Bullshit made in Germany

Linus Neumann

Bild: MathiasM

Agenda

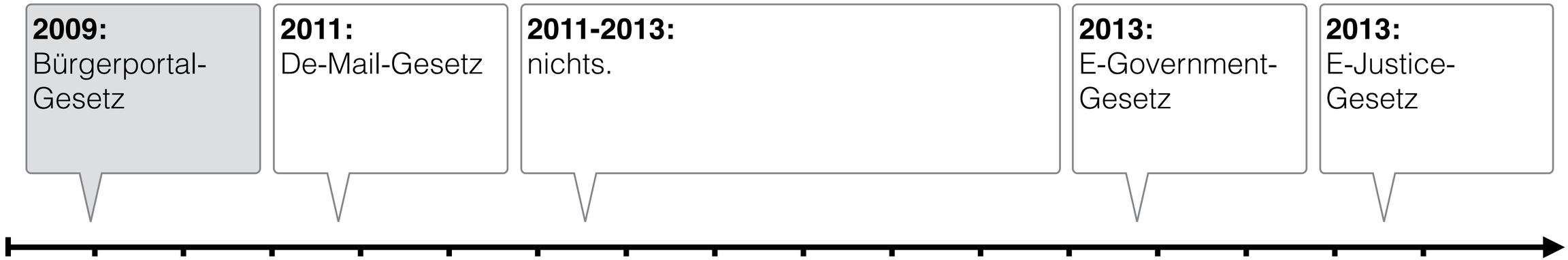
- **De-Mail**
- Email made in Germany
- Schlandnet
- Cloud

De-Mail Ziel:

- ➡ sicherer
- ➡ vertraulicher und
- ➡ nachweisbarer Geschäftsverkehr
- ➡ für jedermann
- ➡ im Internet

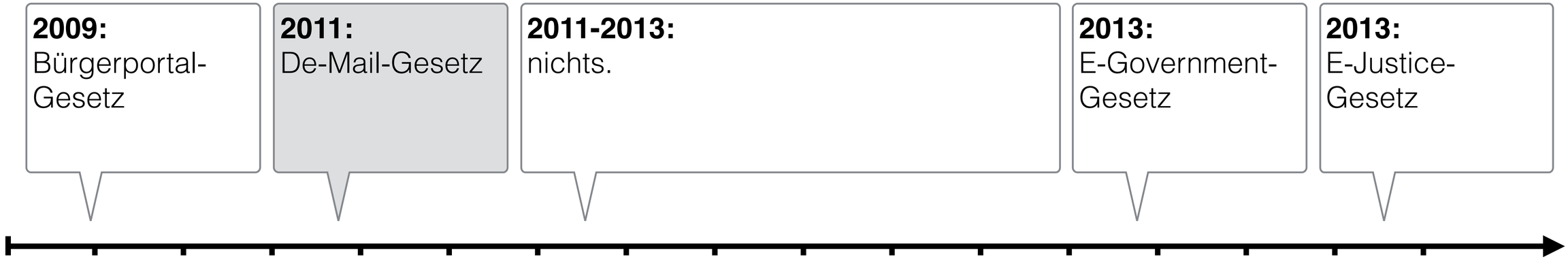
§1(1) De-Mail-Gesetz

Was bisher geschah:



„§5(1): (1) Der akkreditierte Diensteanbieter hat dem Nutzer ein sicheres elektronisches Postfach und einen sicheren Versanddienst für elektronische Nachrichten anzubieten.“

Was bisher geschah:



„§1(1): De-Mail-Dienste sind Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.“

Für jedes technische Problem gibt es eine juristische Lösung.

Problem:

- Jeder kann hasi69@yahoo.com reservieren.
- Empfänger kann Empfangsbestätigung verweigern

Lösung:

✓ Man muss seinen Ausweis zeigen.

✓ Nutzer wird zum Abholen verpflichtet, Empfangs-bestätigung kommt automatisch

Für jedes technische Problem gibt es eine juristische Lösung.

Problem:

- Kann man kein Geld mit verdienen
- Verteiltes System mit vielen konkurrierenden Anbietern

Lösung:

✓ Kostet 0,39€ pro Stück.

✓ Teure Zertifizierung

Für jedes technische Problem gibt es eine juristische Lösung.

Problem:

- Einige Anbieter bieten unverschlüsselte Verbindungen an
- Nicht jeder Nutzer unterstützt PGP oder S/Mime
- Email-Würmer (1990)

Lösung:

✓ SSL durchgängig

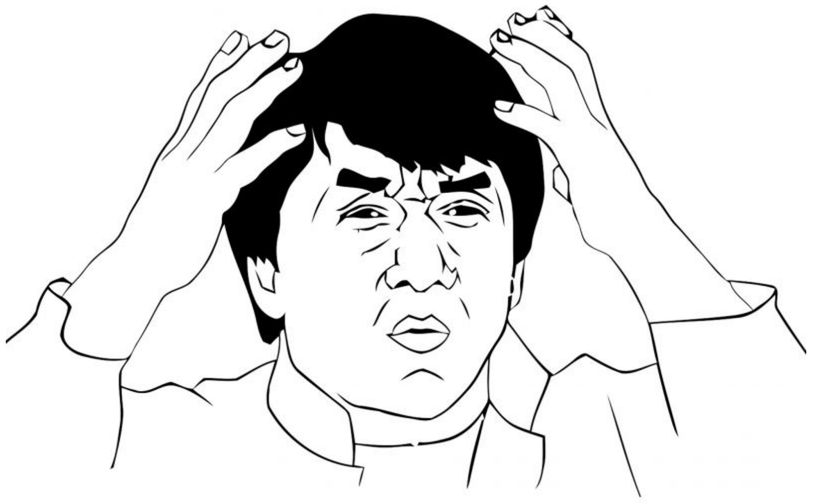
✓ Keine Ende-zu-Ende-Verschlüsselung

✓ Virenscan beim Anbieter

Virenscan beim Anbieter?

De-Mail

- ist auf den Namen registriert
- kostet 39ct
- halten die Nutzer für sicher



Für Massen-Angriffe:

- zu teuer

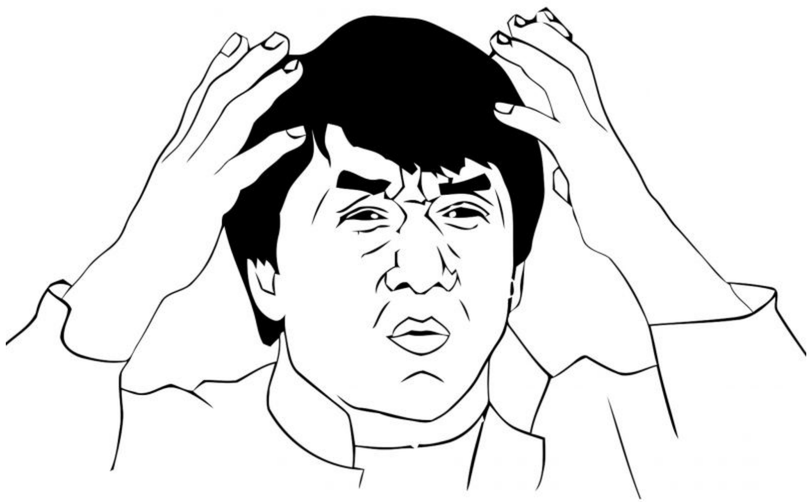
Für gezielte Angriffe:

- senkt die Vorsicht der Nutzer
- ermöglicht Obfuscation-Training

Virenscan beim Anbieter?

De-Mail

- ist auf den Namen registriert
- kostet 39ct
- halten die Nutzer für sicher



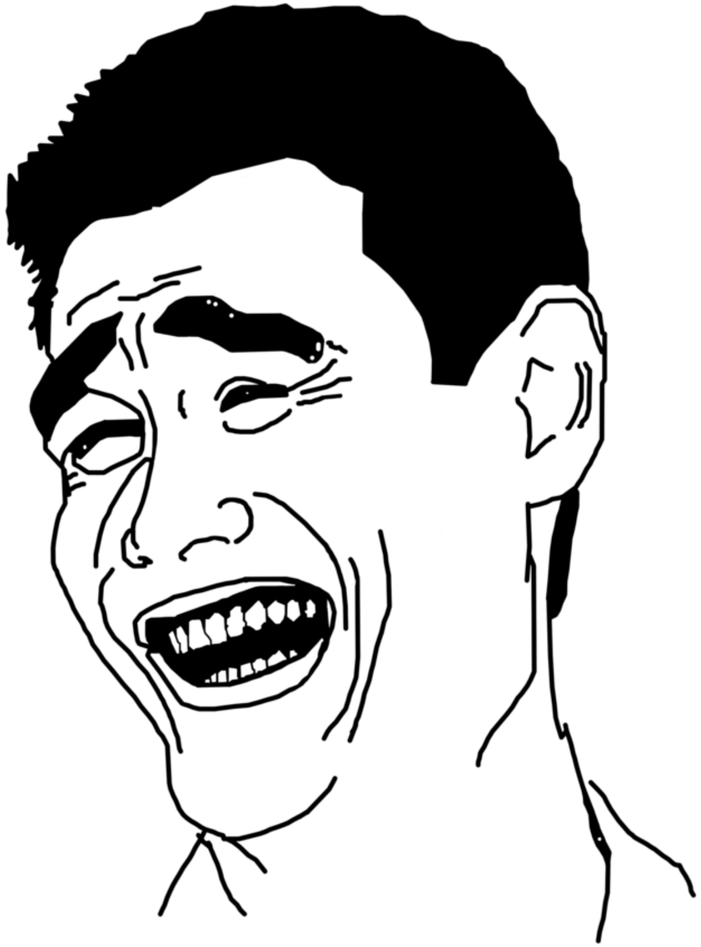
Andere Wege:

- URL statt Datei de-mailen
- Email
- Software-Download
- Flash-Expolit
- Java-Exploit
- …

Virenscan beim Anbieter?

Andere Wege:

- URL statt Datei de-mailen
- Email
- Software-Download
- Flash-Expolit
- Java-Exploit
- …



Virenscan beim Anbieter?

Andere Wege:

- URL statt Datei de-mailen
- Email
- Software-Download
- Flash-Expolit
- Java-Exploit
- …

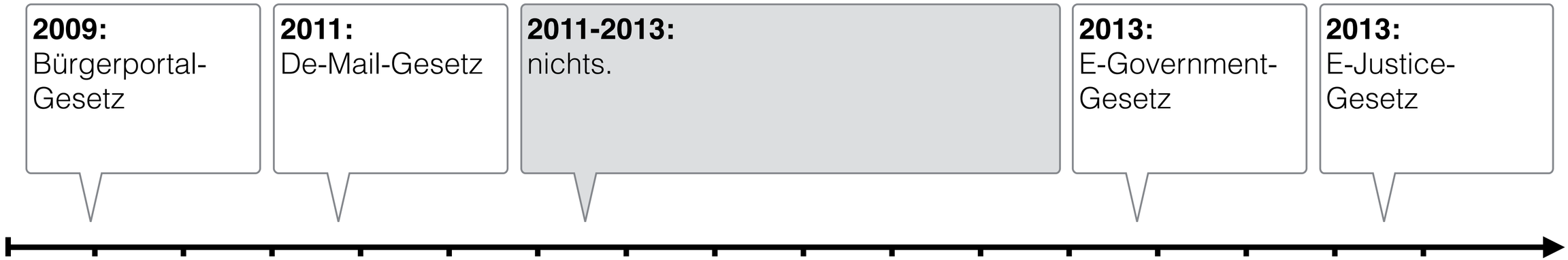
De-Mail Ein Traum für Angreifer

- ✓unverschlüsselt
- ✓nur wenige Anbieter
- ✓sensible Kommunikation

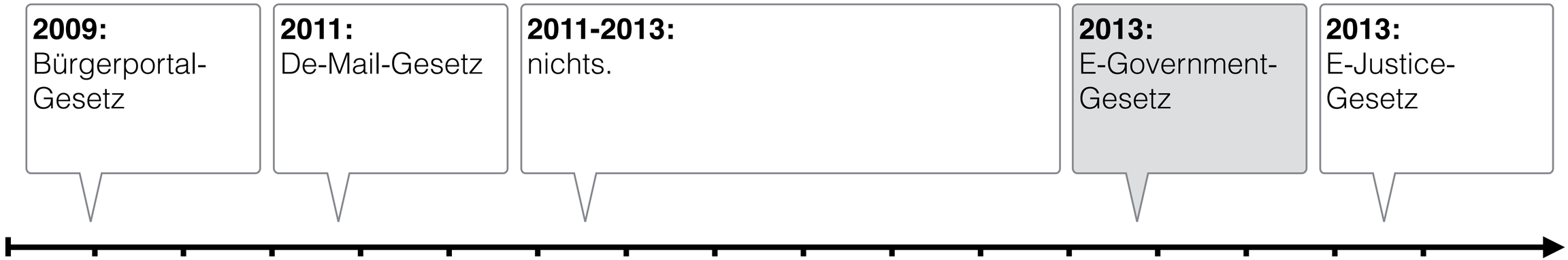
Ein Traum für BKA & BfVS

- ✓unverschlüsselt
- ✓nur wenige Anbieter
- ✓sensible Kommunikation
- ✓kein Spam

Was bisher geschah:

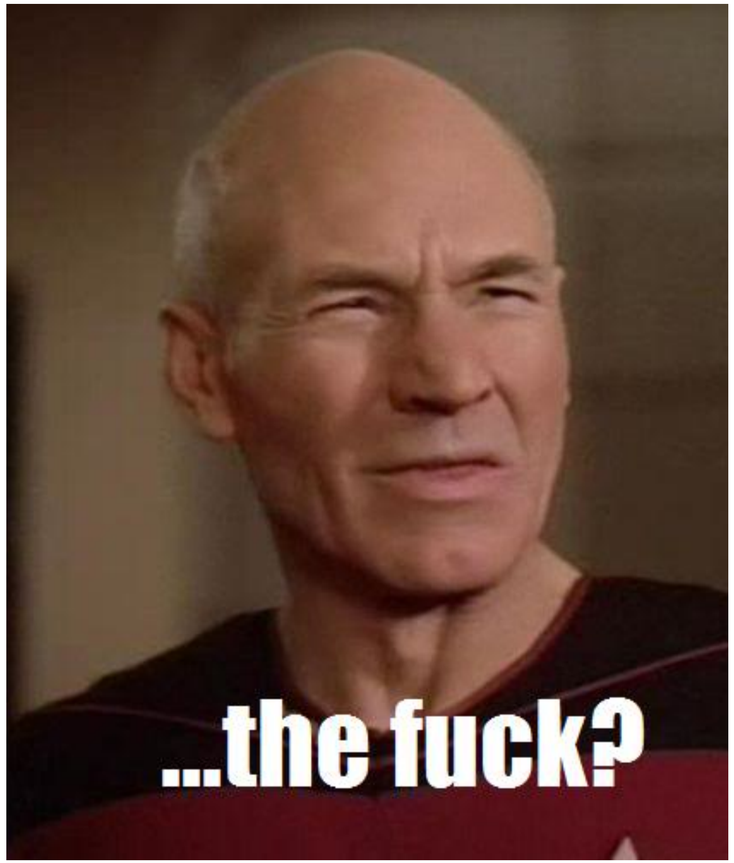


Was bisher geschah:



"...das Senden von Sozialdaten durch eine De-Mail-Nachricht an die jeweiligen akkreditierten Diensteanbieter – zur kurzfristigen automatisierten Entschlüsselung zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht – ist kein Übermitteln“

„Eine Entschlüsselung verstößt nicht gegen das Verschlüsselungsgebot.“



Werden dem Steuergeheimnis unterliegende Daten durch einen Amtsträger oder diesem nach Absatz 3 gleichgestellte Personen nach Maßgabe des § 87a Absatz 4 über De-Mail-Dienste im Sinne des § 1 des De-Mail-Gesetzes versendet, liegt **keine unbefugte Offenbarung**, Verwertung und kein unbefugter Abruf von dem Steuergeheimnis unterliegenden Daten vor, wenn beim Versenden eine kurzzeitige automatisierte **Entschlüsselung durch den akkreditierten Diensteanbieter** zum Zweck der Überprüfung auf Schadsoftware und zum Zweck der Weiterleitung an den Adressaten der De-Mail-Nachricht stattfindet.“

Die Hacker sollen erstmal hacken.

Dass in der Hackerszene die Überzeugung besteht, es gibt keinen Server auf dieser Welt, den ich nicht knacken kann und deren Lieblingsobjekte die Geheimdienste, NASA usw. sind, das mag schon sein.

Aber danach kann ich nicht einen vernünftigen Standard für einen Alltagsaustausch der Kommunikation etablieren.

