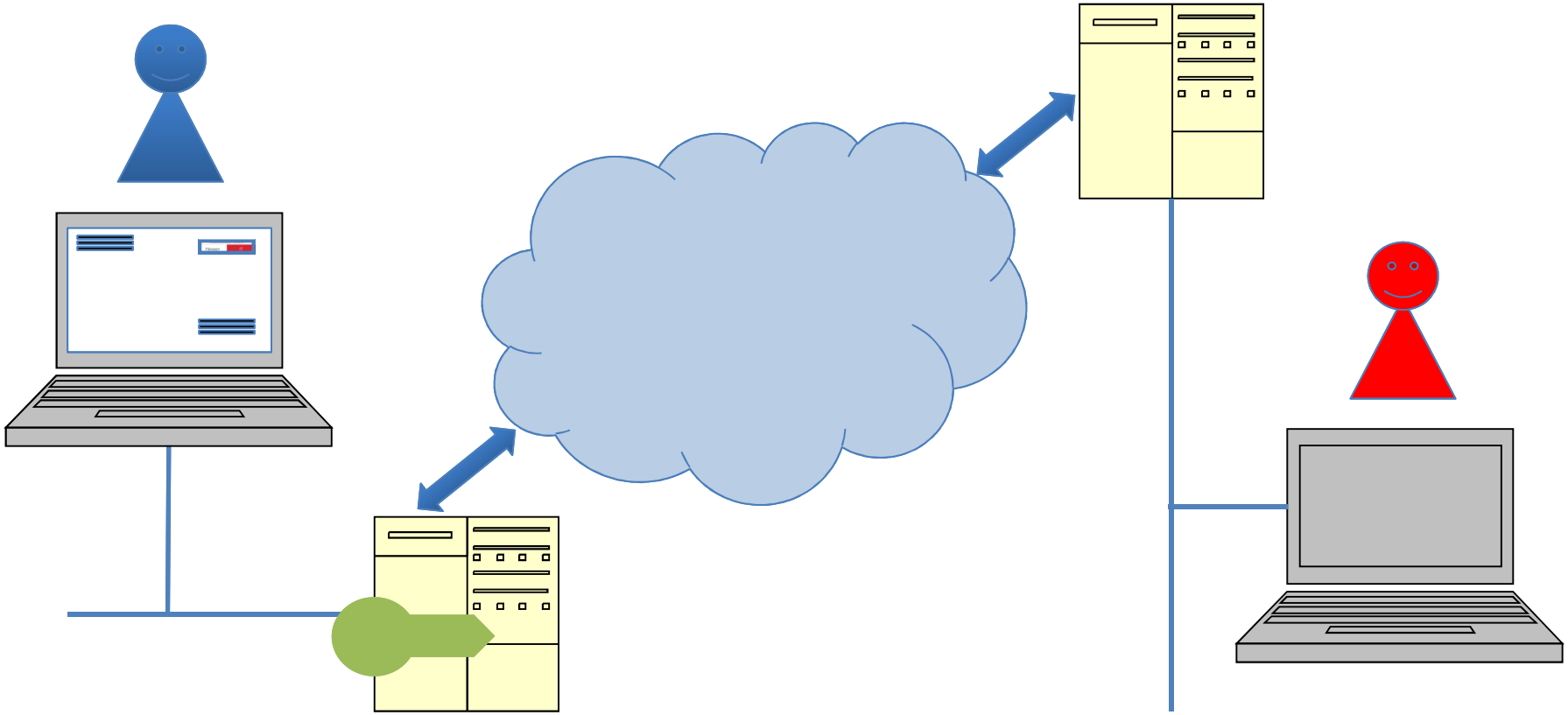


Serverbasierte Verschlüsselungsmethoden

- Verschlüsselung erfolgt auf Mailserver
- Bieten Vertraulichkeit zwischen den Mailservern
- Erfordern in der Regel keine Clientseitige Einrichtung
- Verlagern den administrativen Aufwand auf die Serverseite
- Zur Erfüllung ges. Vorschriften (z.B. GdPdU) sind ggf. zusätzliche Maßnahmen erforderlich
  (z.B. ADK = additional decryption key)

GEMISCHTE LÖSUNGEN MÖGLICH!

