KNF KONGRESS 2013

E-Mail im NSA-Zeitalter

JÖRG KINZEBACH

E MAIL

IM NSA-ZEITALTER

KONTROLLE

Kommunikation mit denen, die es angeht, nicht mit denen, die gerne mithören wollen

GLOBAL

Informationen werden überall erfasst und miteinander verknüpft

KONTAKTE

wer kommuniziert wann mit wem?

TOOLS

Kommunikation kann nicht vermieden werden, aber man kann den Teilnehmerkreis einschränken

NICHT AUFGEBEN

Es gibt immer etwas, das man tun kann, man muss nur damit anfangen

DIE STRATEGIE

ich kann nicht alles verhindern, aber manches vermeiden

lets's go have some privacy

TOOLS

Kommunikation kann nicht vermieden werden, aber man kann den Teilnehmerkreis einschränken

DIE STRATEGIE

ich kann nicht alles verhindern, aber manches vermeiden

KONTROLLE

Kommunikation mit denen, die es angeht, nicht mit denen, die gerne mithören wollen

KONTAKTE

wer kommuniziert wann wem?

Hit View
to view

BAL

nen werden überall
d miteinander verknüpft

EDWARD SNOWDEN

privacy

KEINE SORGE

ich habe nichts zu verbergen
und nichts zu befürchten

ICH HABE NICHTS ZU VERBERGEN

oder etwa doch?

MITHÖRER WIRKLICH OKAY

Ist es wirklich okkay, dass es Stellen gibt, die auf die eigene Kommunikation Zugriff haben, auch in die Vergangenheit gerichtet?

BEKANNTE

Auch wer denkt kein Ziel von Überwachung sein zu könen, hat eventuell lose Kontakte zu Zielen, die Interesse auslösen.

VERDACHTSMOMENTE

Auch einzeln betrachtet harmlose Fakten können durch eine Verknüpfung ein Interesse an der Person erwecken.

FALSCHE VERKNÜPFUNG

Die wenig spezifische Suche in großen Datenmengen kann auch irrtümliche Ergebnisse und Verdachtsmomente liefern.

ES KANN JEDEN **TREFFEN**

ohne Vorwarnung

VERKNÜPFUNG VON INFORMATIONEN

Verdachtsmomente entstehen auch durch unvollständige Daten.

AUSWIRKUNG UNVERHERSEHBAR

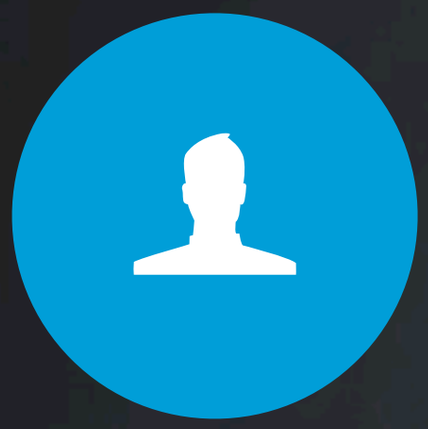
Die Sammlung von Daten würde nicht erfolgen, würde man diese nicht auswerten wollen und Aktionen einleiten.

3 BEZIEHUNGSGRADE

in der „Nähe“ von Zielobjekten

Die NSA darf offiziell in der Privatsphäre in 3 Stufen Entfernung von Terror-Verdächtigen herumschnüffeln. Exemplarisch dargestellt mit f-Freundschaften:

ERSTER GRAD



Freunde

50 Personen

ZWEITER GRAD

Freunde von Freunden

8.170 Personen

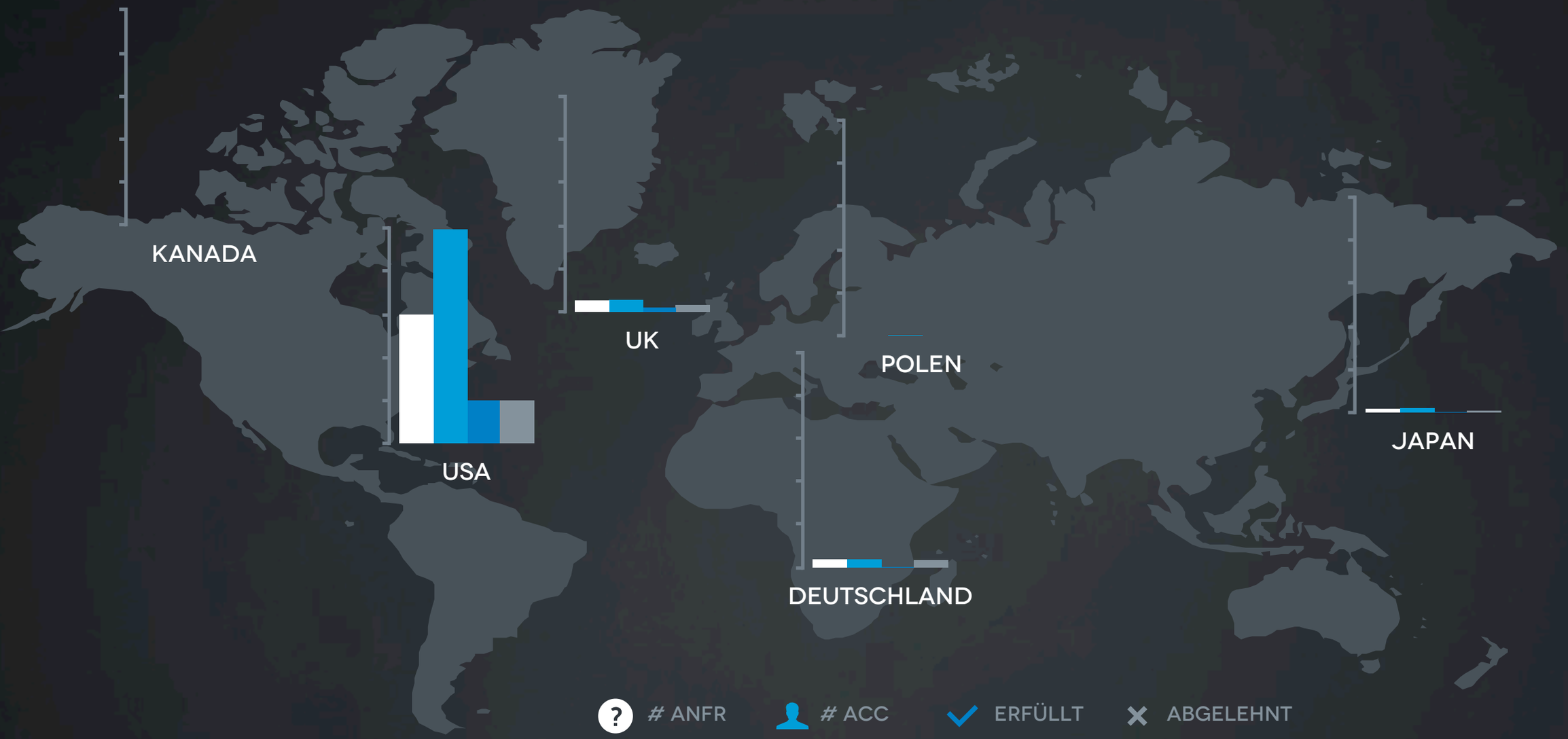
DRITTER GRAD

Freunde von Freunden von Freunden

1.334.978 Personen

BEHÖRDEN ANFRAGEN

Zahlen von Apple



KNF KONGRESS 2013

E-Mail im NSA-Zeitalter

SICHERHEIT

der Privatsphäre

SICHERHEITS ZIELE

bei E-Mail Kommunikation

KOMMUNIKATION OHNE MITHÖRER

Der Inhalt eines Nachrichtenaustauschs soll nicht von dritten belauscht werden können.