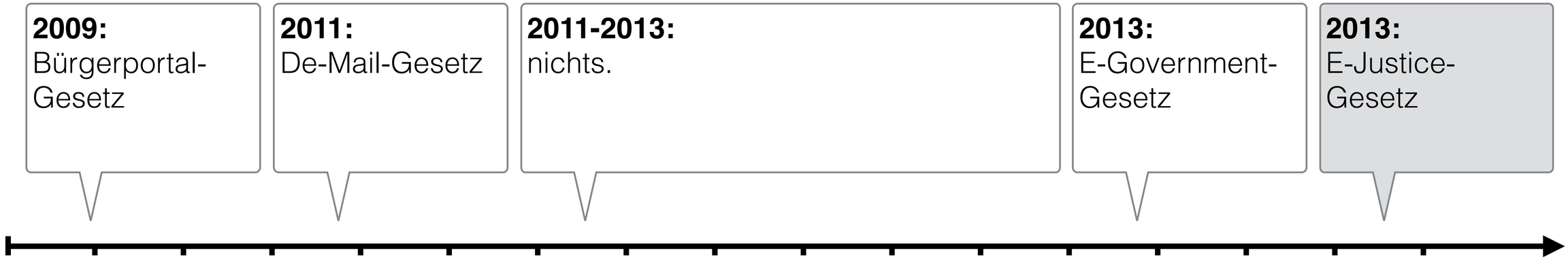
Dr. Helmut Fogt

Ende-zu-Ende-Verschlüsselung ist zu umständlich.

„Wenn ich im Urlaub in der Türkei in einen Internetshop gehe und meine De-Mail abrufen möchte, wie geht das?“

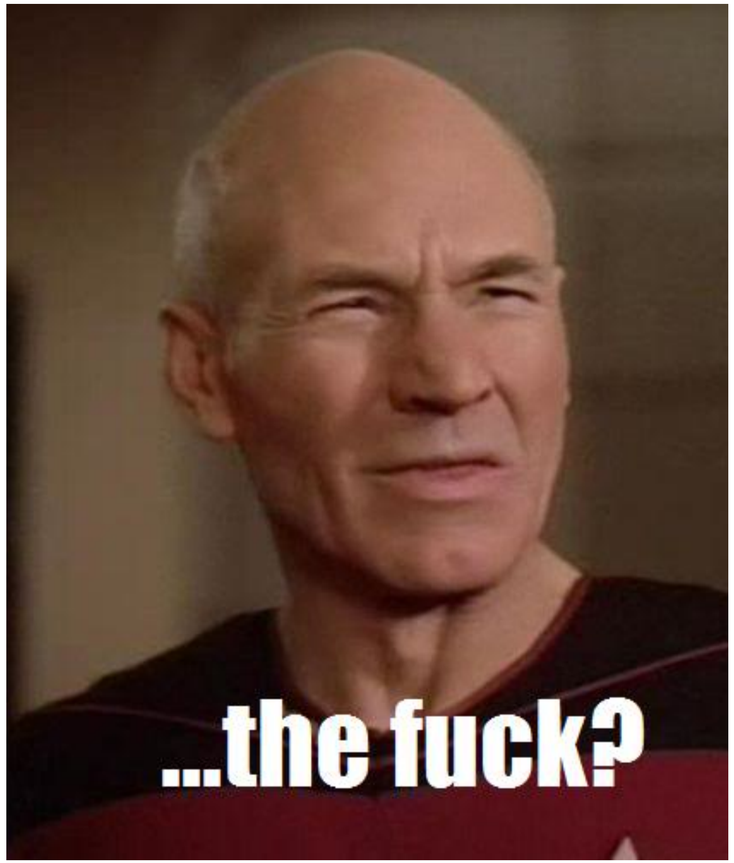
Manuel Höferlin, FDP

Was bisher geschah.



„…weil es sich bei der De-Mail-Nachricht auch um ein elektronisches Dokument im Sinne von § 371 handelt…“

De-Mails sind rechtsverbindlich, weil sie vom Anbieter signiert werden.



Auch wenn es sich bei **De-Mail** um ein Transportmedium, bei der **qualifizierten elektronischen Signatur** hingegen um ein dokumentenbezogenes Sicherungsmittel handelt, ist im Beweisrecht eine **Gleichbehandlung** beider Instrumente geboten, weil es sich bei der De-Mail-Nachricht auch um ein elektronisches Dokument im Sinne von § 371 handelt und die Absenderbestätigung dazu führt, **dass die Nachricht mit einer qualifizierten elektronischen Signatur des Providers versehen wird.**

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Funktion	Zweck	Techn. Umsetzung
Qualifizierte Elektronische Signatur 	▸Identitätsbeleg gegenüber Dritten ▸dokumentierte Willensbekundung	▸Dokumentgebundene Cryptographische Signatur mittels Private key auf SmartCard / Perso
eID	▸einmalige Identitäts-feststellung	▸einfaches Lesegerät, Code-Eingabe durch Nutzer

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Ausweiskontrolle:
Absender zeigt irgendwann mal seinen Ausweis.

De-Mail:

eID

Anmeldung

einmalige Identitätsfeststellung

De-Mail

Senden

Dokumentgebundene Cryptographische Signatur…

des Anbieters!

Qualifizierte elektronische Signatur

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Ausweiskontrolle:
Absender zeigt irgendwann mal seinen Ausweis.

Briefkasten:
Der Brief ist frankiert, adressiert und mit Absender versehen.

De-Mail:

eID

Anmeldung

einmalige Identitätsfeststellung

De-Mail

Senden

Dokumentgebundene Cryptographische Signatur…

des Anbieters!

Qualifizierte elektronische Signatur

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Ausweiskontrolle:
Absender zeigt irgendwann mal seinen Ausweis.

Briefkasten:
Der Brief ist frankiert, adressiert und mit Absender versehen.

De-Mail:

eID

Anmeldung

einmalige Identitätsfeststellung

De-Mail

Senden

Dokumentgebundene Cryptographische Signatur…

des Anbieters!

Qualifizierte elektronische Signatur

Vom Identitätsnachweis zur qualifizierten elektronischen Signatur

Ausweiskontrolle:
Absender zeigt irgendwann mal seinen Ausweis.

Briefkasten:
Der Brief ist frankiert, adressiert und mit Absender versehen.

Unterschrift:
Die Post unterschreibt. Und zwar jeden Brief.

De-Mail:

eID

Anmeldung

einmalige Identitätsfeststellung

De-Mail

Senden

Dokumentgebundene Cryptographische Signatur…

des Anbieters!

Qualifizierte elektronische Signatur

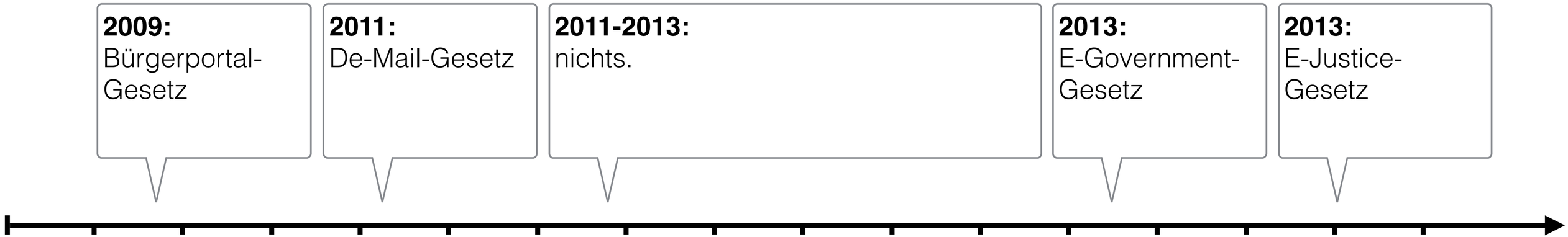
strengstens 100% kontrolliert

…immer diese Geheimniskrämerei!

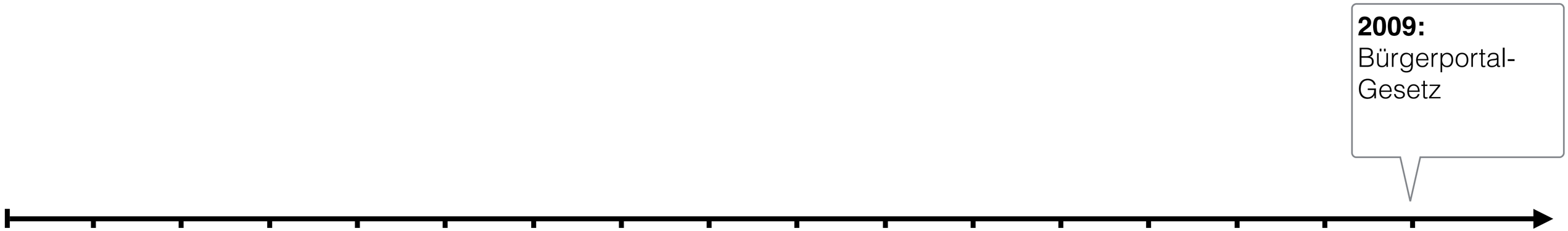
„Klageschriften kann man auch per Postkarte einreichen, eine Klageschrift, die im Briefumschlag ist, ist auch nicht in Geheimschrift abgefasst, sondern in Klartext.“

Richter Dr. Wolfram Viefhues

Die Hintermänner



Die Hintermänner



Die Hintermänner: Giersch Ventures

Maschinen für Sortierung, Frankierung Wägung […] insbesondere Briefen, Päckchen und Paketen […] Dienstleistungen über elektronische Kommunikationswege wie Internet und World Wide Web […] Zustellung von […] Briefen, Päckchen und Paketen […]

Die Hintermänner: Giersch Ventures

für „Rechenmaschinen, DV-Geräte und Computer, Werbung, Geschäftsführung, Unternehmensverwaltung, Büroarbeiten, Telekommunikation…“

Die Hintermänner: Giersch Ventures

für „Rechenmaschinen, DV-Geräte und Computer, Werbung, Geschäftsführung, Unternehmensverwaltung, Büroarbeiten, Telekommunikation…“

Die Hintermänner: Giersch Ventures

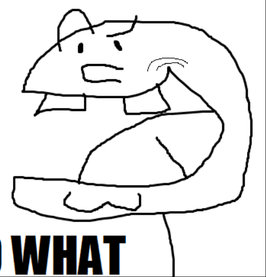
„nicht für die Dienstleistungen Tranportwesen, Postdienstleistungen…“

2.

Das BMI verpflichtet sich gegenüber Giersch Ventures, die Zeichen 'D-Mail' und/oder 'De-Mail' nicht für die Dienstleistungen

> *Transportwesen, insbesondere Postdienstleistungen, Abholung, Lagerung, Sortierung, Frankierung, Wägung, Bündelung, Verpackung und Zustellung von Postsendungen, insbesondere Briefen, Päckchen und Paketen; Kurierdienst; Paketdienst (Klasse 39)*

zu benutzen. Die Vertragsparteien sind sich darüber einig, dass von der in Satz 1 dieses Absatzes vereinbarten Unterlassungsverpflichtung insbesondere der Gebrauch der Zeichen "D-Mail" und/oder "De-Mail" für die Produktion und Weiterleitung physischer Postsendungen erfasst ist, nicht jedoch der Ziffer II. genannte De-Mail-Leistungsumfang.



Sicher online kommunizieren mit dem E-POSTBRIEF

Mit dem E-POSTBRIEF erledigen Sie alles in einem Portal: hier verschicken und empfangen Sie bequem digitale Briefe, Einschreiben online und sogar Faxe kostenlos. Überall, rund um die Uhr und dabei immer vertraulich und sicher.

Ihre Vorteile

- ✓ Wichtige und vertrauliche Unterlagen jederzeit bequem online versenden, empfangen oder im **› Online-Speicher** kostenlos ablegen.
- ✓ Mit der **› E-POST App** für's iPhone und Android Smartphones auch unterwegs E-POSTBRIEFE und digitalisierte Post online empfangen.

Willkommen beim E-POSTBRIEF Partner-Programm

Gemeinsam stärker werden: Profitieren Sie von den attraktiven Vorteilen des E-POSTBRIEF Partner-Programms. Wir möchten mit Ihnen Synergien schaffen, um erfolgreich zu sein: in Marketing & Vertrieb, in der Produktentwicklung und während der Betriebsphase. Partnerschaft heißt für uns: Gemeinsam alle Vorteile nutzen, die sich entlang der Wertschöpfungskette realisieren lassen.

Unsere Partner | Programm | Ziele | Vorteile

Unsere Partner

Sie möchten mehr über die Teilnehmer des E-POSTBRIEF Partner-Programms wissen? Hier finden Sie eine Auswahl:

BearingPoint GmbH

BearingPoint berät Unternehmen und Organisationen aus den Bereichen

Unsere Partner

Sie möchten mehr über die Teilnehmer des E-POSTBRIEF Partner-Programms wissen? Hier finden Sie eine Auswahl:

BearingPoint GmbH

BearingPoint berät Unternehmen und Organisationen aus den Bereichen Commercial Services, Financial Services und Public Services bei der Lösung ihrer dringendsten und wichtigsten Aufgaben.

›Mehr erfahren


BearingPoint®


CSC

Quizfrage:

Kunden, die bei 

kauften, kauften auch:

Quizfrage:

Kunden, die bei CSC De-Mail kauften, kauften auch:

Quizfrage:

Kunden, die bei CSC De-Mail kauften, kauften auch:

Staatstrojaner code review

Fazit: De-Mail

- ➡ Geht nicht über übliche Email-Sicherheit hinaus
- ➡ Ist unnötigerweise und absichtlich inkompatibel mit dem Rest der Welt
- ➡ Verschlüsselung nur auf dem Transportweg
- ➡ Wenige Server, erhöhte Attraktivität als Angriffsziel
- ➡ Rechtliche Nachteile und Risiken für die Nutzer
- ➡ **Ziele: Wirtschaftsförderung, Abhörbarkeit erhalten**

Keine Regierung ist so blöd,
ihren Bürgern ein abhörsicheres
Kommunikationsmedium zu geben.

Problem:

Agenda

- De-Mail
- **Email made in Germany**
- Schlandnet
- Cloud

GMX T-Online WEB.DE freenet

[Docs] [txt|pdf] [draft-hoffman-smt...] [Diff1] [Diff2]

Obsoleted by: 3207 PROPOSED STANDARD

Network Working Group P. Hoffman
Request for Comments: 2487 Internet Mail Consortium
Category: Standards Track January 1999

SMTP Service Extension for Secure SMTP over TLS

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

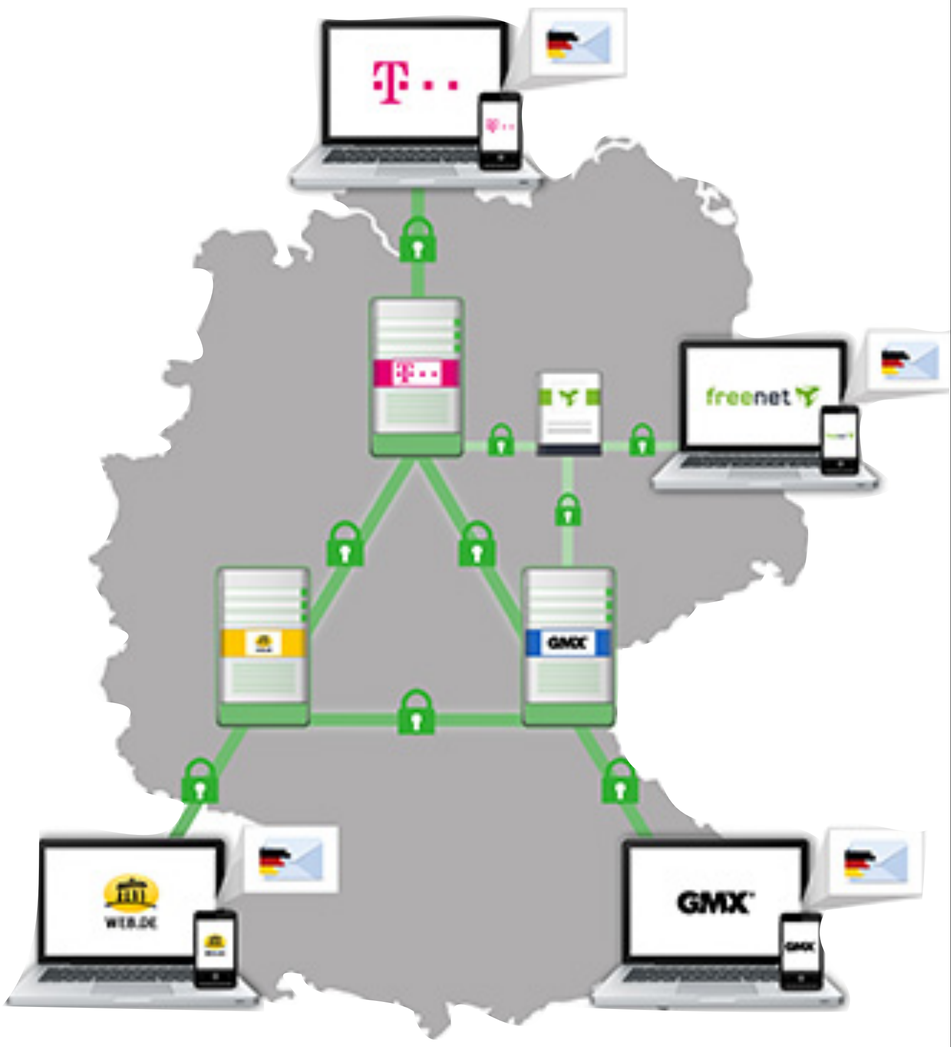
1. Abstract

This document describes an extension to the SMTP service that allows an SMTP server and client to use transport-layer security to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

2. Introduction

SMTP [RFC-821] servers and clients normally communicate in the clear over the Internet. In many cases, this communication goes through one or more router that is not controlled or trusted by either entity. Such an untrusted router might allow a third party to monitor or alter the communications between the server and client.