Serverbasierte Verschlüsselungsmethoden



Technologien für sicheren E-Mail-Verkehr - Anwendungszwecke

Passwortverschlüsselte Archive als Anhang

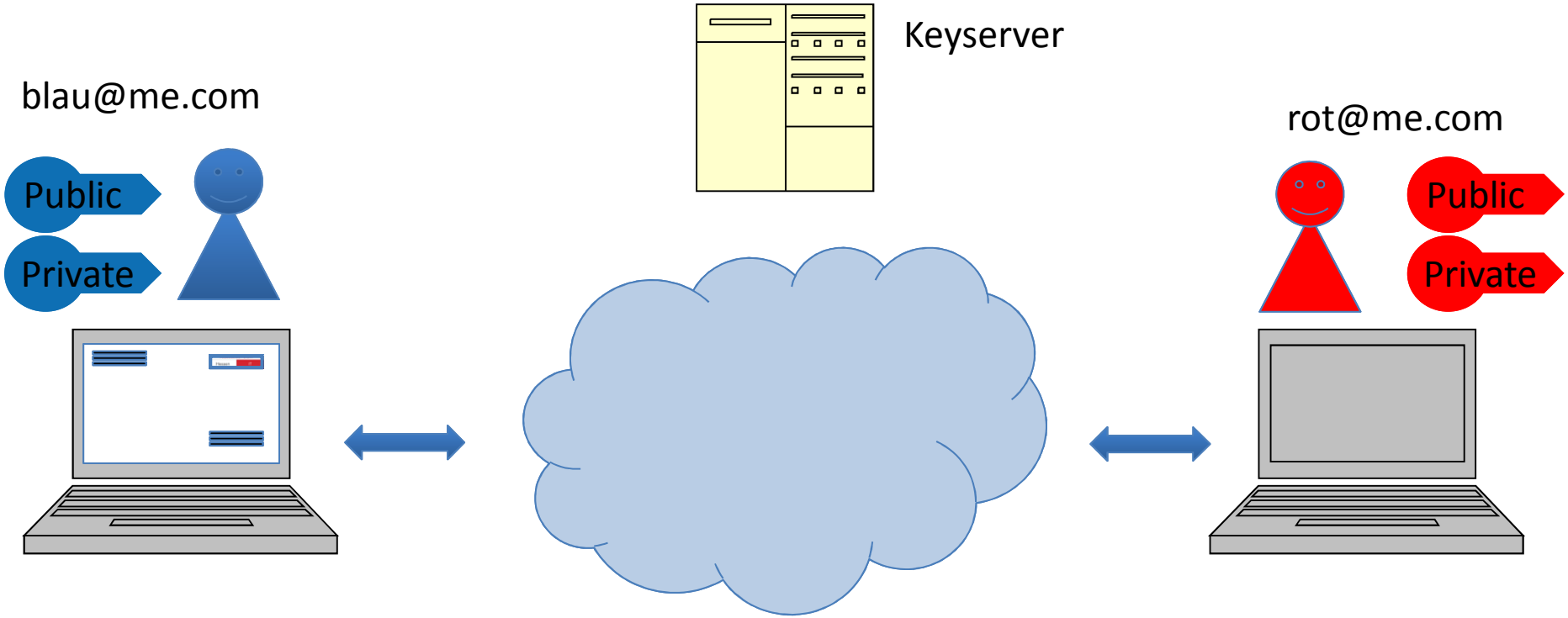
Passwort vorher bekannt oder über separaten Kanal