KEINE KENNTNIS DER KOMMUNIKATION

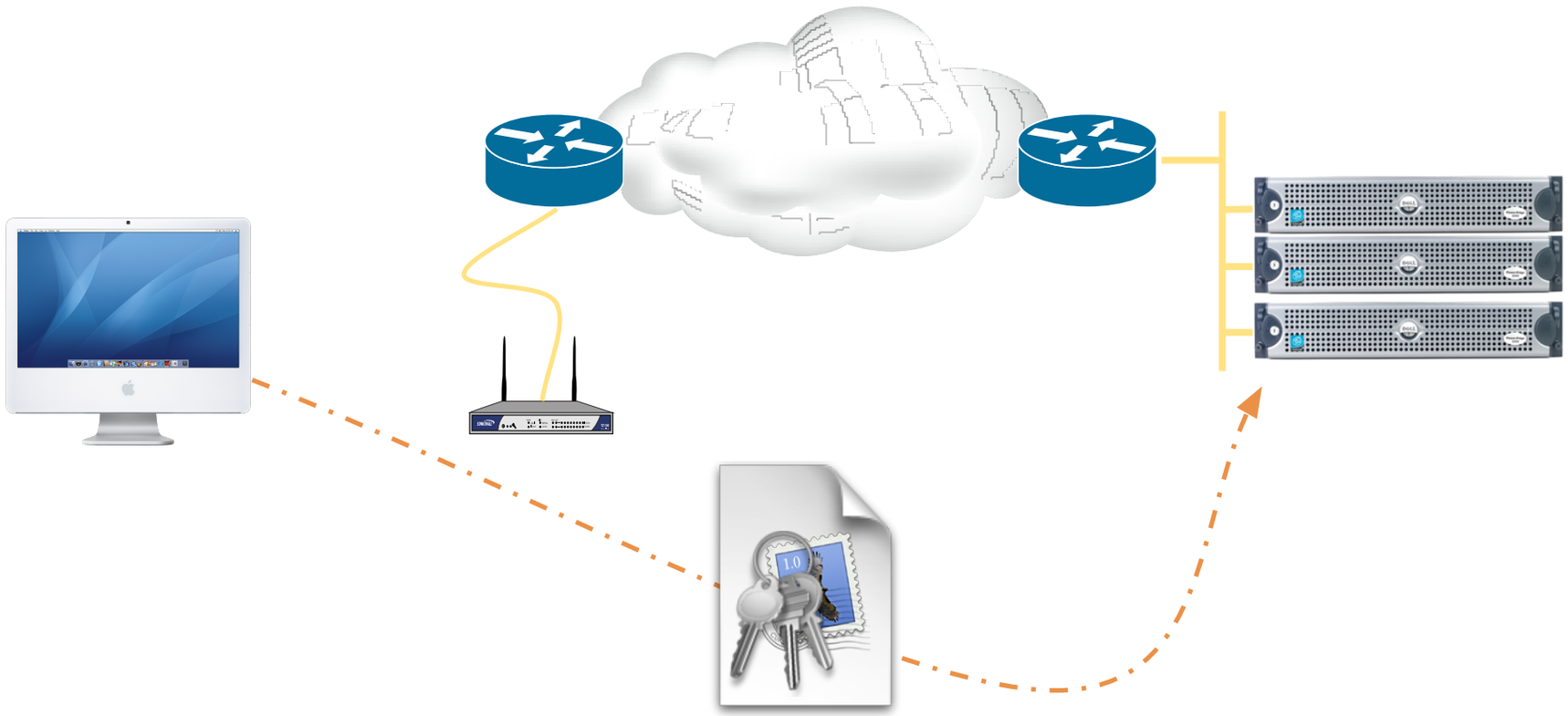
Auch ohne Kenntnis des Inhalts werden Rückschlüsse aus dem Verhalten gezogen.

KOMMUNIKATION MIT DEM RICHTIGEN

Sicherheit, dass der Gesprächsparter auch der richtige ist.

TRANSPORT SICHERHEIT

SSL/TLS für Serververbindungen



VERBINDUNG

Für die Übertragung von Login und Passwort unter allen Umständen sinnvoll, auch wenn dies Behörden eher wenig in der Überwachung einschränkt.

VERSCHLÜSSELUNGS TYPEN

Grundlagen der Verschlüsselung

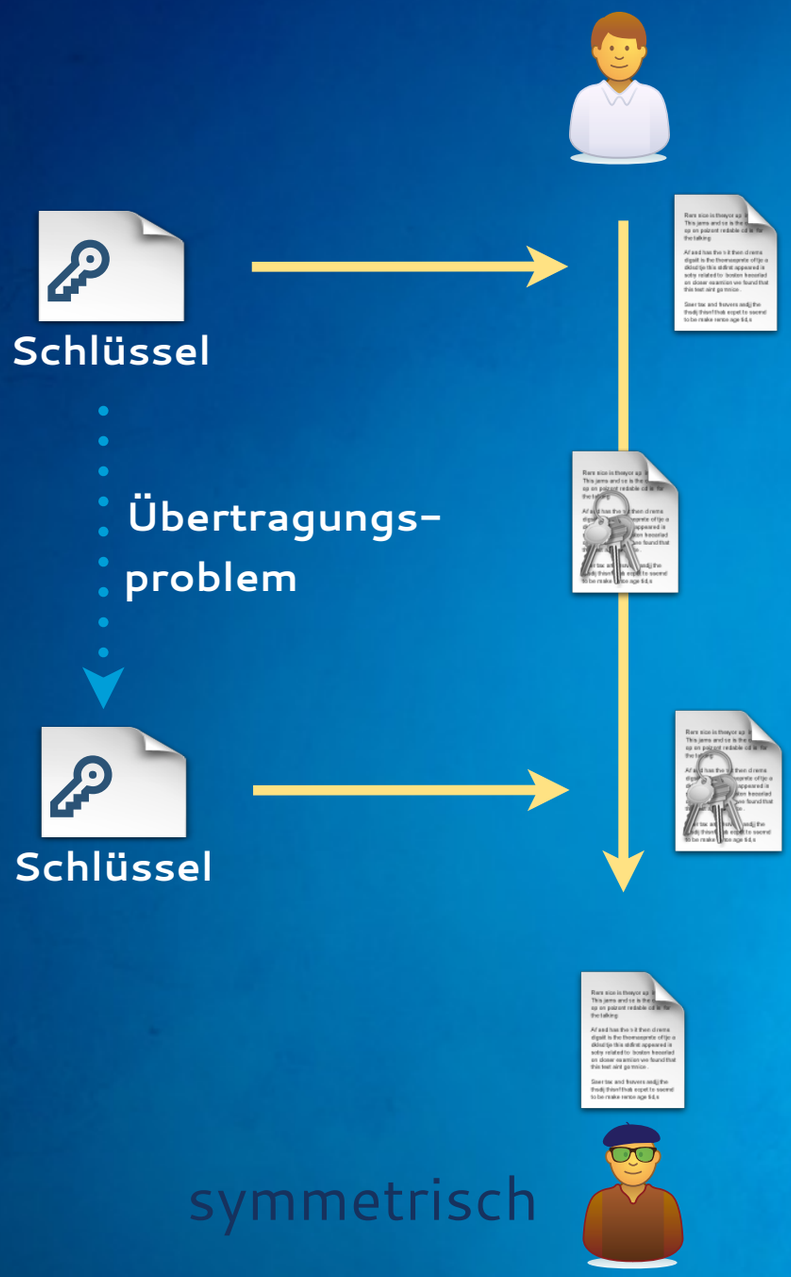
SYMMETRISCH

Zwei miteinander verschlüsselt kommunizierende Parteien haben beide den Schlüssel zum Ver- und Entschlüsseln.