Further, there is often a desire for two SMTP agents to be able to authenticate each others' identities. For example, a secure SMTP server might only allow communications from other SMTP agents it knows, or it might act differently for messages received from an agent it knows than from one it doesn't know.



PROPOSED STANDARD
Errata Exist

Network Working Group
Request for Comments: 3207
Obsoletes: 2487
Category: Standards Track

P. Hoffman
Internet Mail Consortium
February 2002

SMTP Service Extension for Secure SMTP over Transport Layer Security

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

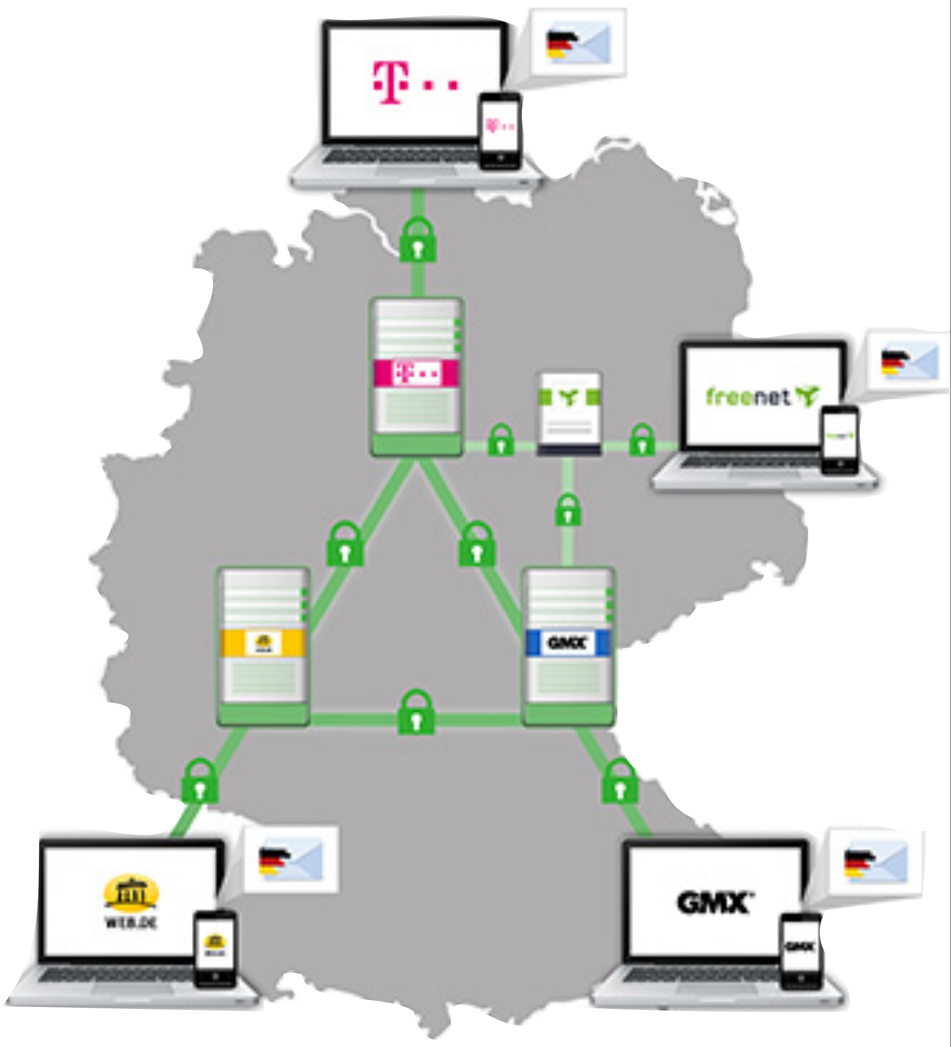
Abstract

This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

1. Introduction

SMTP [RFC2821] servers and clients normally communicate in the clear over the Internet. In many cases, this communication goes through one or more router that is not controlled or trusted by either entity. Such an untrusted router might allow a third party to monitor or alter the communications between the server and client.

Further, there is often a desire for two SMTP agents to be able to authenticate each others' identities. For example, a secure SMTP



[Docs] [txt|pdf] [draft-hoffman-rfc...] [Diff1] [Diff2] [Errata]

PROPOSED STANDARD
Errata Exist

Network Working Group
Request for Comments: 3207
Obsoletes: 2487
Category: Standards Track

P. Hoffman
Internet Mail Consortium
February 2002

SMTP Service Extension for Secure SMTP over Transport Layer Security

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

1. Introduction

SMTP [RFC2821] servers and clients normally communicate in the cle
over the Internet. In many cases, this communication goes through
one or more router that is not controlled or trusted by either
entity. Such an untrusted router might allow a third party to
monitor or alter the communications between the server and client.

Further, there is often a desire for two SMTP agents to be able t
authenticate each others' identities. For example, a secure SI

PROPOSED STANDARD
Errata Exist

Network Working Group
Request for Comments: 3207
Obsoletes: 2487
Category: Standards Track

P. Hoffman
Internet Mail Consortium

February 2002

SMTP Service Extension for Secure SMTP over Transport Layer Security

Status of this Memo

Copyright Notice

Abstract

This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

1. Introduction

SMTP [RFC2821] servers and clients normally communicate in the clear over the Internet. In many cases, this communication goes through one or more router that is not controlled or trusted by either entity. Such an untrusted router might allow a third party to monitor or alter the communications between the server and client.

Further, there is often a desire for two SMTP agents to be able to authenticate each others' identities. For example, a secure SMTP

[Docs] [txt|pdf] [draft-hoffman-rfc...] [Diff1] [Diff2] [Errata]

PROPOSED STANDARD
Errata Exist

Network Working Group — P. Hoffman
Request for Comments: 3207 — Internet Mail Consortium
Obsoletes: 2487 — February 2002
Category: Standards Track

SMTP Service Extension for Secure SMTP over Transport Layer Security

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

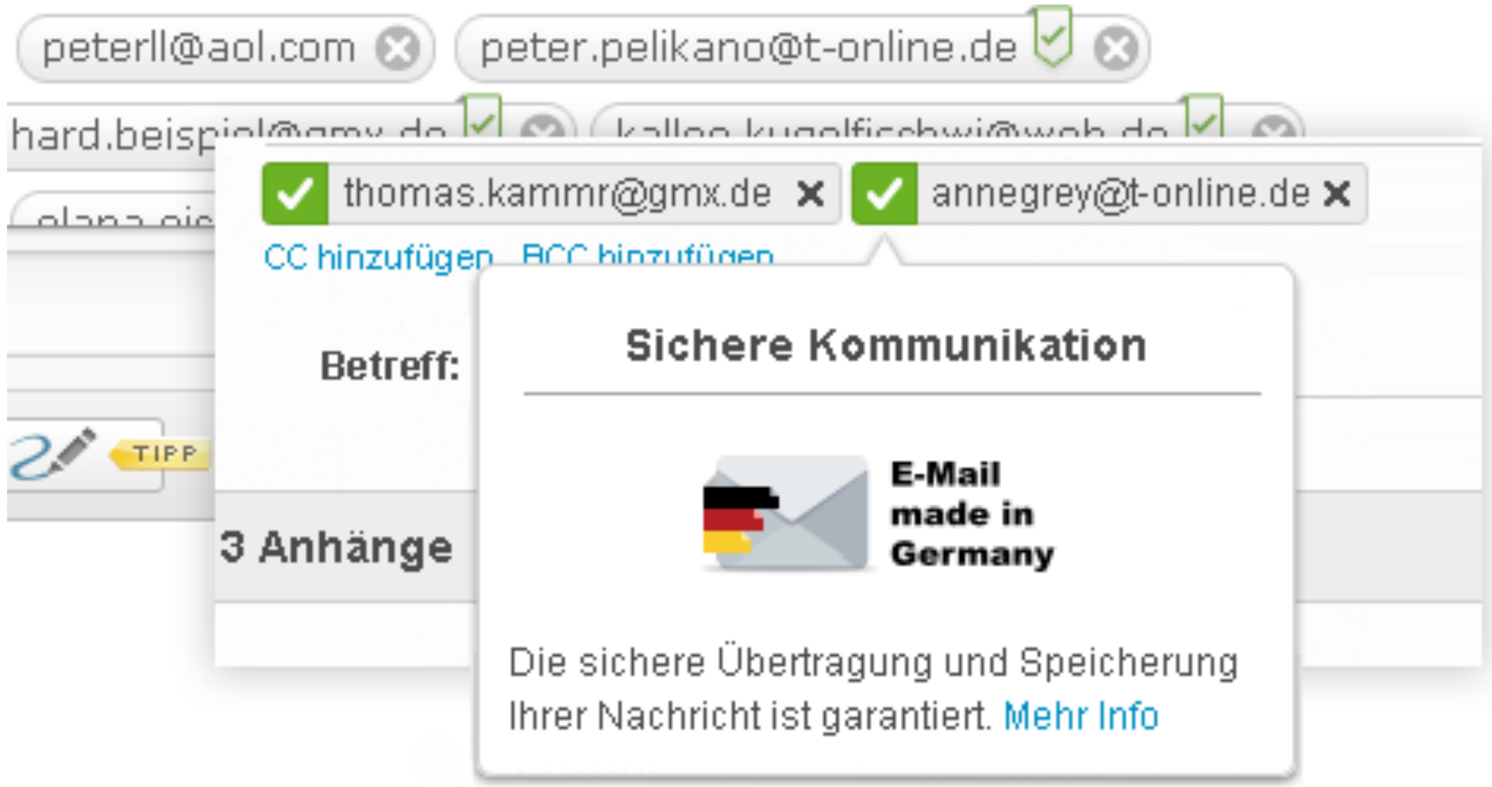
Abstract

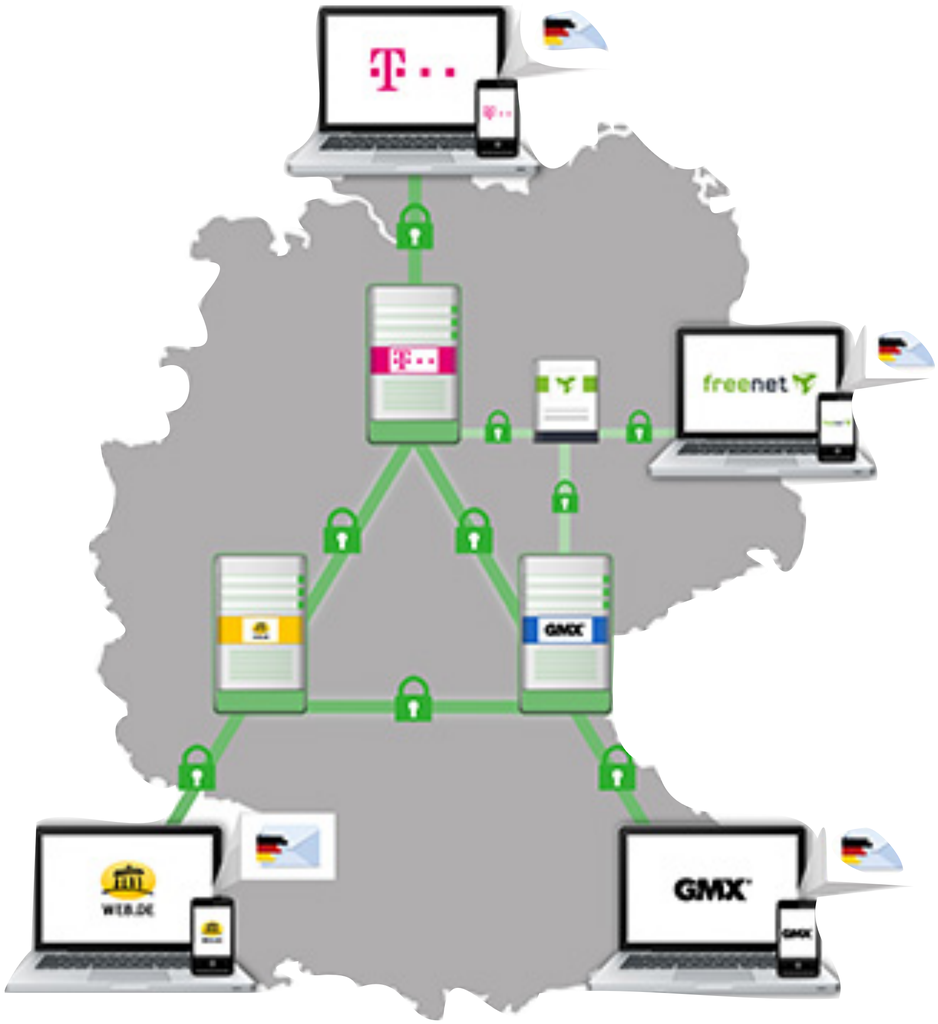
This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

1. Introduction

SMTP [RFC2821] servers and clients normally communicate in the clear over the Internet. In many cases, this communication goes through one or more router that is not controlled or trusted by either entity. Such an untrusted router might allow a third party to monitor or alter the communications between the server and client.

Further, there is often a desire for two SMTP agents to be able to authenticate each others' identities. For example, a secure SMTP


peterll@aol.com
peter.pelikano@t-online.de
thomas.kammr@gmx.de
annegrey@t-online.de
CC hinzufügen
BCC hinzufügen
Betreff:
TIPP
3 Anhänge
Sichere Kommunikation
E-Mail
made in
Germany
Die sichere Übertragung und Speicherung
Ihrer Nachricht ist garantiert. Mehr Info


freenet
GMX
WEB.DE
GMX

made in Germany. — Eingang

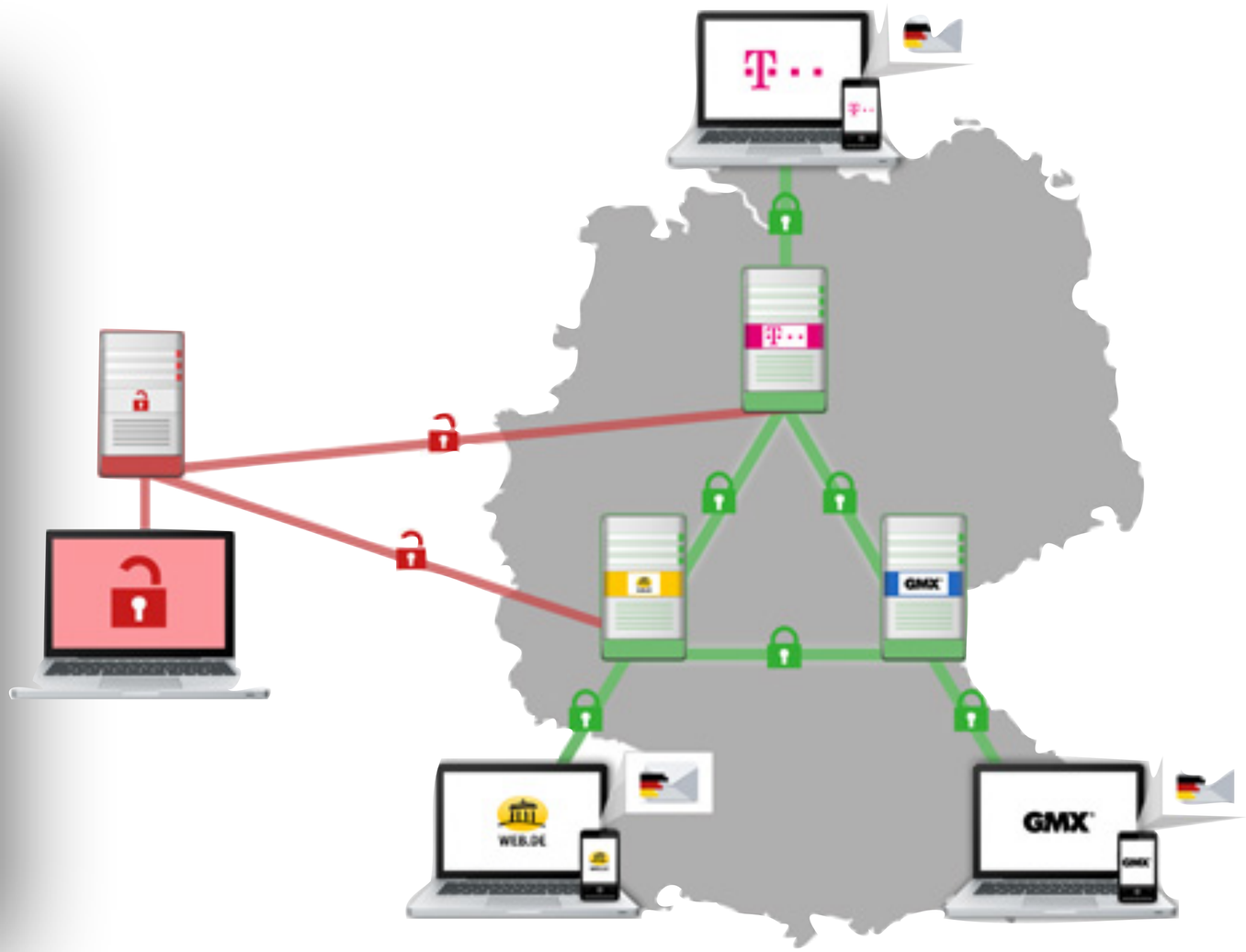
[redacted] 23. Dezember 2013 15:29

[redacted] Details ausblenden

made in Germany.