- Methode auch als PSK (Preshared Key) bekannt
- Funktioniert ohne zusätzliche Infrastruktur für Schlüssel
- Auf vielen Plattformen verfügbar
- Authentizität nur begrenzt prüfbar

Technologien für sicheren E-Mail-Verkehr – Anwendungszwecke

OpenPGP Verschlüsselung und Signatur

Mit oder ohne PKI (Public Key Infrastruktur)

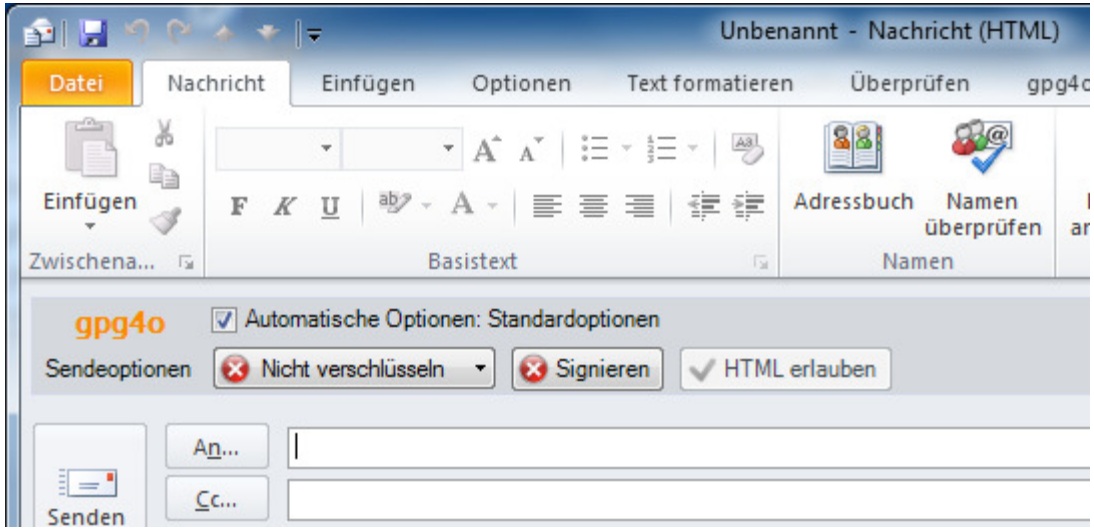


- Authentizität wird manuell und durch Plausibilität geprüft
- Funktioniert mit/ohne zusätzliche Infrastruktur für Schlüssel
- Auf vielen Plattformen verfügbar, weltweiter Standard
- Leichtere Handhabung durch PKI / Kein Medienbruch erforderlich

gpg4o für Outlook – starkes AddIn

Ausgereiftes Verschlüsselungs AddIn für Microsoft Outlook ab Version 2010

- Installation auch für weniger IT-affine Menschen ohne große Probleme möglich
- gpg4o unterstützt den Anwender durch geeignete Benutzerführung
  -> Stark in Usability
- Einfache Verteilung im Netzwerk. Funktionalität via Policy Editor einschränkbar
- Am Puls der Zeit – aktuelle Windows-Betriebssysteme und Outlook-Versionen werden komplett unterstützt.
- gpg4o ist kommunikativ – unterstützt alle am Markt gängigen OpenPGP Implementationen.
- gpg4o ist interoperabel – z.B. Durch Koexistenzfähigkeit mit S/MIME Implementationen
- gpg4o ist international durch Unterstützung von UTF-8