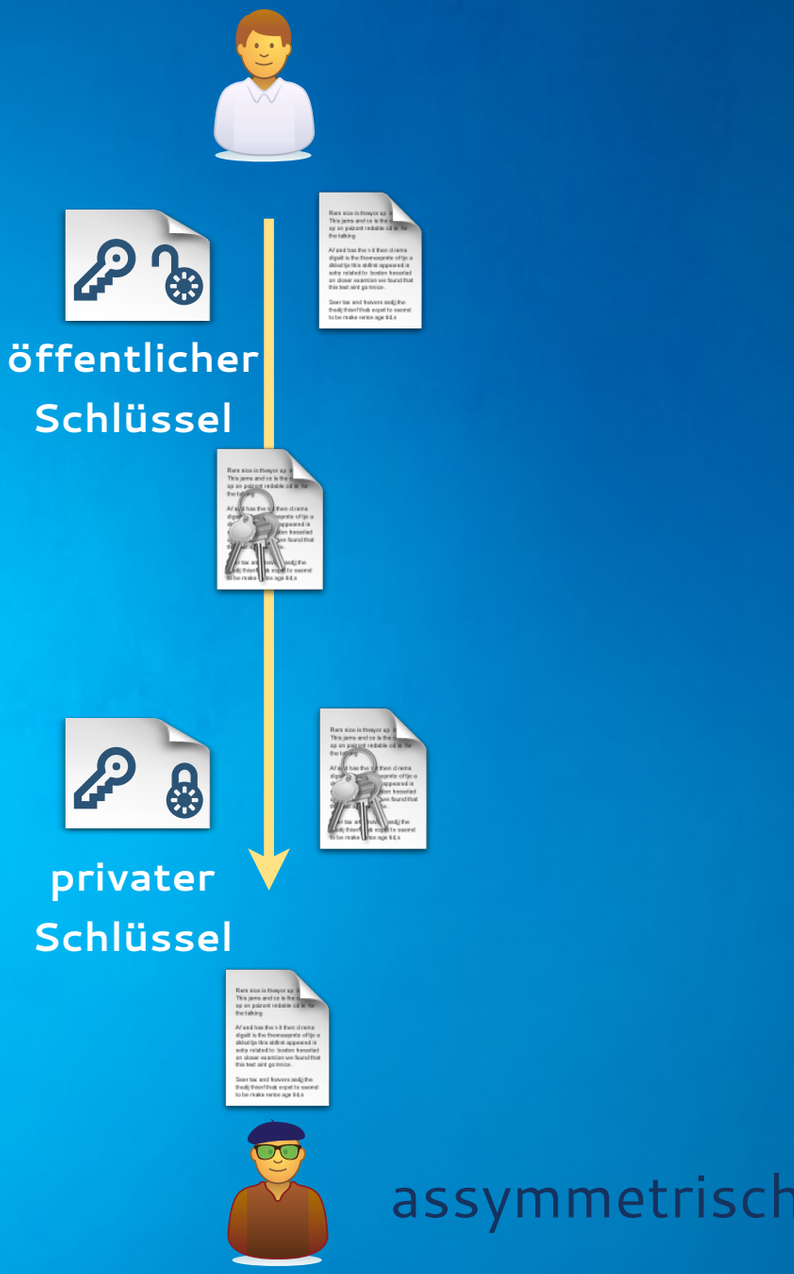
ASSYMETRISCH

Der Sender einer verschlüsselten Nachricht hat einen öffentlichen Schlüssel des Empfängers, welcher Nachrichten mit seinem privaten Schlüssel dechiffriert.

VERSCHLÜSSELUNGS TYPEN



symmetrisch



assymetrisch

III

DIE ANSÄTZE

Wie kann die totale Überwachung zumindest eingeschränkt werden

SICHERE PROVIDER IN .DE

die Schnapsidee

SICHER ZWISCHEN PROVIDER IN .DE

Keine Datenübertragung über ausländische Netze für deutsche Nutzer

TLS ZWISCHEN PROVIDERN

Warum erst jetzt?

WAS IST MIT MAILS AN ANDERE?

Wo ist ein GMail oder Yahoo-Account?

VOLLES VERTRAUEN IN PROVIDER?

GMX, Web.DE, 1&1, Telekom sind vertrauenswürdig?

SICHERHEIT MIT DE-MAIL

gesetzlich verankerte Sicherheit

VERIFIZIERTER ABSENDER

Keine Mails von nicht eindeutig identifizierten Parteien.

VERSCHLÜSSELTE ÜBERTRAGUNG

Einlieferung, Weitertransport und Speicherung erfolgt verschlüsselt.

RECHTSVERBINDLICH

Eine De-Mail muss von Behörden akzeptiert werden, obwohl sie nicht den Anforderungen der Schriftform genügt.

SICHERHEIT DE-MAIL

gesetzlich verankert

Die Sicherheit von DE-MAIL konzentriert sich eher auf die Absicherung des Mailempfängers als auf die Absicherung der Kommunikation.

TRANSPORT

Mails werden i.d.R. mit SSL/TLS verschlüsselt eingeliefert und auch weitertransportiert.

SCANNING

Jede Mail wird beim Provider entschlüsselt und auf z.B. Viren untersucht.

END-TO-END

Mails werden potentiell mehrfach in Klartext zurückverwandelt und analysiert.

EINSEHBAR

Login und Passwort sind ohne Richterliche Anordnung an Strafverfolgungsbehörden auszuliefern.