Bullshit.

Diese E-Mail wurde aus dem Sicherheitsverbund E-Mail made in Germany versendet: http://www.gmx.net/e-mail-made-in-germany



made in Germany. — Eingang

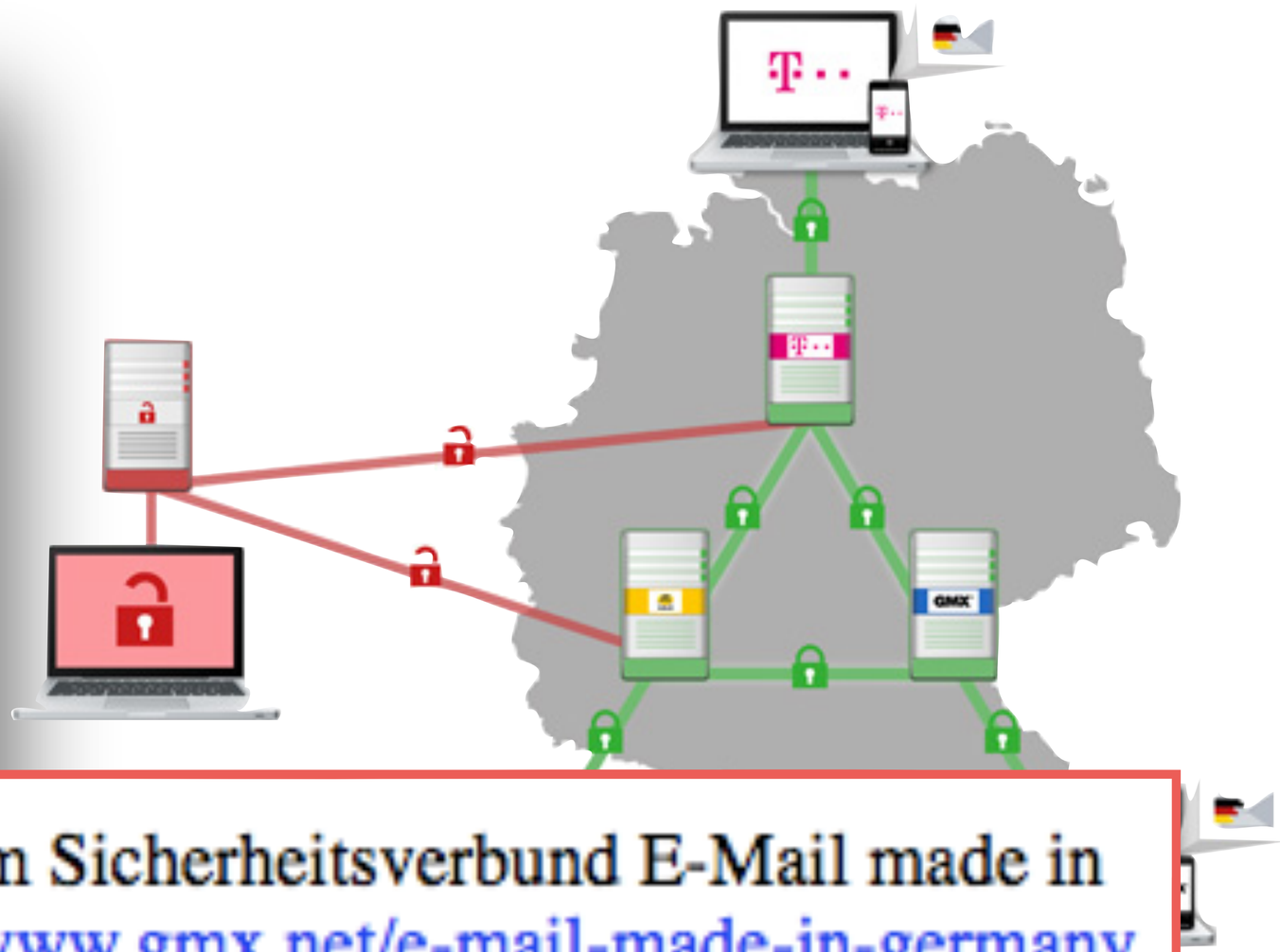
[redacted] 23. Dezember 2013 15:29

[redacted] Details ausblenden

made in Germany.

Bullshit.

Diese E-Mail wurde aus dem Sicherheitsverbund E-Mail made in Germany versendet: http://www.gmx.net/e-mail-made-in-germany



Diese E-Mail wurde aus dem Sicherheitsverbund E-Mail made in Germany versendet: http://www.gmx.net/e-mail-made-in-germany

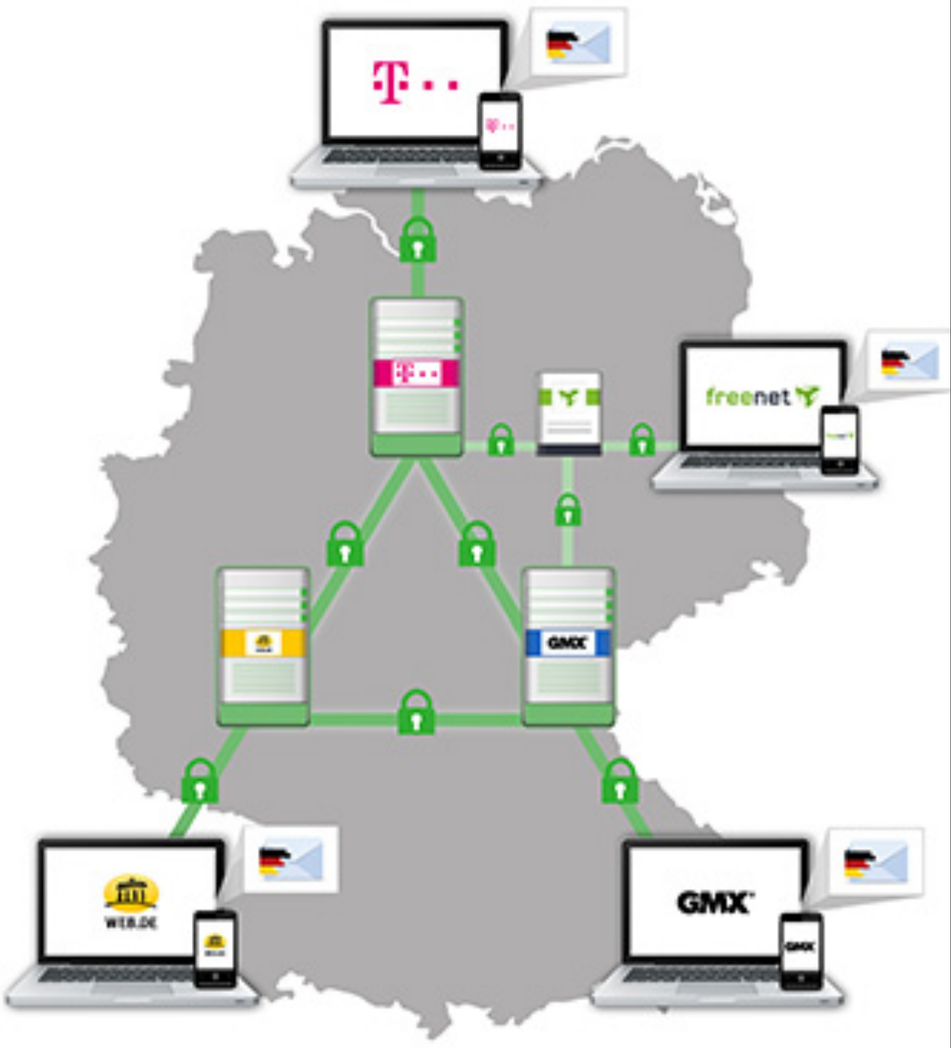
Quizfrage: Wo ist die unverschlüsselte Email?

A. Absender

B. Telekom

C. web.de

D. Empfänger



Quizfrage: Wo ist die unverschlüsselte Email?