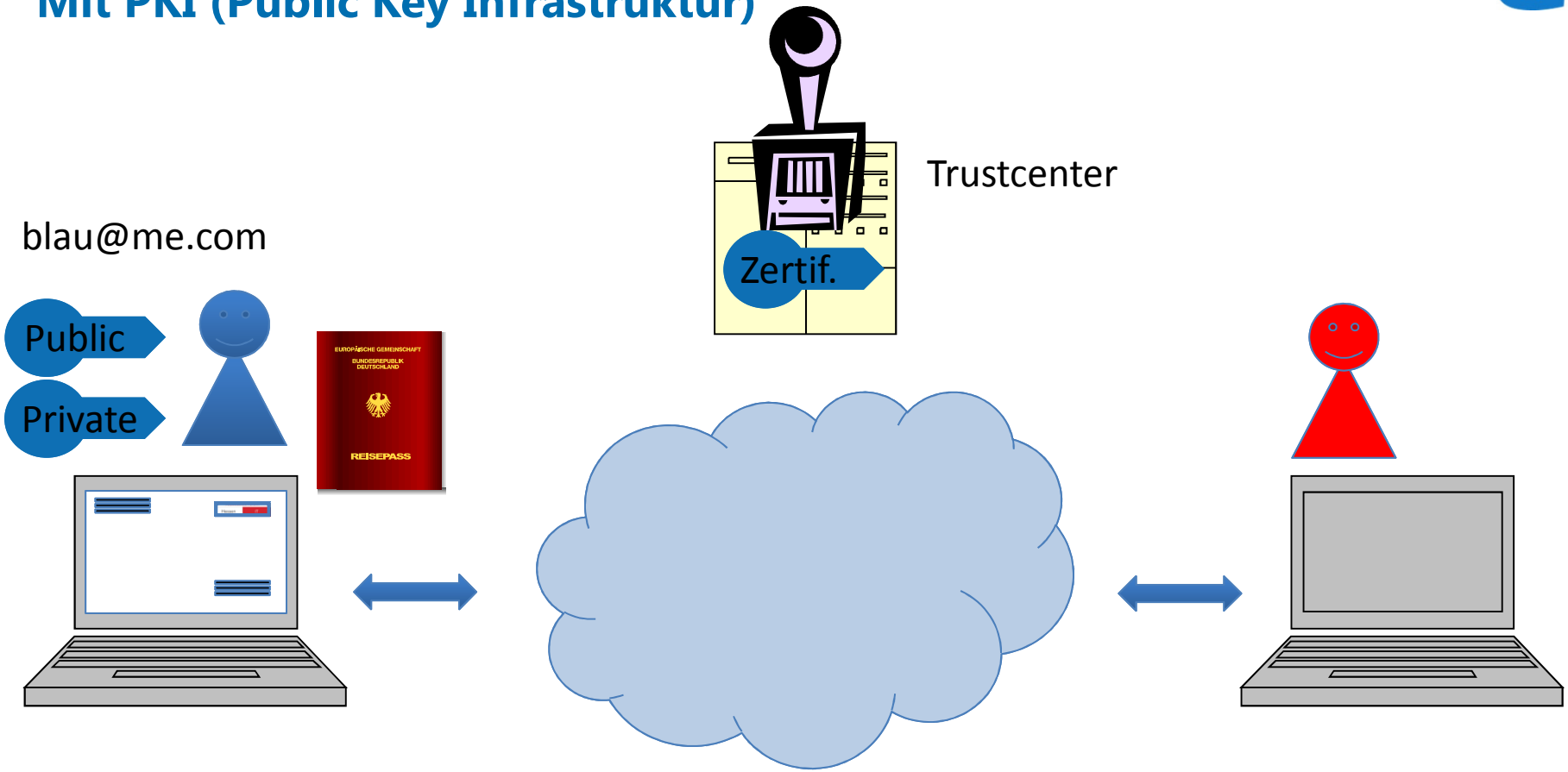
OpenPGP – weitere Fakten

- Weltweit hohe Verbreitung
- Hoher Sicherheitsstandard seit fast 25 Jahren
- Im Gegensatz zu S/MIME auch für Datei-Verschlüsselung gedacht und geeignet.
- Kritikpunkte:
  - Schlüsselmanagement erfordert Wissen und Befassung
  - Viele Implementationen nicht Bedienerfreundlich