TLS PROBLEME

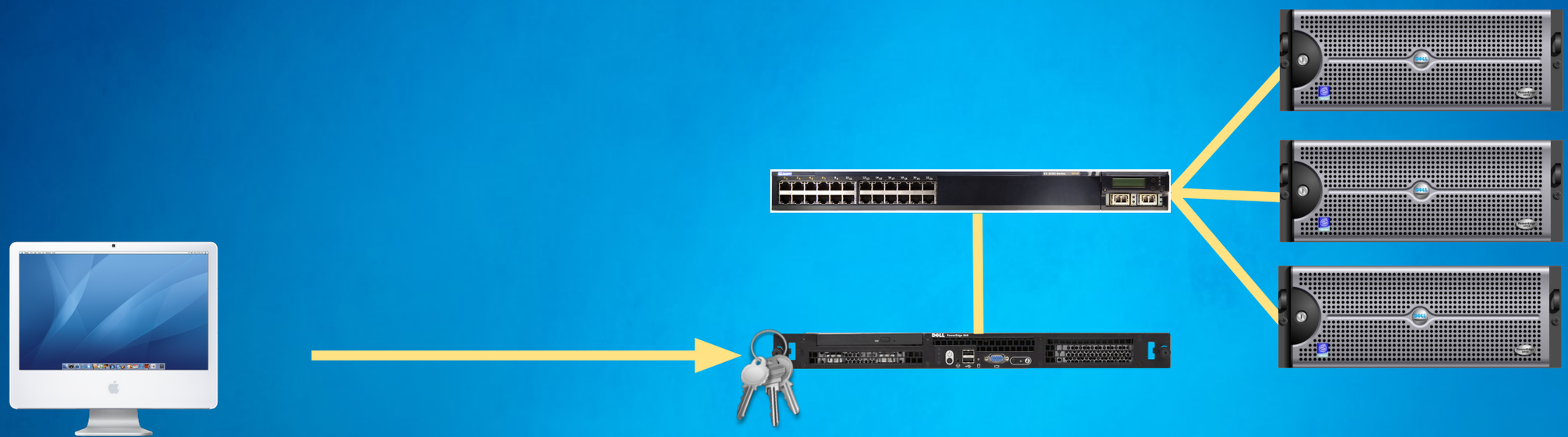
SSL/TLS ist prinzipiell als sicher anzusehen, aber...

TLS PROBLEM #1

Wo ist die Verschlüsselung

TLS PROBLEM #1

Wo ist die Verschlüsselung



TLS PROBLEM #2

Zertifikate

Client

Server

TLS PROBLEM #2

Zertifikate

?

Server

Client

Server

TLS PROBLEM #2

Zertifikate

?

Signer

Server

Client

Server

TLS PROBLEM #2

Zertifikate

CA

in CA-Liste

Signer

Server

Client

Server

TLS PROBLEM #2

Zertifikate

CA

in CA-Liste

CA2

Signer

Signer2

Server

Server

Client

Intercept

Server

LEHRE **ZIEHEN**

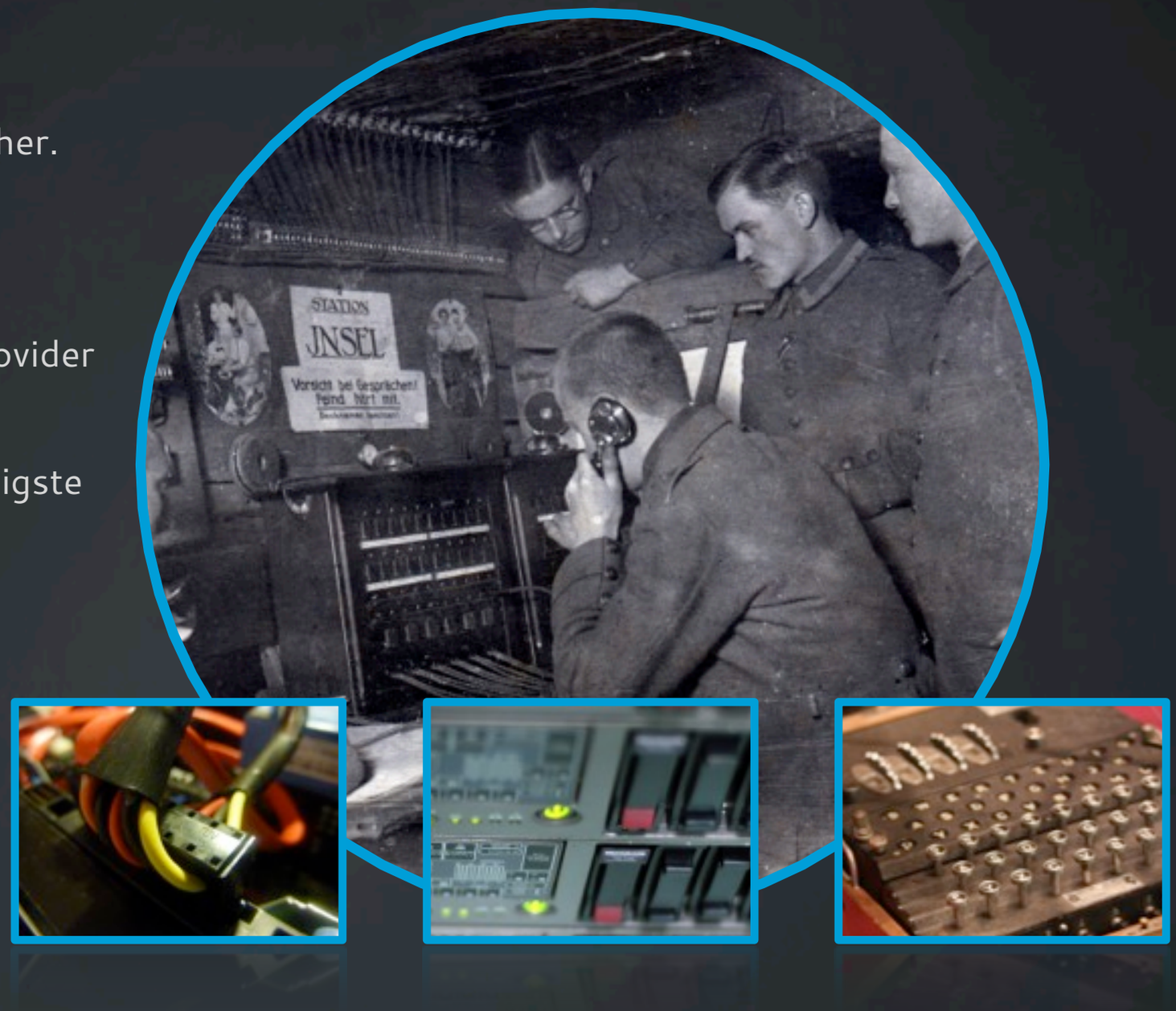
end-to-end Verschlüsselung

ABHÖRSICHER: vermeintlich private Kommunikationskanäle sind nicht sicher.

VERSCHLÜSSELUNG: muss selbst kontrolliert werden.

SPEICHERUNG: Klartextkopie bei Provider immer Abhörbar.

PROVIDER: auch der vertrauenswürdigste Provider muss sich dem Gesetzgeber unterwerfen.



KNF KONGRESS 2013

E-Mail im NSA-Zeitalter

ADOBE SECURE DOCUMENTS

signierte und verschlüsselte PDF Dokumente

ERZEUGUNG

Jede E-Mail wird zu einem PDF-File, das als „Anhang“ verschickt wird.

SIGNIERUNG

Dokumente können mit X.509 Keys signiert werden.

SOFTWARE

Adobe Acrobat...

S/MIME X.509

built-in encryption technology

ABSENDER/CERT

Mails können signiert werden um den Absender zu bestätigen.