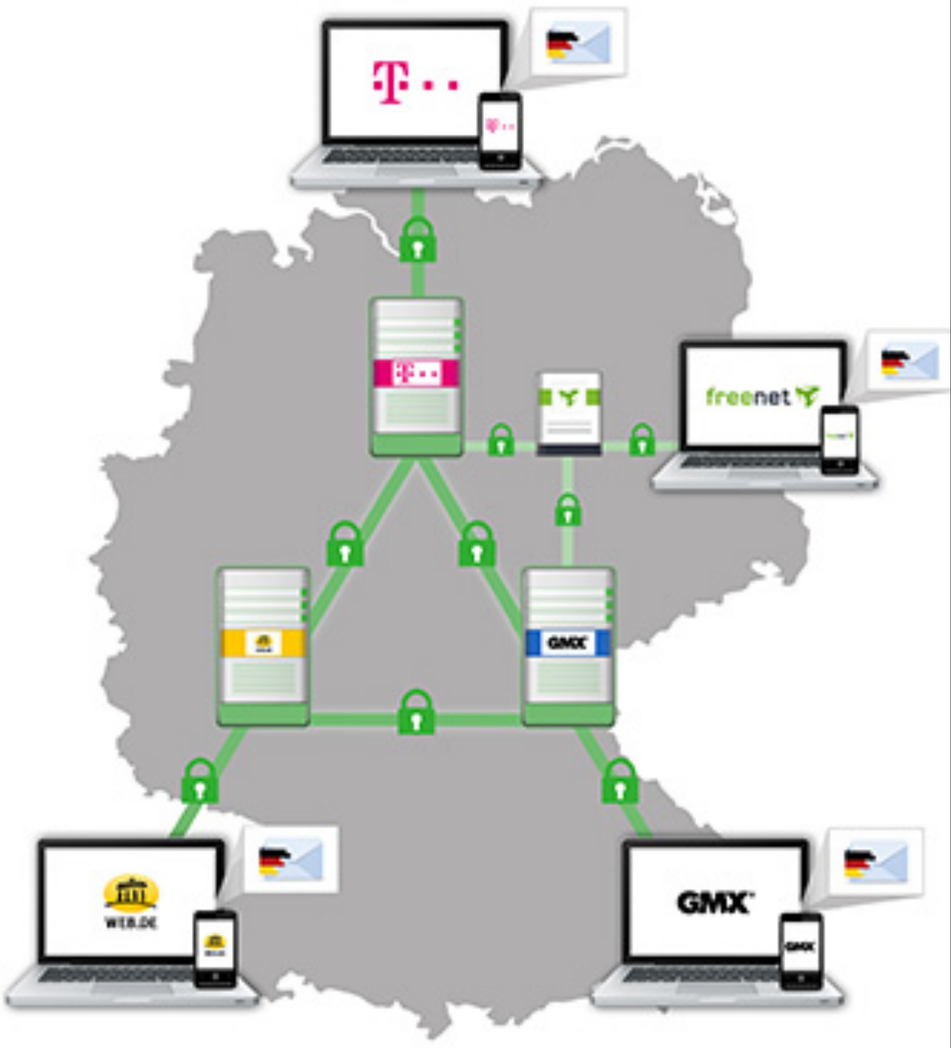
A. Absender

B. Telekom

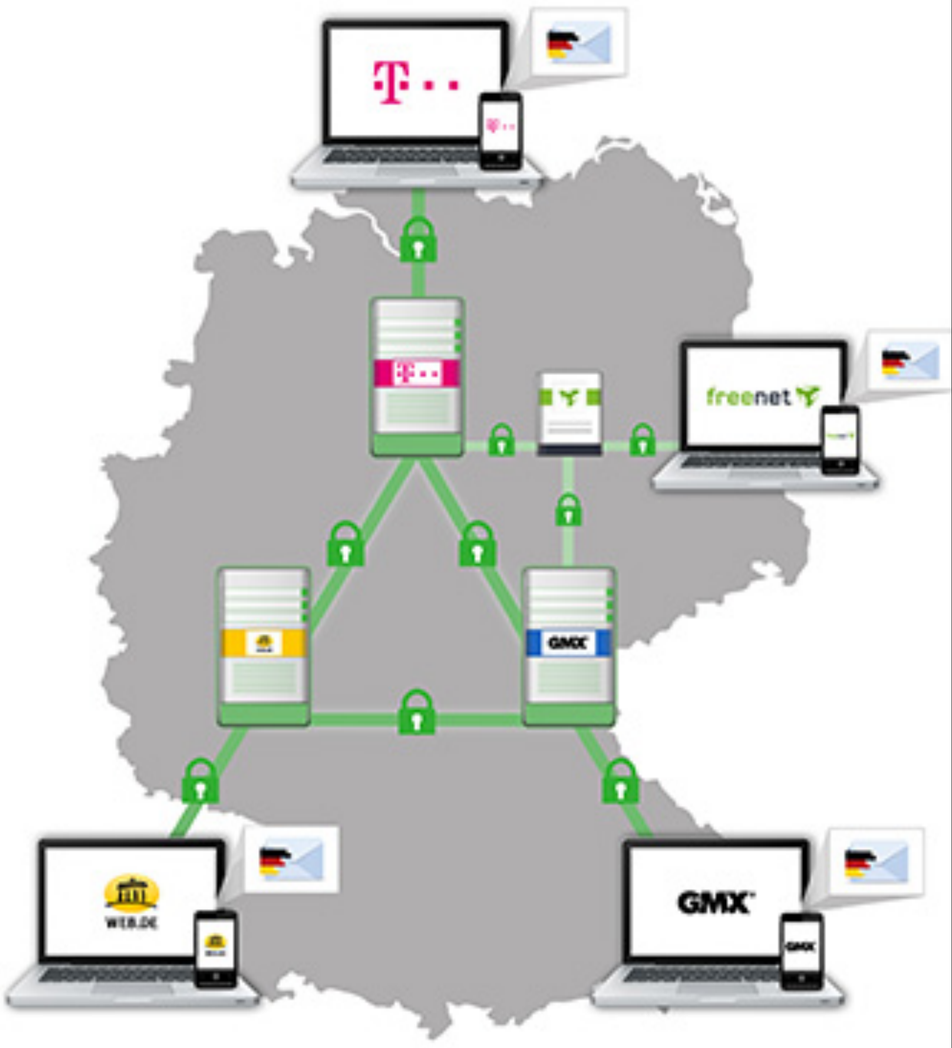
C. web.de

D. Empfänger

E. A, B, C und D.

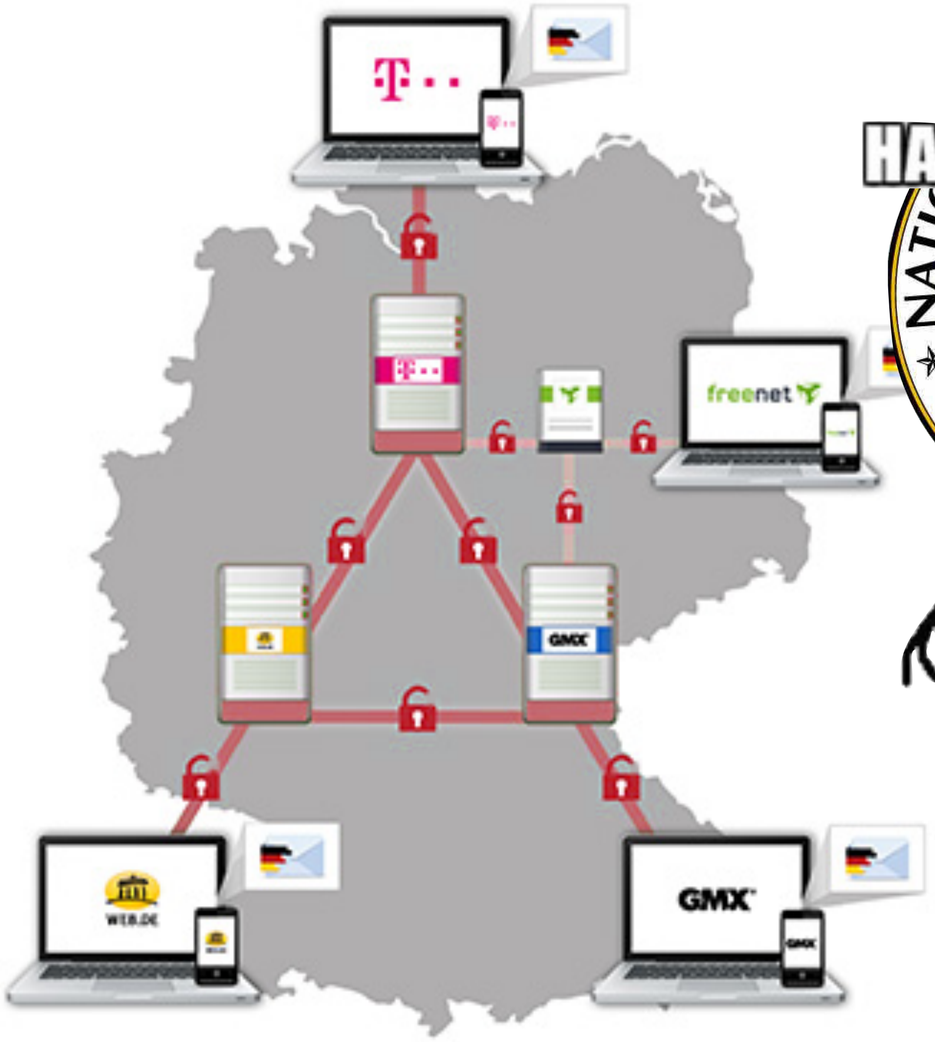


Quizfrage: Wie sah es denn vorher aus?




freenet
GMX
WEB.DE
GMX

Bundesnachrichtendienst
Bundeskriminalamt



HACK A WIFI PASSWORD

LIKE A BOSS

Bundesnachrichtendienst

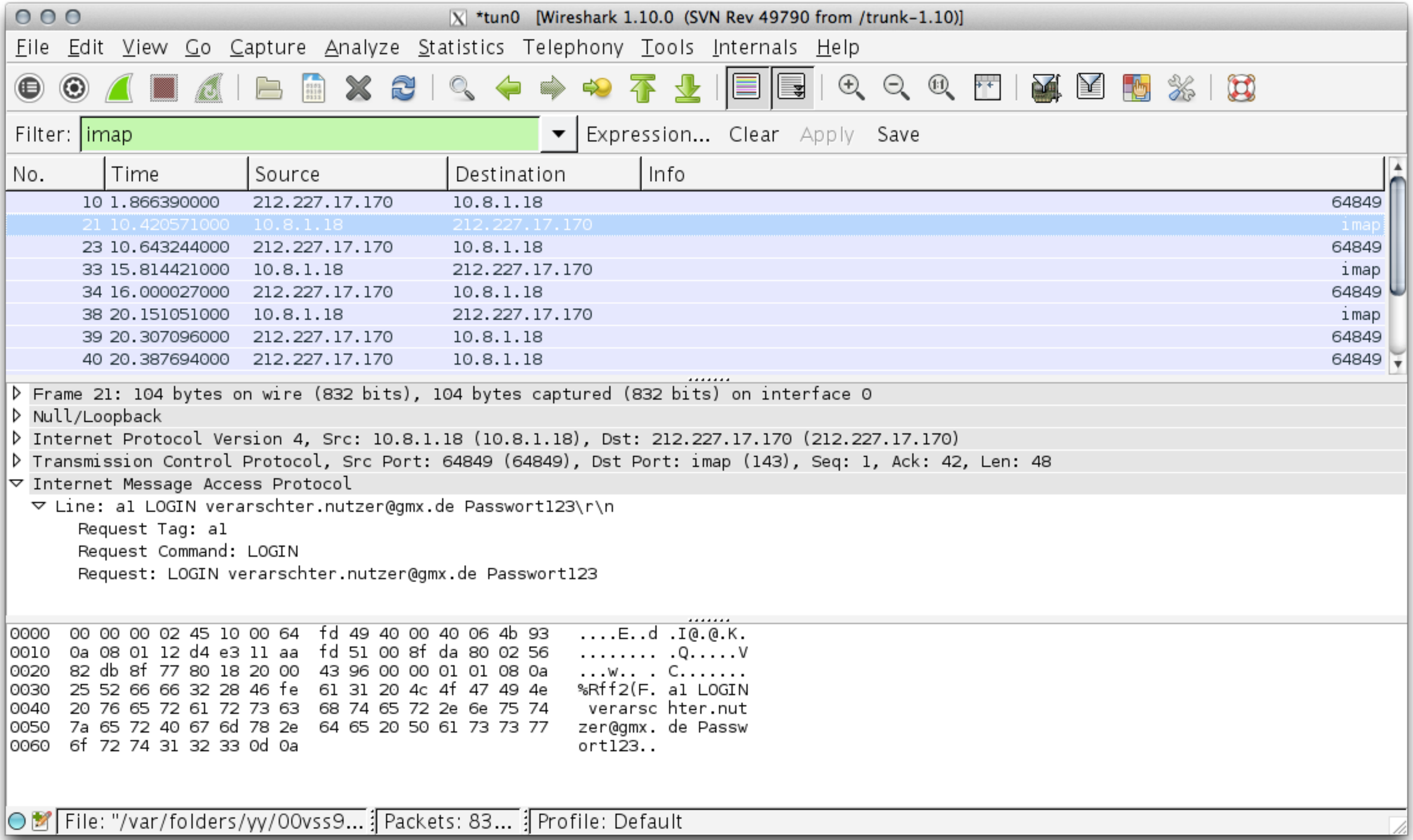
Bundeskriminalamt

Emails werden weiterhin auch unverschlüsselt übertragen

```
nc imapmail.t-online.de 143
a1 LOGIN noch.ein.nutzer@t-online.de Passwort123
a2 LIST "" "*"
a3 EXAMINE INBOX
a4 FETCH 2 BODY[]
a5 LOGOUT
EOF
```

Emails werden weiterhin auch unverschlüsselt übertragen

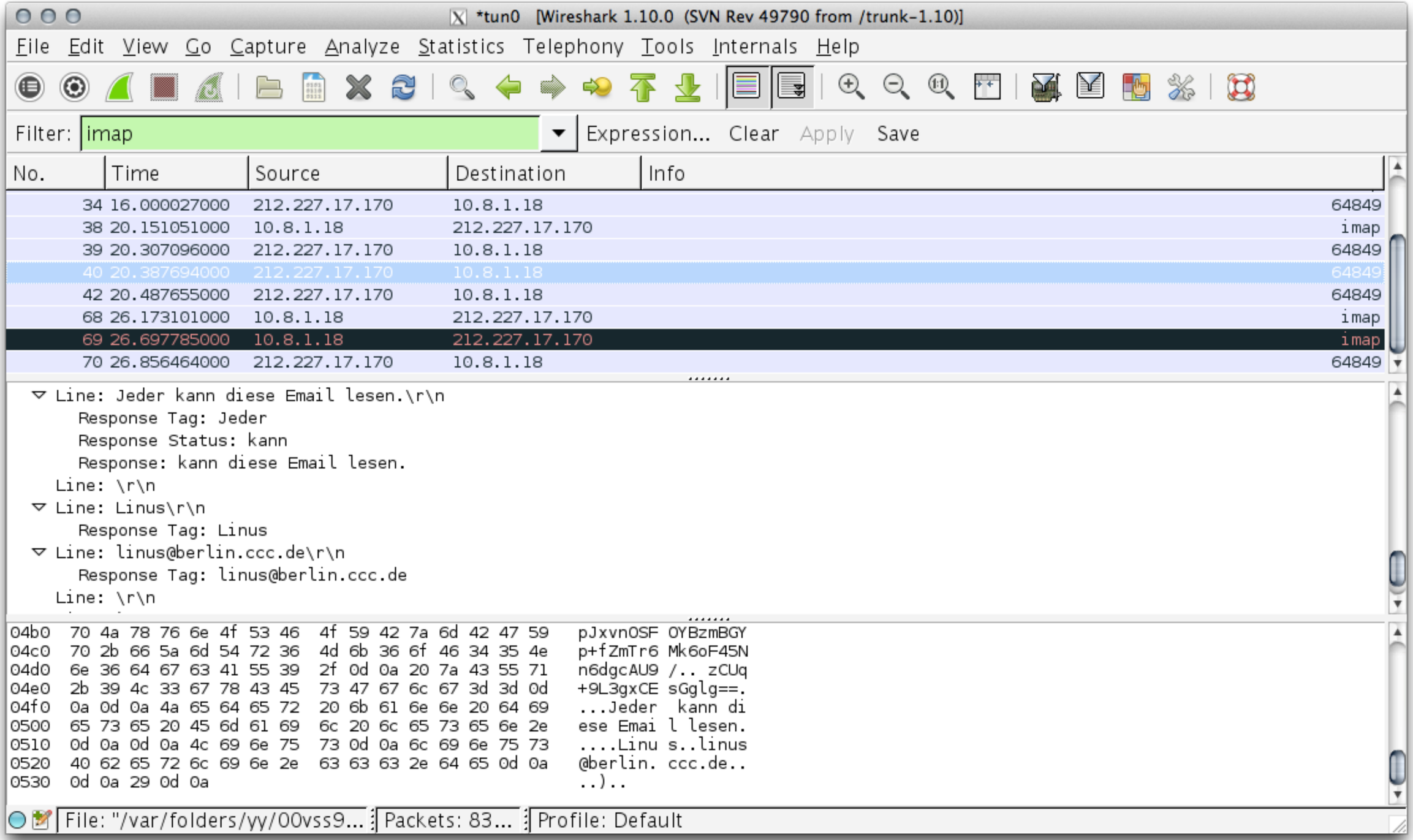
```
nc imap.gmx.net 143 << EOF
a1 LOGIN verarschter.nutzer@gmx.de Passwort123
a2 LIST "" "*"
a3 EXAMINE INBOX
a4 FETCH 3 BODY[]
a5 LOGOUT
EOF
```


*tun0 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: imap
Expression... Clear Apply Save
No. Time Source Destination Info
10 1.866390000 212.227.17.170 10.8.1.18 64849
21 10.420571000 10.8.1.18 212.227.17.170 imap
23 10.643244000 212.227.17.170 10.8.1.18 64849
33 15.814421000 10.8.1.18 212.227.17.170 imap
34 16.000027000 212.227.17.170 10.8.1.18 64849
38 20.151051000 10.8.1.18 212.227.17.170 imap
39 20.307096000 212.227.17.170 10.8.1.18 64849
40 20.387694000 212.227.17.170 10.8.1.18 64849
Frame 21: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 10.8.1.18 (10.8.1.18), Dst: 212.227.17.170 (212.227.17.170)
Transmission Control Protocol, Src Port: 64849 (64849), Dst Port: imap (143), Seq: 1, Ack: 42, Len: 48
Internet Message Access Protocol
Line: a1 LOGIN verarschter.nutzer@gmx.de Passwort123\r\n
Request Tag: a1
Request Command: LOGIN
Request: LOGIN verarschter.nutzer@gmx.de Passwort123
0000 00 00 00 02 45 10 00 64 fd 49 40 00 40 06 4b 93 ....E..d .I@.@.K.
0010 0a 08 01 12 d4 e3 11 aa fd 51 00 8f da 80 02 56 ..... .Q.....V
0020 82 db 8f 77 80 18 20 00 43 96 00 00 01 01 08 0a ...w.. . C.....
0030 25 52 66 66 32 28 46 fe 61 31 20 4c 4f 47 49 4e %Rff2(F. a1 LOGIN
0040 20 76 65 72 61 72 73 63 68 74 65 72 2e 6e 75 74 verarsc hter.nut
0050 7a 65 72 40 67 6d 78 2e 64 65 20 50 61 73 73 77 zer@gmx. de Passw
0060 6f 72 74 31 32 33 0d 0a ort123..
File: "/var/folders/yy/00vss9...
Packets: 83...
Profile: Default

```
    40 20.387694000   212.227.17.170      10.8.1.18

rame 21: 104 bytes on wire (832 bits), 104 bytes captured (83
ull/Loopback
nternet Protocol Version 4, Src: 10.8.1.18 (10.8.1.18), Dst:
ransmission Control Protocol, Src Port: 64849 (64849), Dst Po
nternet Message Access Protocol
▼ Line: a1 LOGIN verarschter.nutzer@gmx.de Passwort123\r\n
    Request Tag: a1
    Request Command: LOGIN
    Request: LOGIN verarschter.nutzer@gmx.de Passwort123


0  00 00 00 02 45 10 00 64  fd 49 40 00 40 06 4b 93   ....E..d
0  0a 08 01 12 d4 e3 11 aa  fd 51 00 8f da 80 02 56   .....Q.....V
0  82 db 8f 77 80 18 20 00  43 96 00 00 01 01 08 0a   ...w.. .C.....
```


*tun0 [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: imap
Expression... Clear Apply Save
No. Time Source Destination Info
34 16.000027000 212.227.17.170 10.8.1.18 64849
38 20.151051000 10.8.1.18 212.227.17.170 imap
39 20.307096000 212.227.17.170 10.8.1.18 64849
40 20.387694000 212.227.17.170 10.8.1.18 64849
42 20.487655000 212.227.17.170 10.8.1.18 64849
68 26.173101000 10.8.1.18 212.227.17.170 imap
69 26.697785000 10.8.1.18 212.227.17.170 imap
70 26.856464000 212.227.17.170 10.8.1.18 64849
Line: Jeder kann diese Email lesen.\r\n
Response Tag: Jeder
Response Status: kann
Response: kann diese Email lesen.
Line: \r\n
Line: Linus\r\n
Response Tag: Linus
Line: linus@berlin.ccc.de\r\n
Response Tag: linus@berlin.ccc.de
Line: \r\n
04b0 70 4a 78 76 6e 4f 53 46 4f 59 42 7a 6d 42 47 59 pJxvnOSF OYBzmBGY
04c0 70 2b 66 5a 6d 54 72 36 4d 6b 36 6f 46 34 35 4e p+fZmTr6 Mk6oF45N
04d0 6e 36 64 67 63 41 55 39 2f 0d 0a 20 7a 43 55 71 n6dgcAU9 /.. zCUq
04e0 2b 39 4c 33 67 78 43 45 73 47 67 6c 67 3d 3d 0d +9L3gxCE sGglg==.
04f0 0a 0d 0a 4a 65 64 65 72 20 6b 61 6e 6e 20 64 69 ...Jeder kann di
0500 65 73 65 20 45 6d 61 69 6c 20 6c 65 73 65 6e 2e ese Emai l lesen.
0510 0d 0a 0d 0a 4c 69 6e 75 73 0d 0a 6c 69 6e 75 73 ....Linu s..linus
0520 40 62 65 72 6c 69 6e 2e 63 63 63 2e 64 65 0d 0a @berlin. ccc.de..
0530 0d 0a 29 0d 0a ..)..
File: "/var/folders/yy/00vss9...
Packets: 83...
Profile: Default

38	20.151051000	10.8.1.18	212.227.17.170
39	20.307096000	212.227.17.170	10.8.1.18
40	20.387694000	212.227.17.170	10.8.1.18
42	20.487655000	212.227.17.170	10.8.1.18
68	26.173101000	10.8.1.18	212.227.17.170
69	26.697785000	10.8.1.18	212.227.17.170
70	26.856464000	212.227.17.170	10.8.1.18

```
▽ Line: Jeder kann diese Email lesen.\r\n
    Response Tag: Jeder
    Response Status: kann
    Response: kann diese Email lesen.
  Line: \r\n
▽ Line: Linus\r\n
    Response Tag: Linus
▽ Line: linus@berlin.ccc.de\r\n
    Response Tag: linus@berlin.ccc.de
  Line: \r\n
```