Technologien für sicheren E-Mail-Verkehr - Anwendungszwecke

S/MIME Verschlüsselung und Signatur

Mit PKI (Public Key Infrastruktur)



- Authentizität anhand X.509-Zertifikaten prüfbar
- Infrastruktur für Schlüsselverwaltung erforderlich
- Auf vielen Plattformen verfügbar, weltweiter Standard
- Leichtere Handhabung, bessere Prüfbarkeit der Authentizität

Technologien für sicheren E-Mail-Verkehr - Anwendungszwecke

DE-Mail

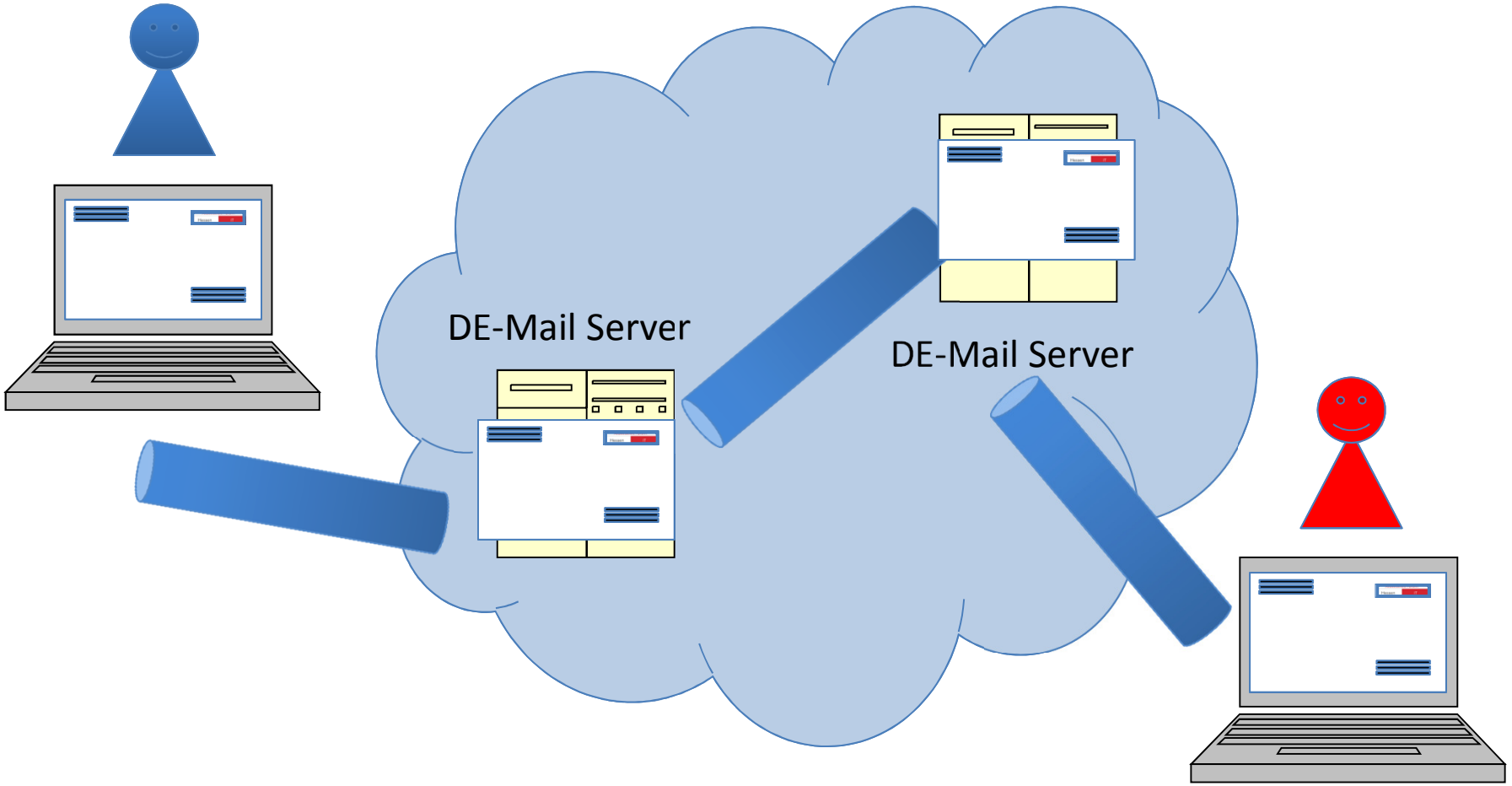
DE-Mail – ein anderer Ansatz

- Umsetzung einer EU-Richtlinie, nach der alle Behörden bis Ende 2009 elektronische Nachrichten akzeptieren sollen
- Basiert auf E-Mail – ist davon aber ein getrennter Dienst