PUBLIC KEYS

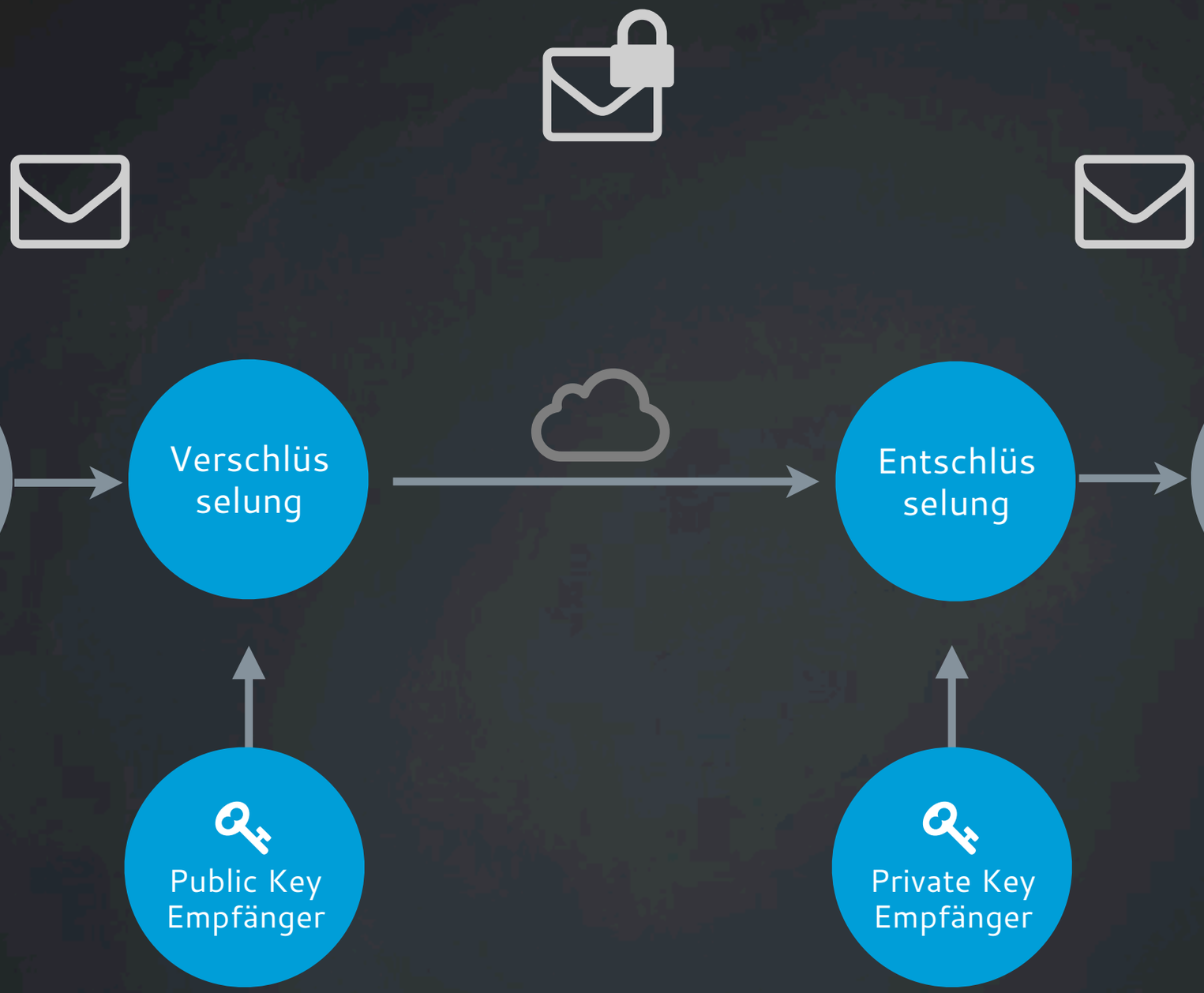
Schlüssel von Empfänger und/oder Sender kann veröffentlicht werden aber trotzdem ist die Kommunikation abhörsicher.

EINGEBAUT

Gängige Mail-Software unterstützt X.509 Keys basierende Signierung und Verschlüsselung ohne Addons.

PUBLIC KEY **ENCRYPTION**

secure transmission/storage



S/MIME X.509

die Technologie

- X.509 ist ein ITU-Standard für Public Key Infrastruktur (PKI) und Rechte-Management.
- S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein Standard für Verschlüsselung und Signatur von E-Mails.
- X.509 nutzt eine hierarchische Signaturkette zur Verfikation der Identität (Baum-Struktur).
- X.509 unterstützt Widerruf eines Zertifikats mittels Blackliste.
- X.509 wird u.a. auch für HTTPS und verschlüsseltes POP3/IMAP verwendet (SSL/TLS).
- S/MIME kann theoretisch auch mit „PGP" verwendet werden.

S/MIME X.509

Probleme

HIERARCHISCHE STRUKTUR

In Unternehmen sicherlich eine passende Vertrauensstruktur, für private Kommunikation eher ungeeignet.

INFRASTRUKTUR

Software und kommerzielle Signierungsstellen ausreichend vorhanden, aber keine Infrakstruktur zum Schlüsselaustausch.

KOMPLEXITÄT

Die Erstellung eines privaten Schlüssels ist nicht trivial, die Signierung noch wesentlich problematischer.

KOMMERZIELL

Kommerzielle Signierung für Privatanwender zu teuer, kostenlose Angebote dieser Anbieter bieten keine akzeptable Sicherheit.

PRETTY GOOD **PRIVACY**

PGP

PHIL ZIMMERMANN, 1991

OpenPGP Standard (RFC 4880) zum ver- und entschlüsseln von Daten mit-Public und Private-Key.

INKOMPATIBILITÄT

Im Zuge der Weiterentwicklung sind neue Algorithmen entstanden, die von älterer Software nicht verstanden werde.

SIGNATUR

Die Methoden zur Identitätsverifizierung können verwenden werden um Nachrichten zu signieren und überprüfen.

PGP VERSCHLÜSSELUNG

verschlüsseln (Sender)

öffentlicher Schlüssel des Empfängers

erzeuge Zufallsschlüssel

RSA Verschlüsselung mit öffentlichem Schlüssel

Nachricht

Symmetrische Verschüsselung mit Zufallsschlüssel

kombiniere

verschlüsselte Nachricht

PGP VERSCHLÜSSELUNG

entschlüsseln (Empfänger)