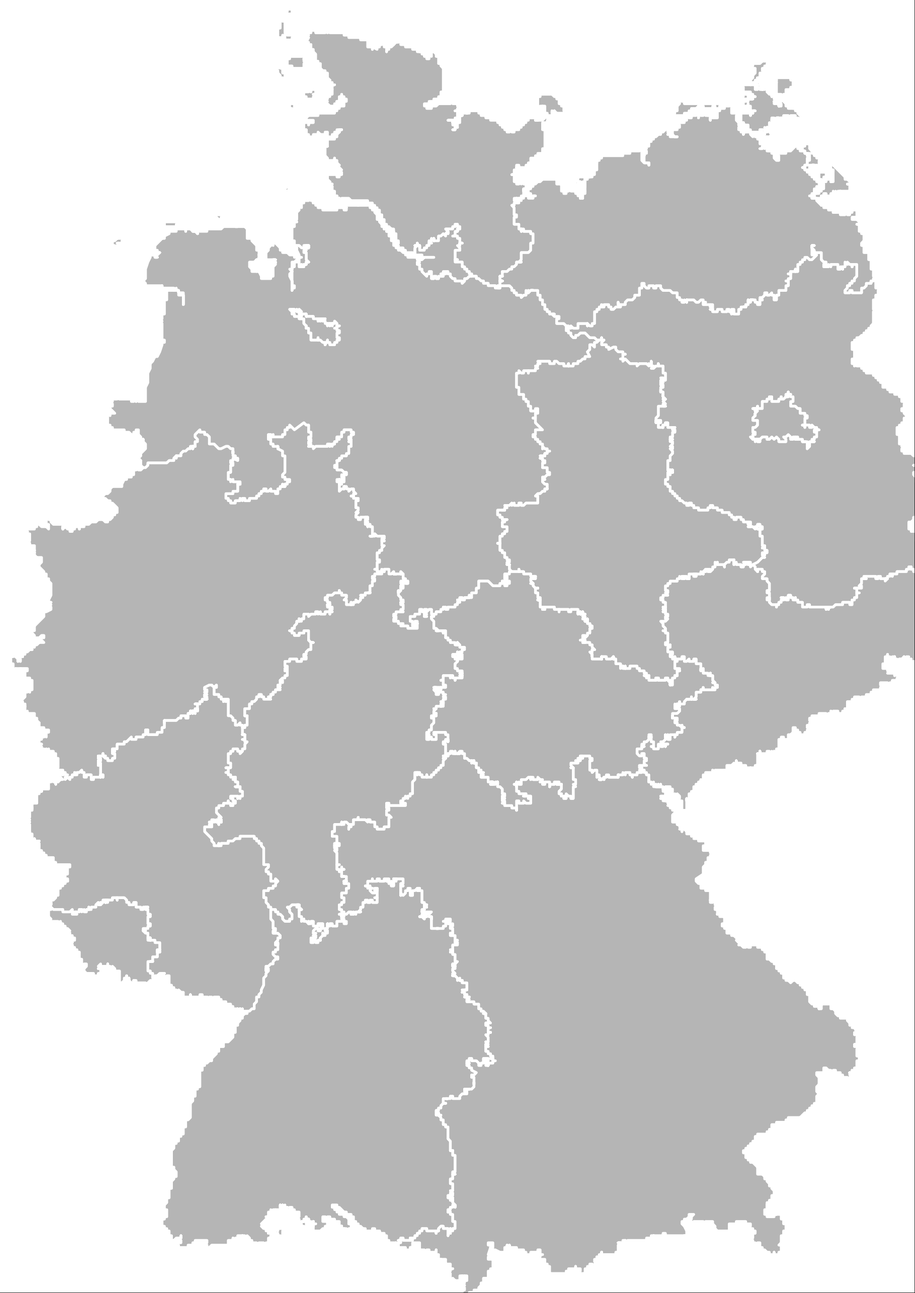
```
04b0  70 4a 78 76 6e 4f 53 46  4f 59 42 7a 6d 42 47 59   pJxvnOSF OYBzmBGY
04c0  70 2b 66 5a 6d 54 72 36  4d 6b 36 6f 46 34 35 4e   p+fZmTr6 Mk6oF45N
04d0  6e 36 64 67 63 41 55 39  2f 0d 0a 20 7a 43 55 71   n6dgcAU9 /.. zCUq
04e0  2b 39 4c 33 67 78 43 45  73 47 67 6c 67 3d 3d 0d   +9L3gxCE sGglg==.
```

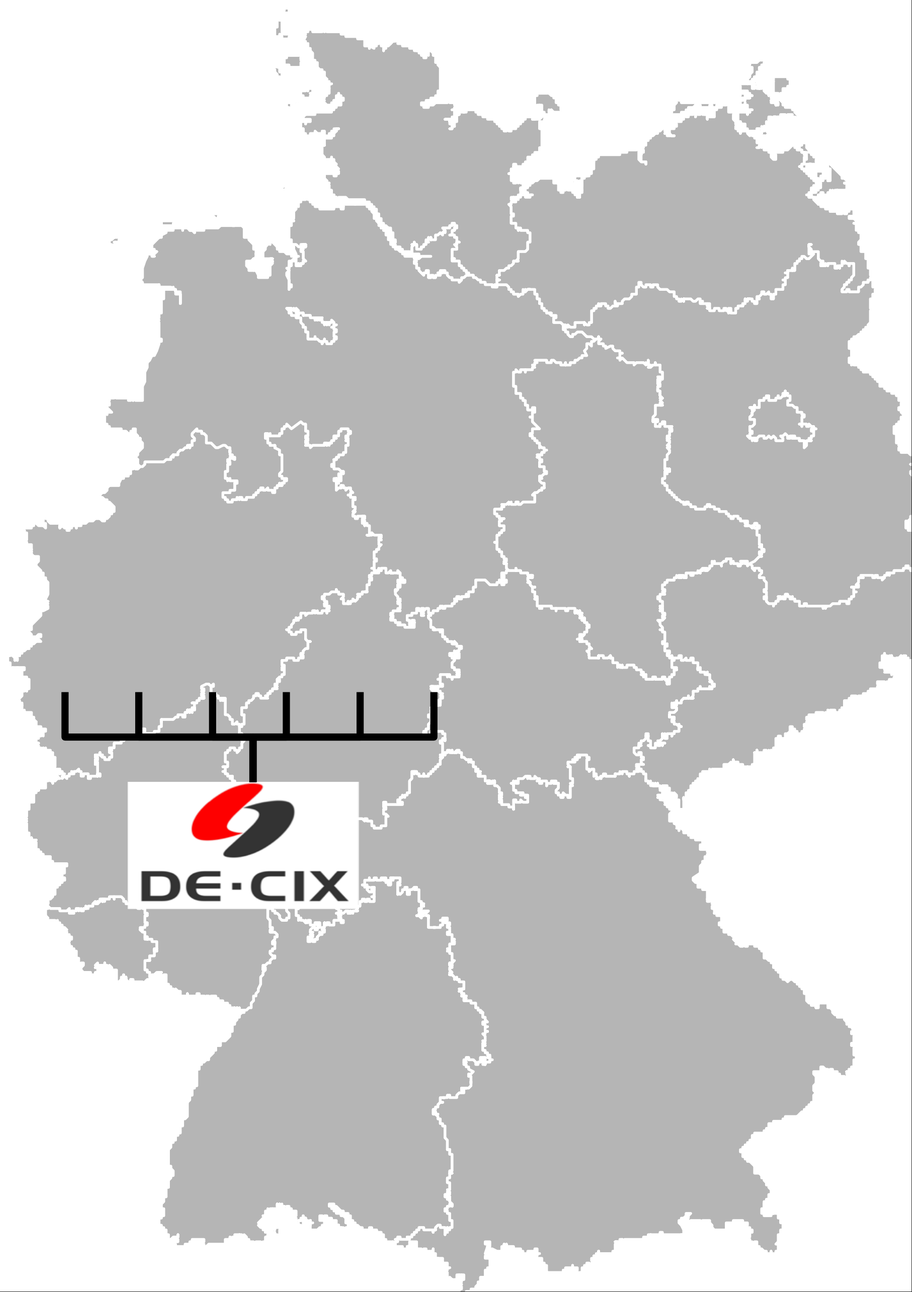
Fazit: Email made in Germany

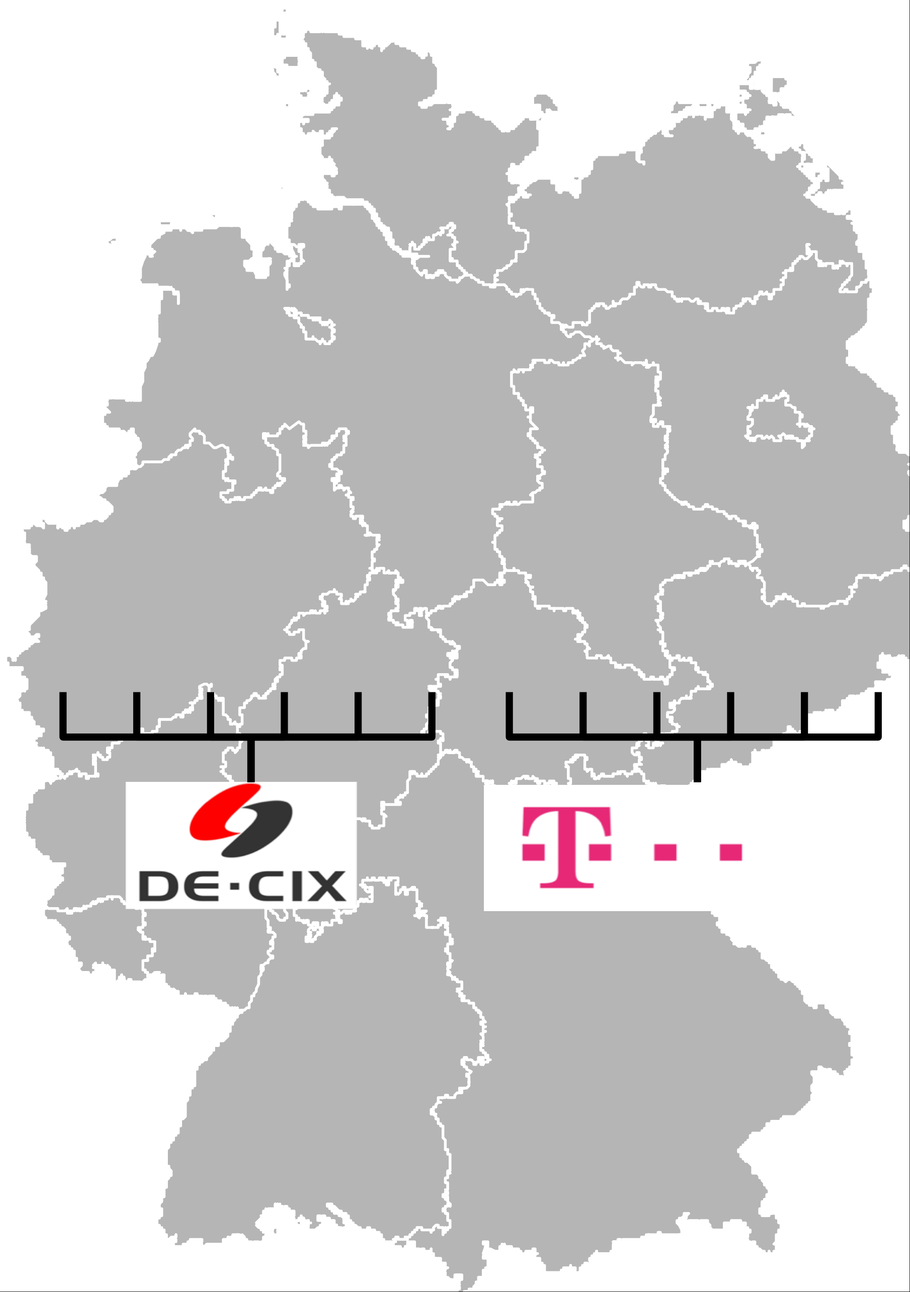
- ➡ Umsetzung von fast 20 Jahre alten Standards
- ➡ Für viele Jahre waren die Emails nicht verschlüsselt
- ➡ Verschlüsselung nur auf dem Transportweg
- ➡ Mit anderen Anbietern genau so möglich
- ➡ Gmail macht es seit jeher
- ➡ Unverschlüsseltes Abholen und Senden weiterhin möglich