- Ziel: Verbindlichkeit des elektronischen Geschäftsbriefes
- Erste Angebote gestartet (zur IFA 08/12; u.a. Deutsche Telekom)
- Verschlüsselung wird durch TLS (Transport Layer Security) gewährleistet

DE-Mail – weitere Fakten

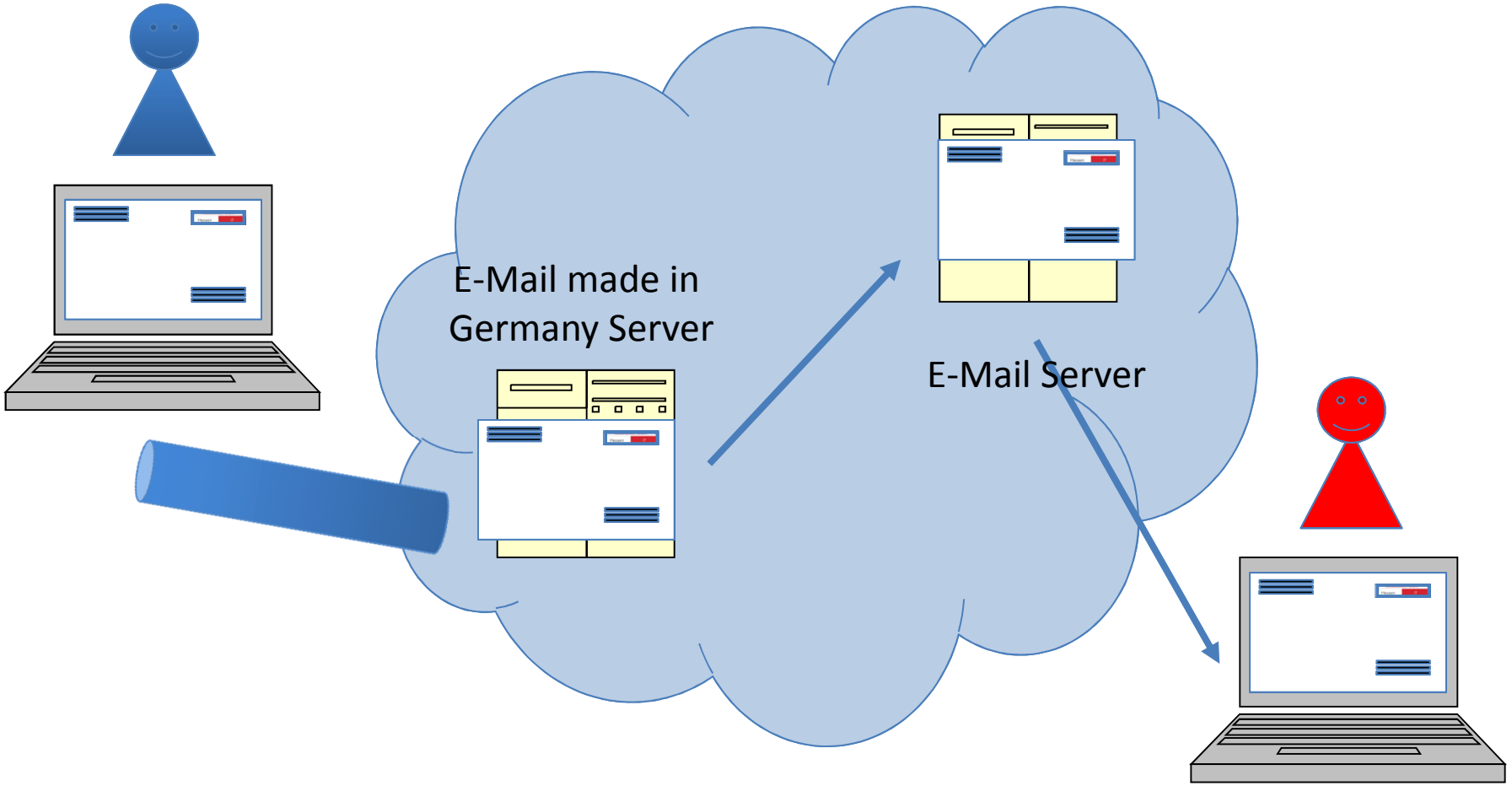
- Anlegen eines Benutzerkontos nur gegen Ausweisung
  - z.B. Personalausweis, Firmenunterlagen bei org. Konten
- Zusätzliche Funktionen möglich:
  - DE-Ident (Identitäts- und Altersnachweis)
  - DE-Safe (Sichere Datenablage)
- Kritikpunkte:
  - Rein deutsche Lösung
    (ausländische Kunden werden nicht akzeptiert)
  - Keine Ende-zu-Ende Verschlüsselung
  - Vertraulichkeit nicht vollinhaltlich garantiert
  - Kunden außerhalb des Dienstes nicht erreichbar