verschlüsselter Zufallsschlüssel

RSA Entschlüsselung mit privatem Schlüssel

verschlüsselte Nachricht

symmetrische Entschlüsselung

Nachricht

WEB OF TRUST

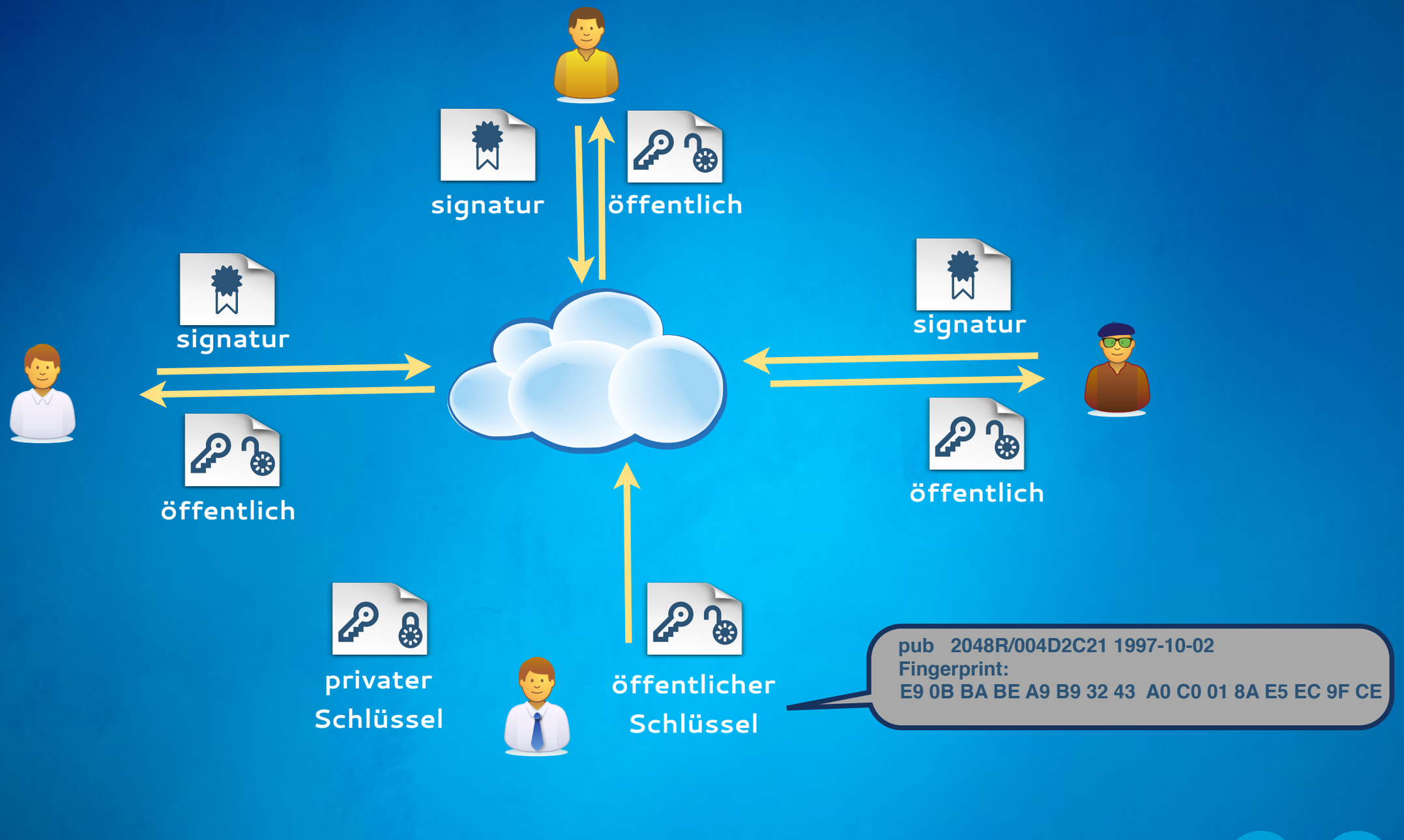
VERTRAUEN IN SCHLÜSSEL-BESITZ

Gehört ein Schlüssel der Person, von der man den Schlüsselbesitz annimmt.

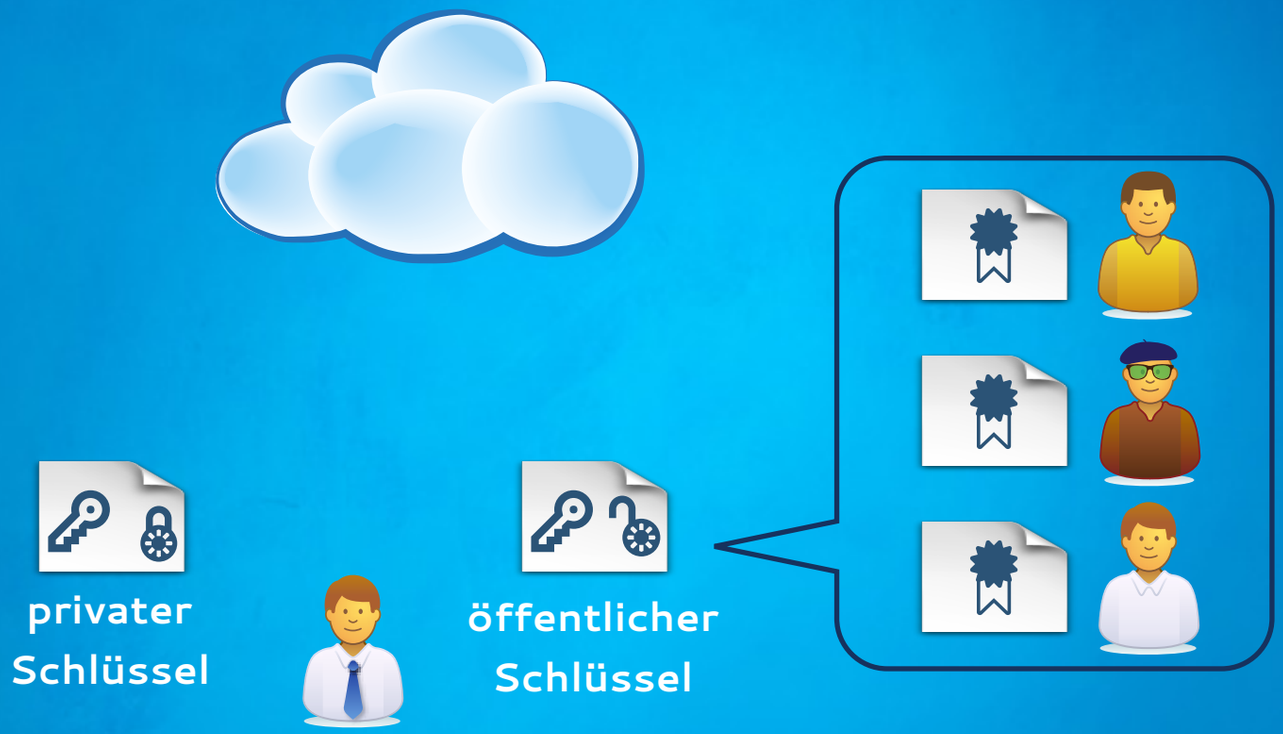
VERTRAUEN IN SCHLÜSSEL-NUTZER

Vertrauen in den Besitzer eines Schlüssels mit Schlüsselsignaturen sorgfältig umzugehen.