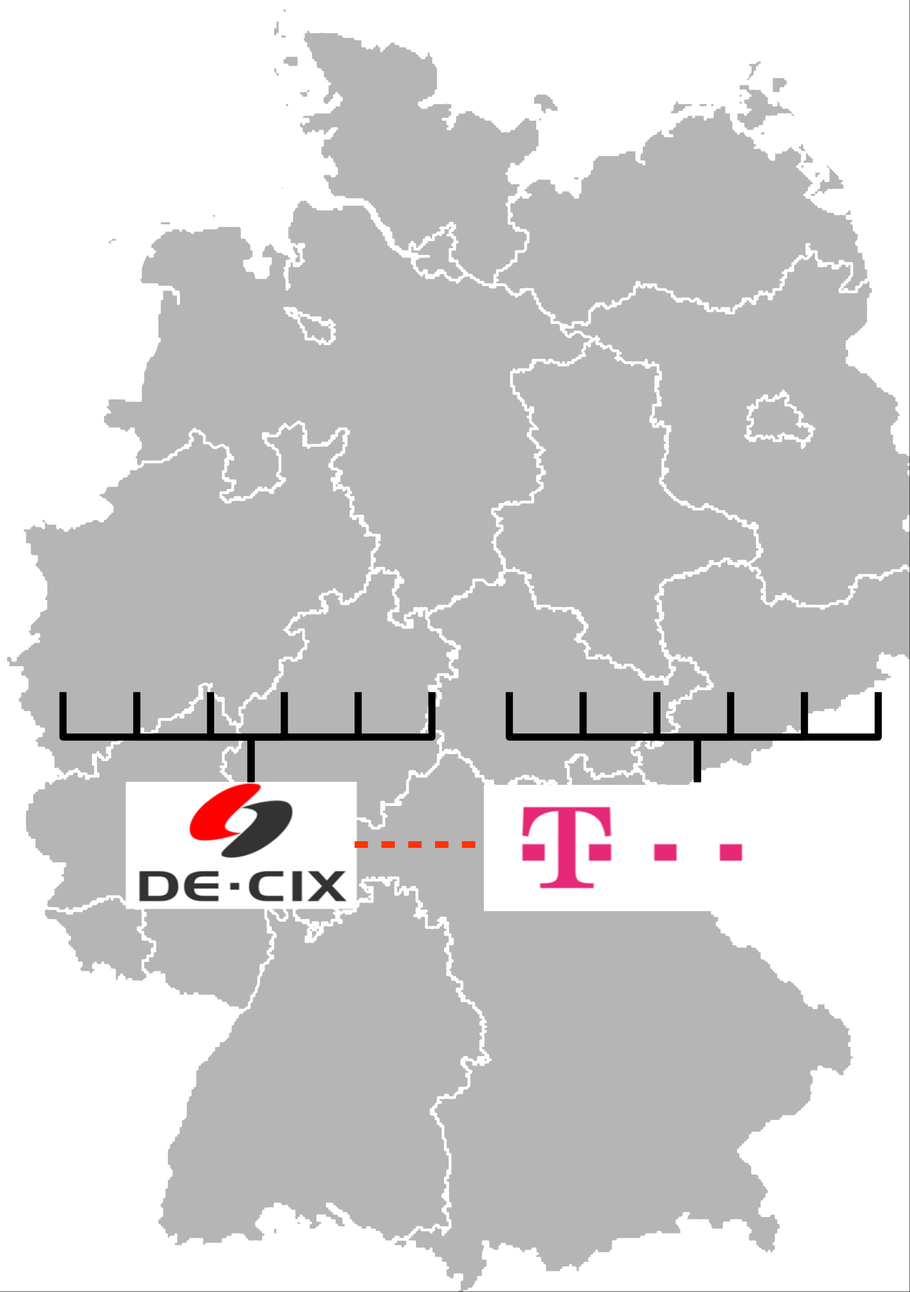
Agenda

- De-Mail
- Email made in Germany
- **Schlandnet**
- Cloud

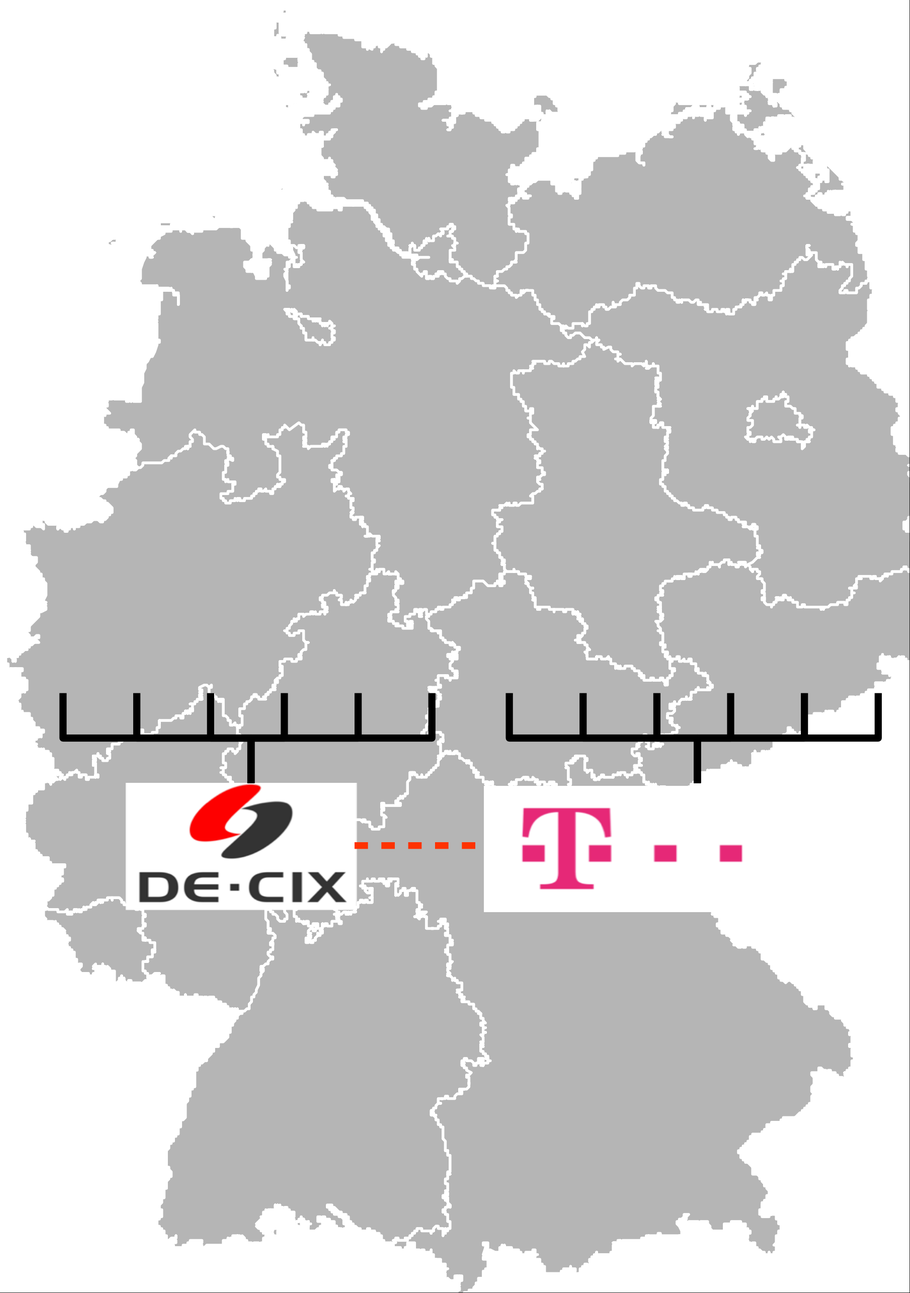



DE·CIX

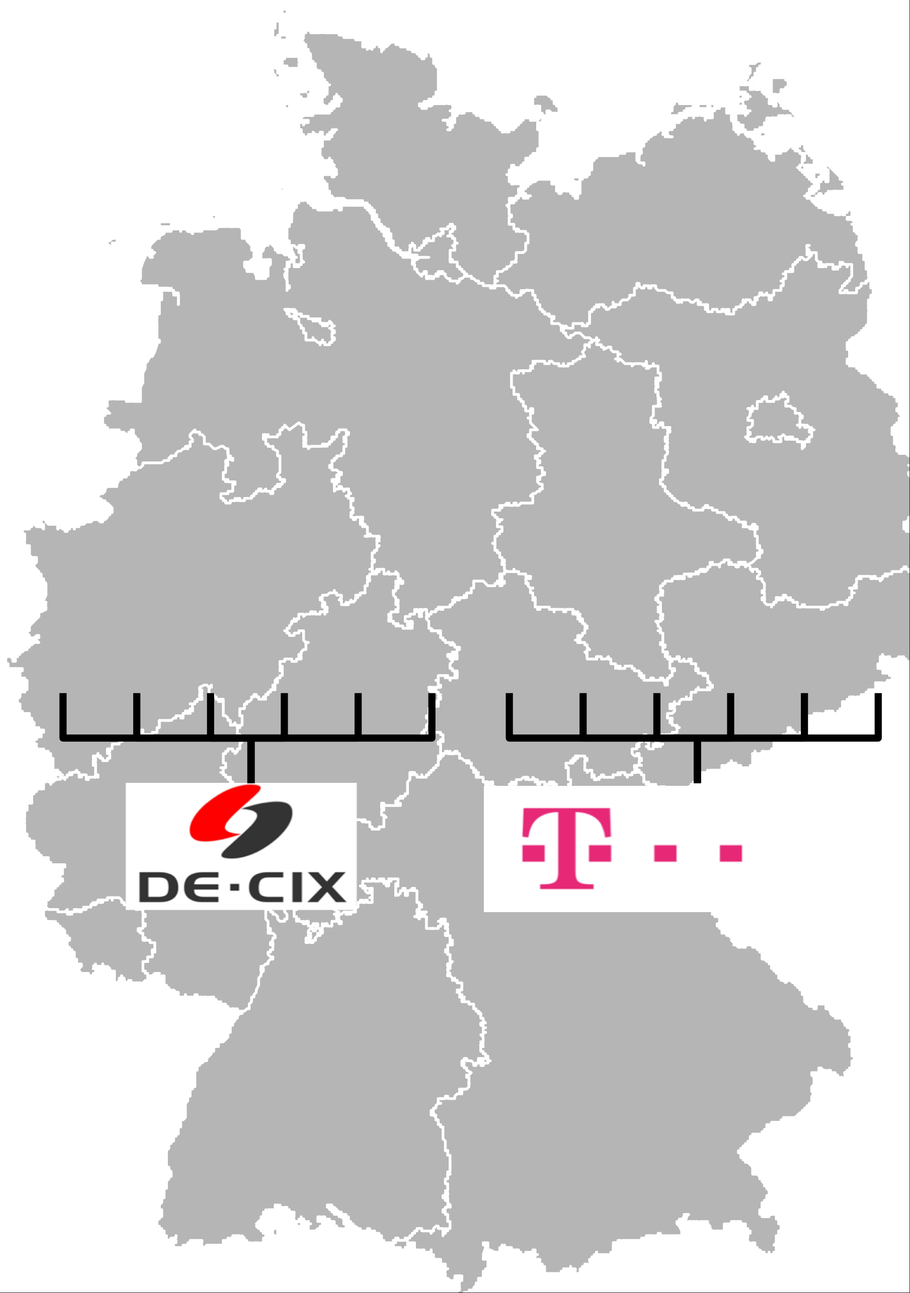

DE·CIX

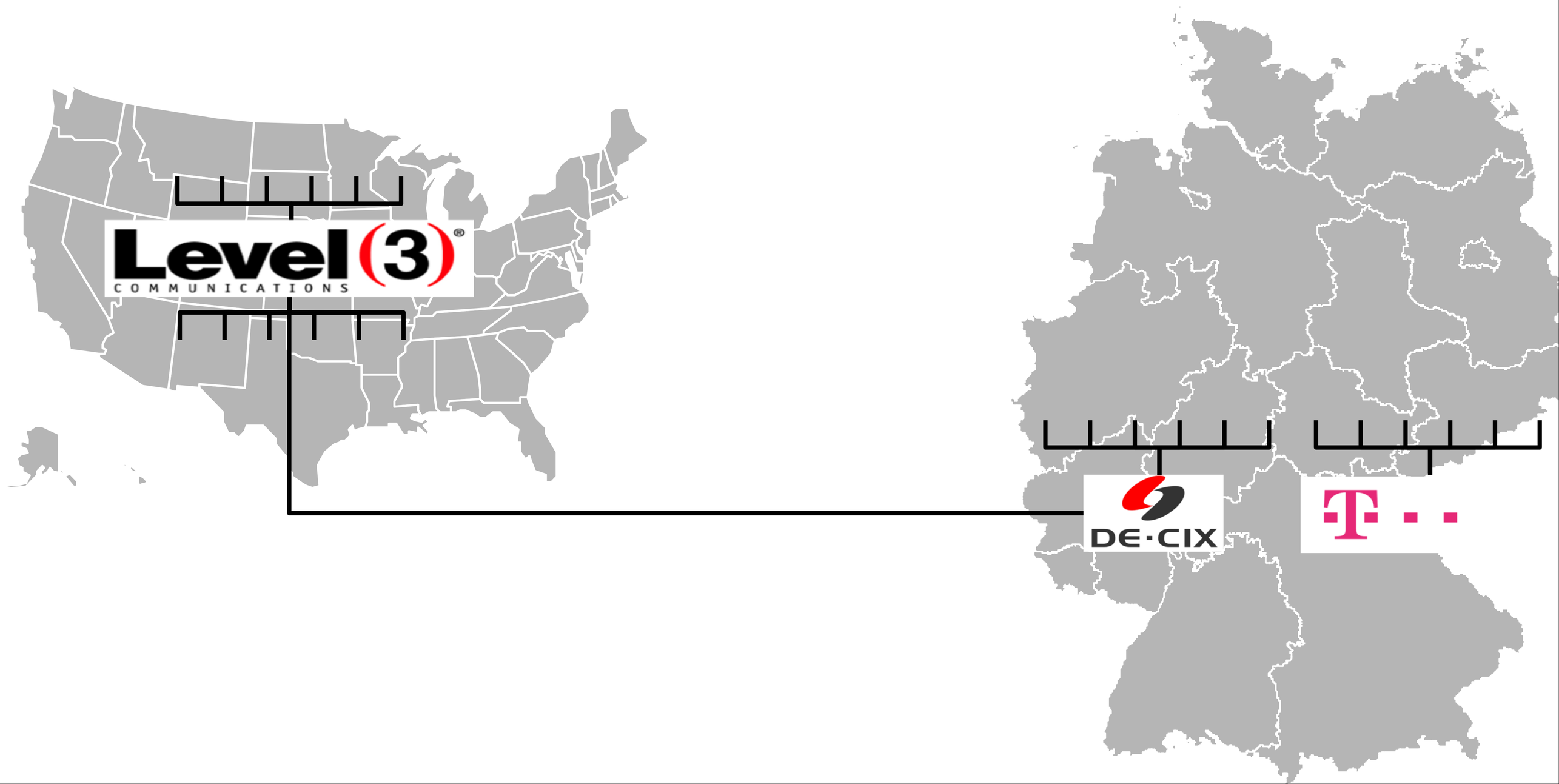

DE·CIX

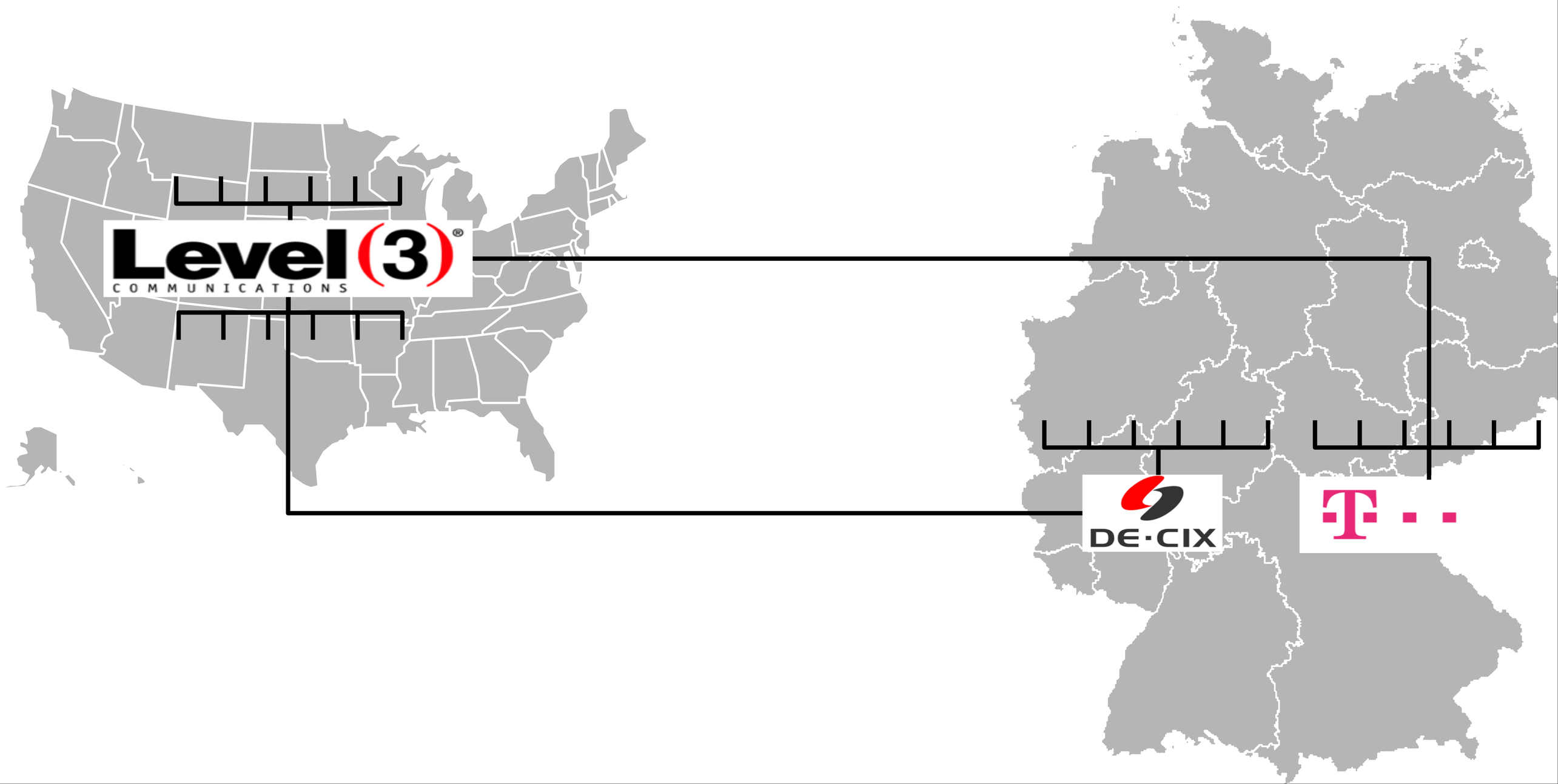
¥€$!