Technisches Prinzip: Keine Ende-zu-Ende Verschlüsselung!



So ähnlich: E-Mail made in Germany!

Hybride Lösung ermöglicht mailen in alle Netze



Auch Verschlüsselungstechnologie hat Grenzen

heise online > News > 2014 > KW 15 > Der GAU für Verschlüsselung im Web: Horror-Bug in Op

08.04.2014 09:20 heise Security « Vorige | Nächste »

Der GAU für Verschlüsselung im Web: Horror-Bug in OpenSSL UPDATE

vorlesen / MP3-Download

Ein äußerst schwerwiegender Programmierfehler gefährdet offenbar Verschlüsselung, Schlüssel und Daten der mit OpenSSL gesicherten Verbindungen im Internet. Angesichts der Verbreitung der OpenSource-Bibliothek eine ziemliche Katastrophe.

Die Entwickler von OpenSSL veröffentlichen ein Update ihrer weit verbreiteten Verschlüsselungsbibliothek, das äußerst schlechte Nachrichten transportiert: Ein Programmierfehler erlaubt es jedem Kommunikationspartner, Speicher der Gegenstelle auszulesen. Konkret bedeutet das: Ein Angreifer kann Schlüssel, Passwörter und andere geheime Daten klauen.

Fazit: Keine Einheitsgröße!

Keine Einheitsgröße!

Was passt für wen?

- Technologieauswahl stark vom Schutzbedarf und von der Aufwandsbereitschaft abhängig
- Behördenkommunikation soll künftig Nutzung von DE-Mail erfordern
- Weltweite Kommunikation über Industrie-Standards
- Kombination von Verfahren (z.B. DE-Mail mit OpenPGP und S/MIME möglich und verschiedentlich ratsam)


Vielen Dank für Ihre Aufmerksamkeit!

Impressum

Giegerich & Partner GmbH
Robert-Bosch-Str. 18
63303 Dreieich
Deutschland

Telefon: +49-(0)6103-5881-0

Telefax: +49-(0)6103-5881-39

Internet: www.giepa.de

Copyrights