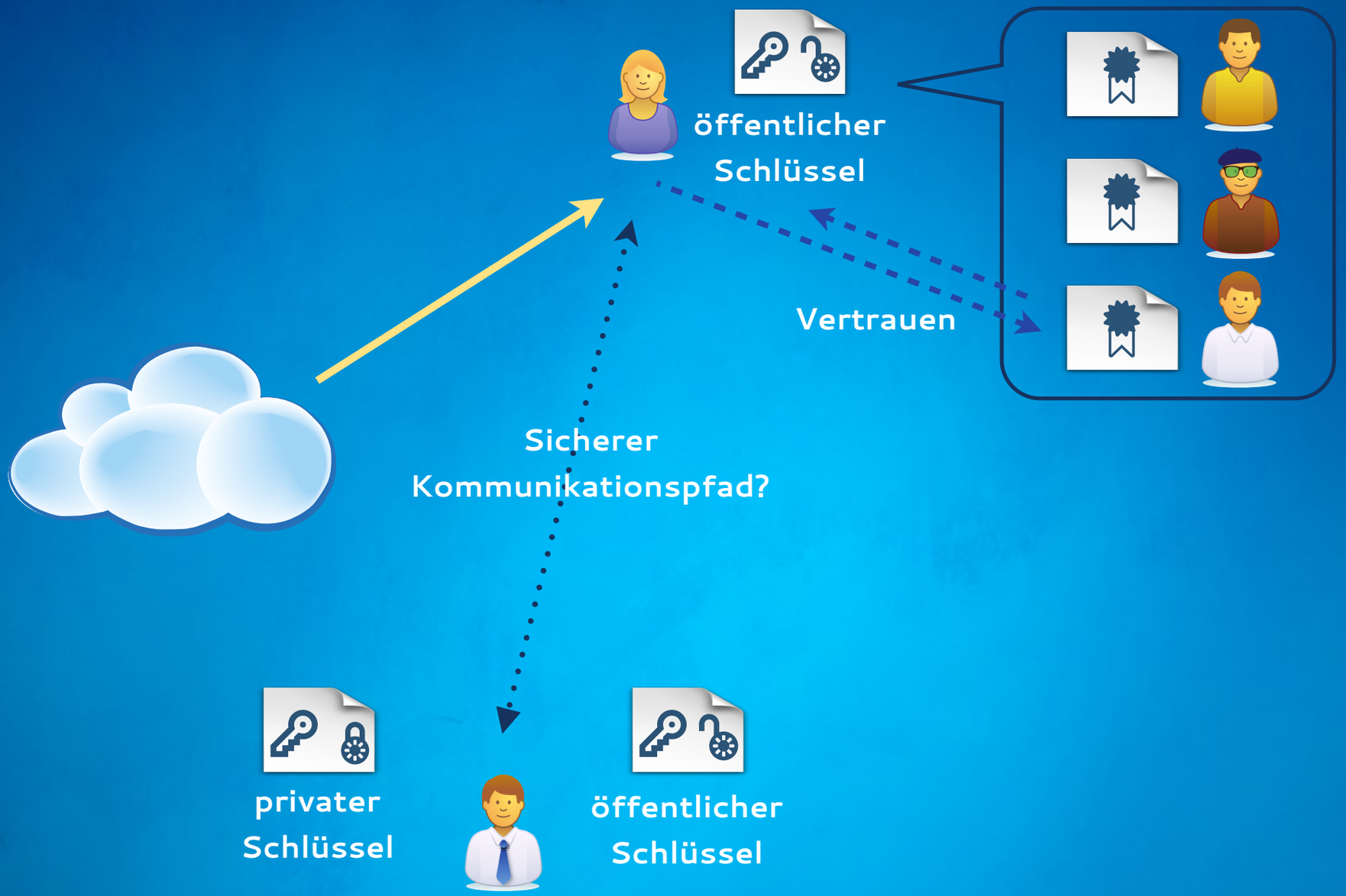
WEB OF TRUST


signatur
öffentlich
signatur
öffentlich
signatur
öffentlich
privater Schlüssel
öffentlicher Schlüssel
pub 2048R/004D2C21 1997-10-02
Fingerprint:
E9 0B BA BE A9 B9 32 43 A0 C0 01 8A E5 EC 9F CE