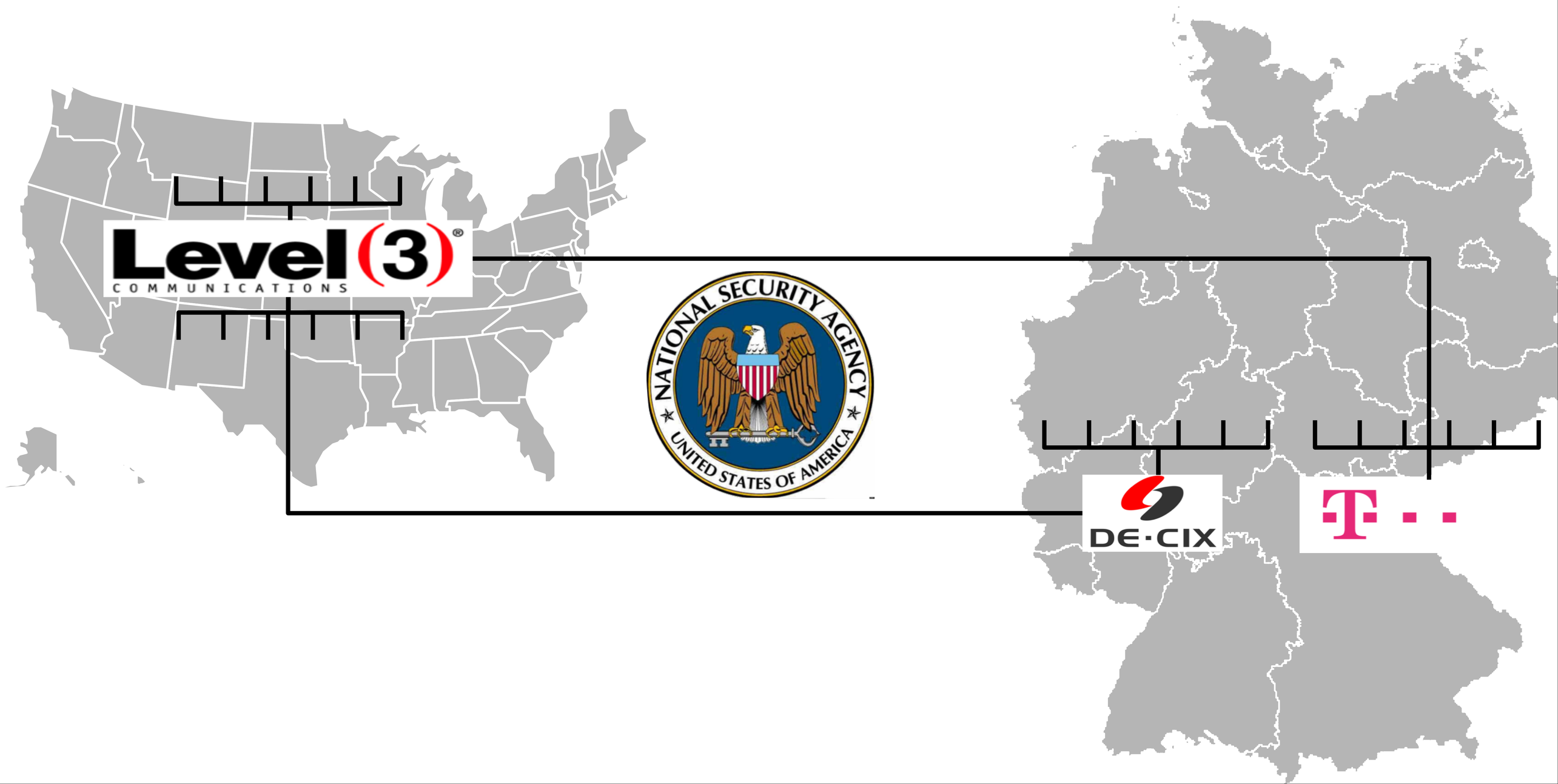

DE·CIX

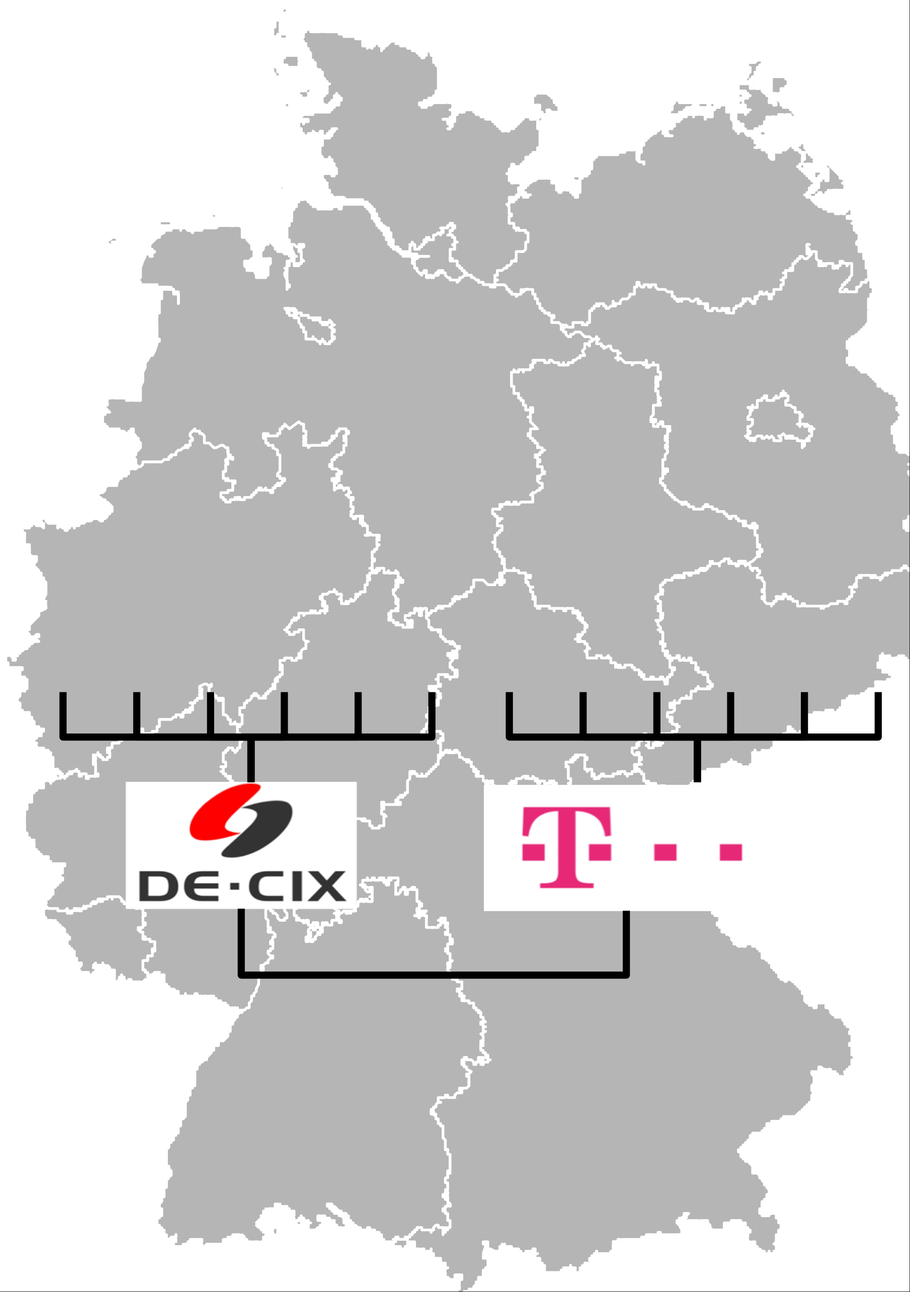

Level (3)
COMMUNICATIONS


DE-CIX
T

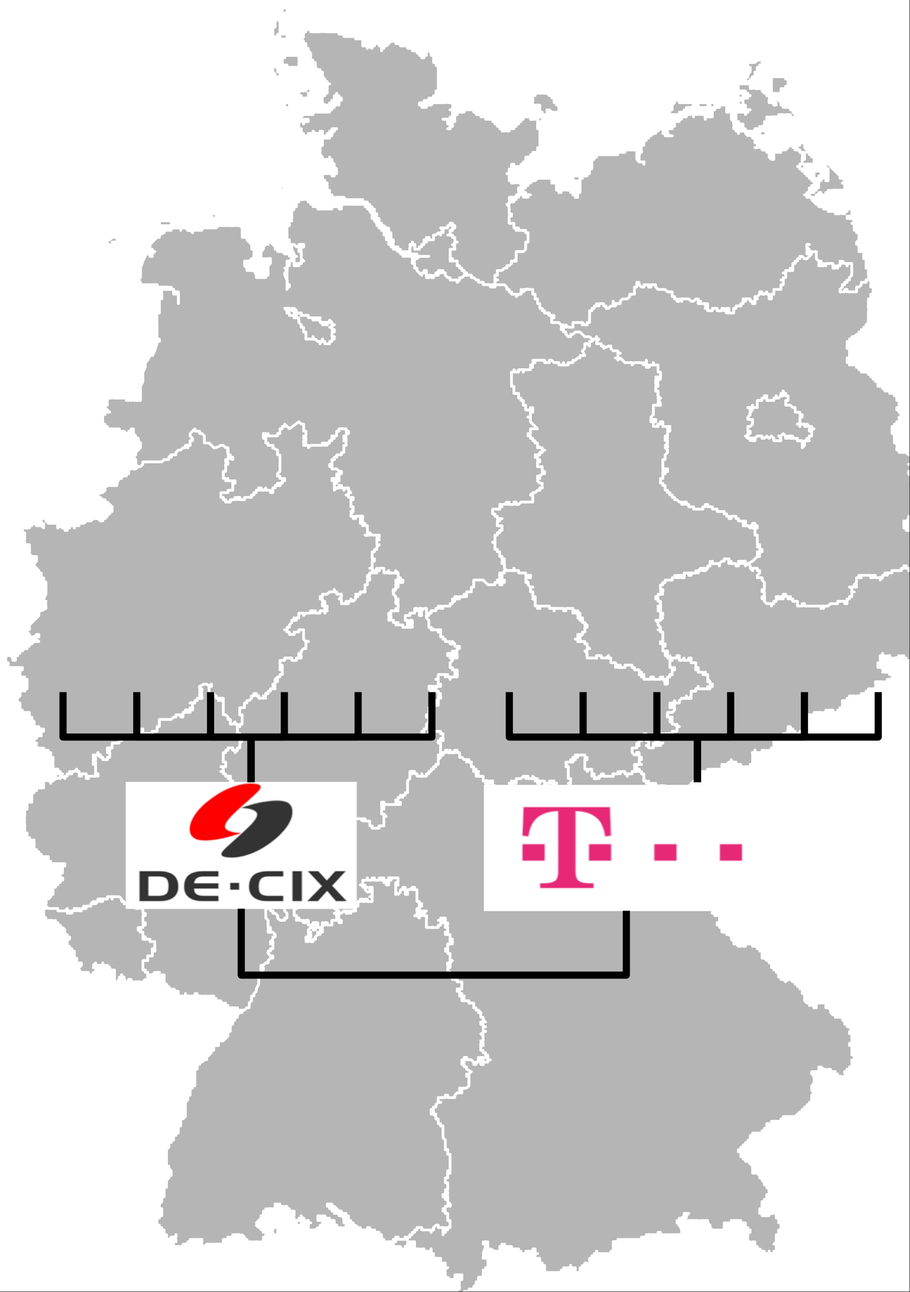

Level (3)
COMMUNICATIONS
DE·CIX
T

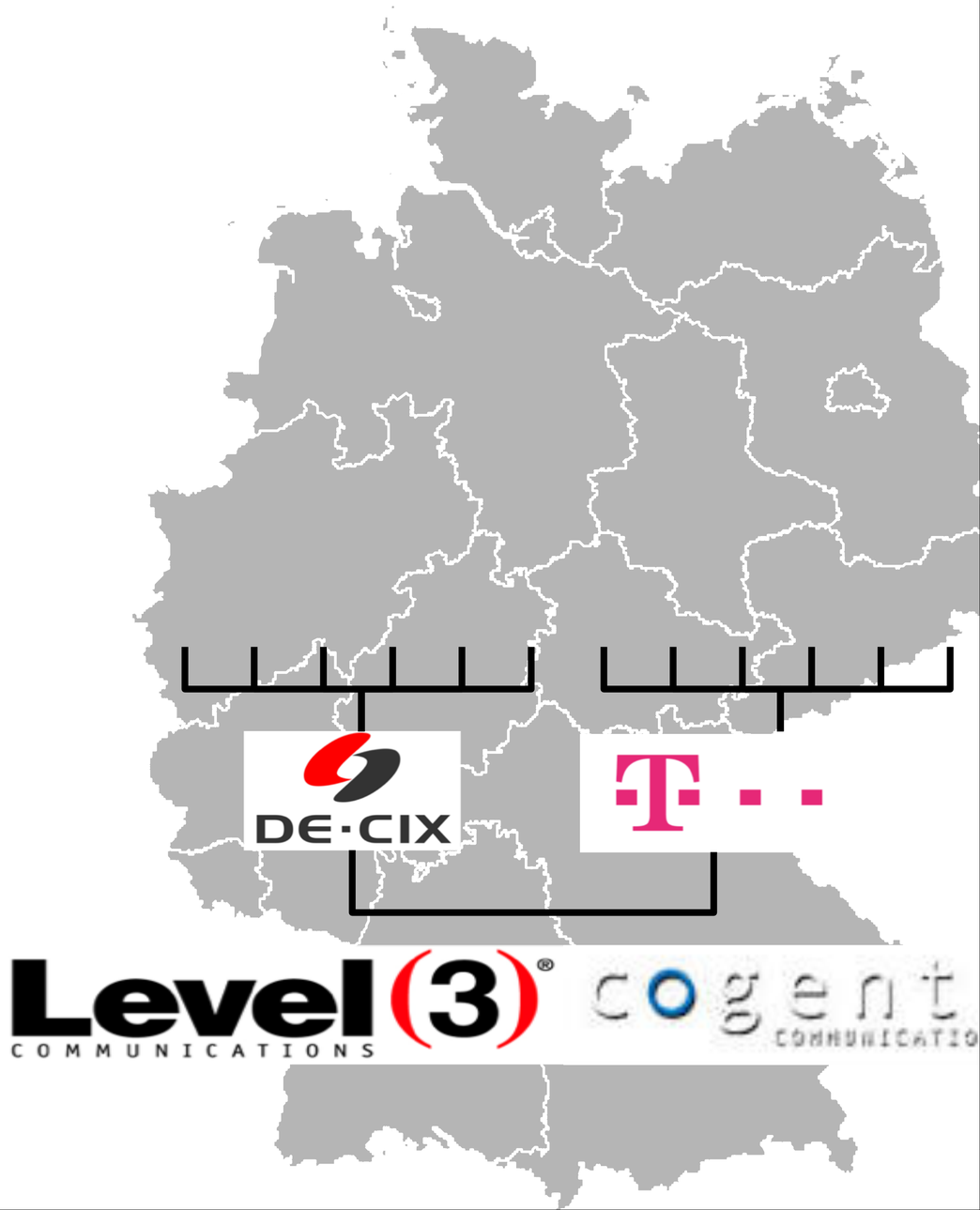

Level (3)
COMMUNICATIONS
DE·CIX
T


Level (3)
COMMUNICATIONS
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
DE-CIX
T


DE·CIX

¥€$!


DE·CIX


DE-CIX
Level(3)
COMMUNICATIONS
cogent

Bundesnachrichtendienst

Fazit: Schlandnet

- ➡ löst kein Problem, sondern zentralisiert es
- ➡ widerspricht physikalischen Gegebenheiten der „Leitungen“
- ➡ erhält erhöht Überwachungsmöglichkeiten für deutsche Dienste
- ➡ erhöht Marktmacht und Umsatz der deutschen Telekom
- ➡ bisherige Politik der deutschen Telekom ist Hauptgrund dafür, dass sich kein Schlandnet ergeben hat.

Agenda

- De-Mail
- Email made in Germany
- Schlandnet
- **Cloud**

Ihre Daten sind woanders,
und Sie wissen nicht, wo.
Davon halte ich prinzipiell nichts.

Frank Rieger

Series

Series: Cloud Computing

Media Center

Documents

Brochure: Security Services and Solutions

Further information

- European Identity Conference
- Interview with Prof. Dr. Eberhard von Faber and Dr. Michael Pauly, T-Systems

June 23, 2010

More growth, lower costs with security

UC meets business

- T-Systems connects doctors and patients at Asklepios Future Hospital.

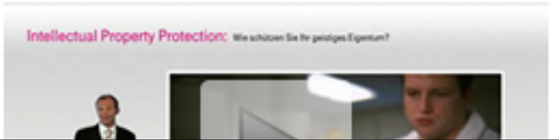
Faster than flying

- Veritas AG cuts travel costs with the UCC solution PLATON.

Productivity to go

- Using your smartphone for customer management saves money.

ICT is becoming more mobile and more flexible thanks to cloud computing. At the same time, security and data protection requirements are increasing. Those who do not have a suitable security plan in this area of conflicting interests are not only at risk of suffering a blow to their reputation should it come to the worst, but also of losing revenues on a scale that could ruin



Das Europaparlament fordert
mehr Datenschutz,
einheitliche Verbraucherschutzregeln und
einen einfachen Anbieterwechsel
bei der Nutzung von Cloud-Computing.

Sabine Verheyen, MdEP

Netzsicherheit	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz, etc.)	✓			✓		
Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway, etc.)		✓	✓	✓		
DDoS-Mitigation (Abwehr von DDoS-Angriffen)			✓	✓		
Geeignete Netzsegmentierung (Isolierung des Management-Netzs vom Datennetz)	✓			✓		
Sichere Konfiguration aller Komponenten der Cloud-Architektur	✓			✓		
Fernadministration durch einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN)	✓			✓		
Verschlüsselte Kommunikation zwischen Cloud Computing Anbieter und Cloud Computing Nutzer (z. B. TLS/SSL)	✓			✓		
Verschlüsselte Kommunikation zwischen Cloud Computing Standorten	✓			✓		
Verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind	✓			✓		
Redundante Vernetzung der Cloud-Rechenzentren			✓			✓


BearingPoint®

Feierabend.