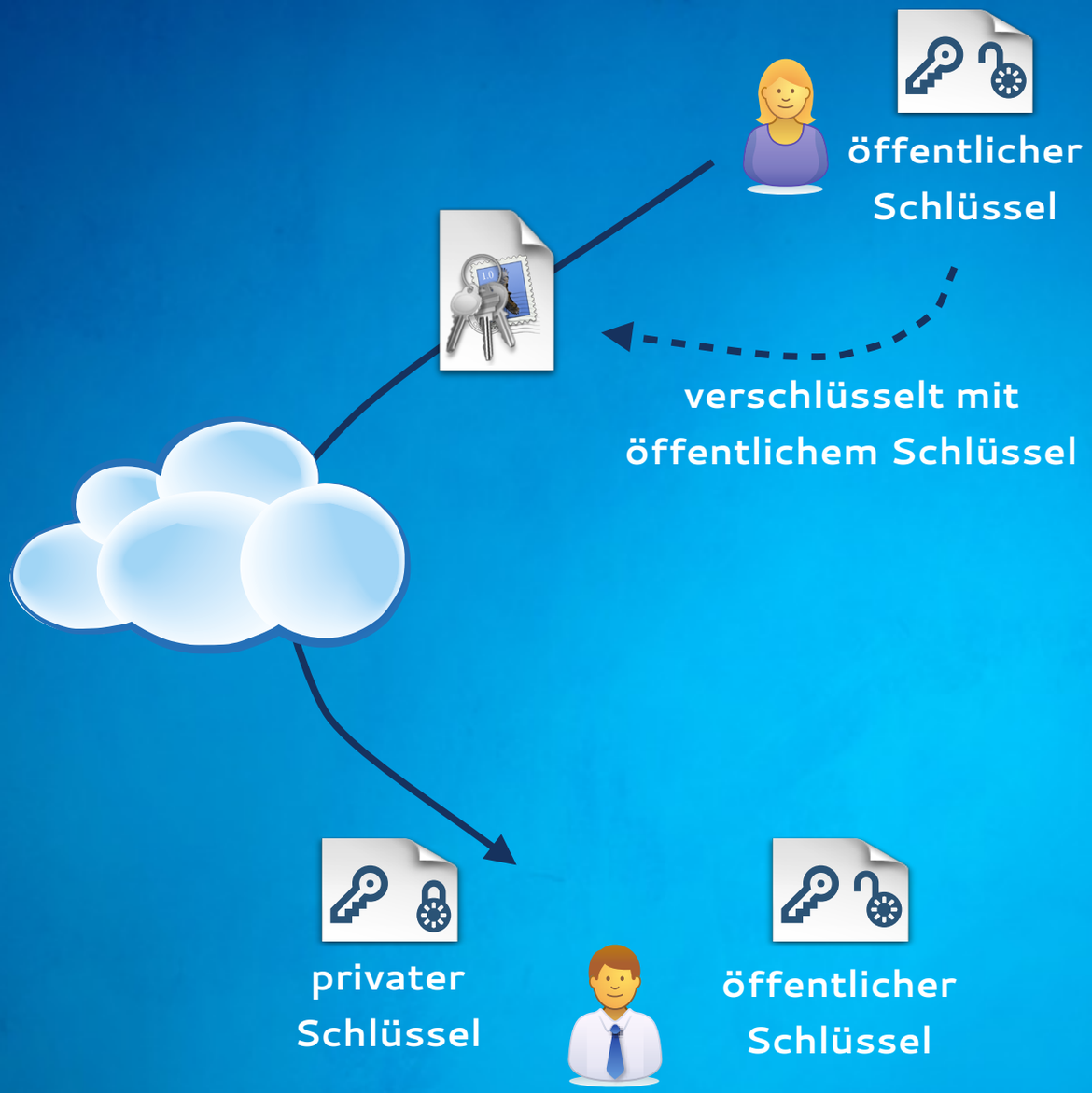
WEB OF TRUST



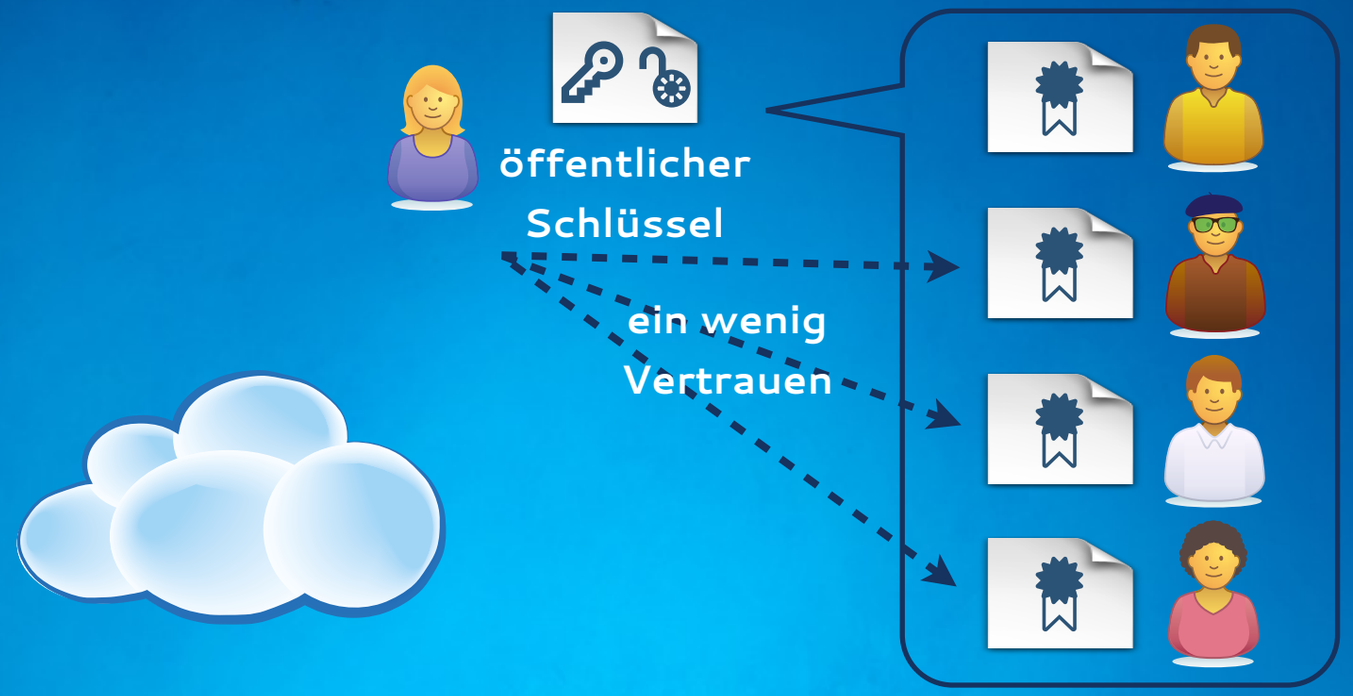
WEB OF TRUST


öffentlicher
Schlüssel
Vertrauen
Sicherer
Kommunikationspfad?
privater
Schlüssel
öffentlicher
Schlüssel

WEB OF TRUST


öffentlicher Schlüssel
verschlüsselt mit öffentlichem Schlüssel
privater Schlüssel
öffentlicher Schlüssel

WEB OF TRUST


öffentlicher
Schlüssel
ein wenig
Vertrauen


privater
Schlüssel
öffentlicher
Schlüssel

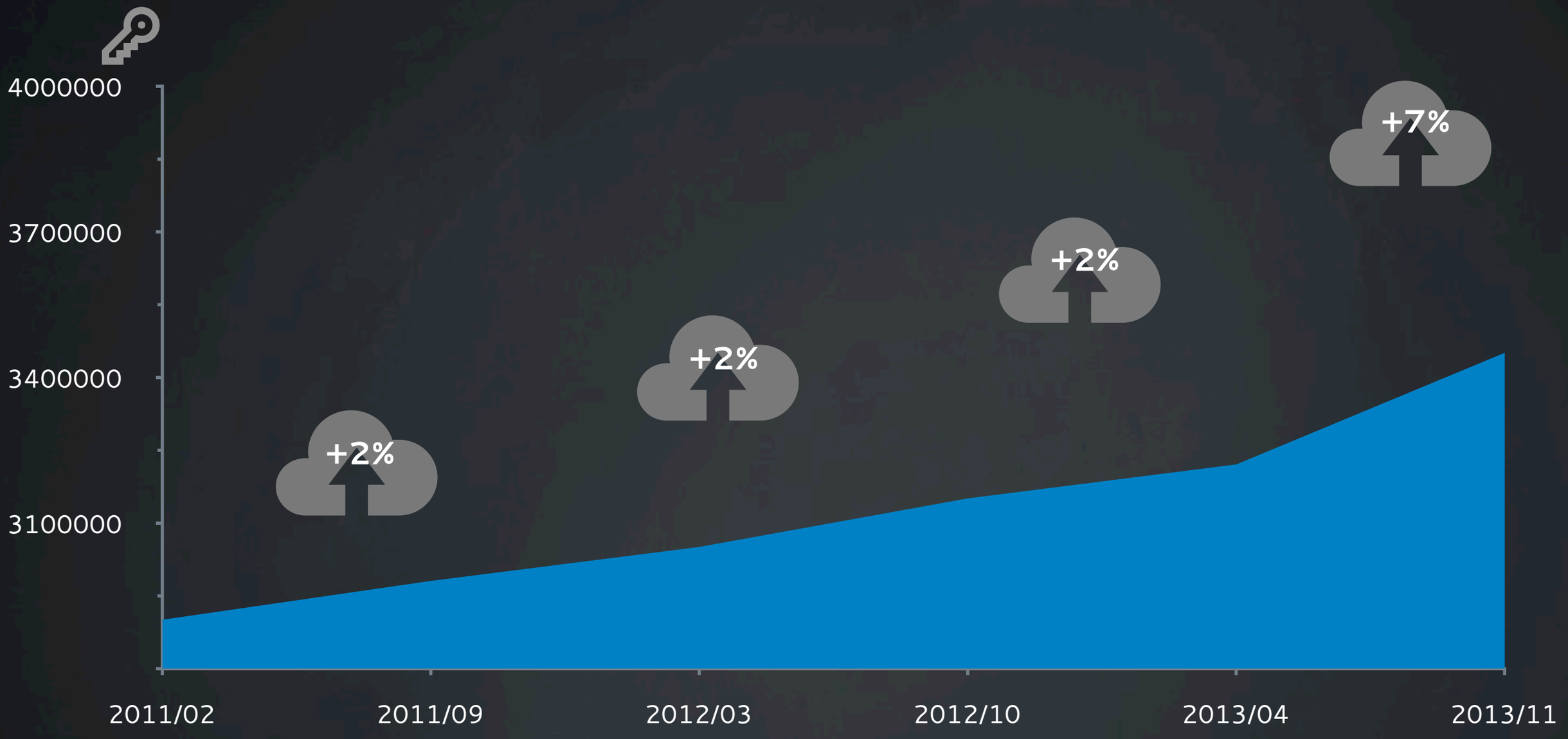
PGP VERSCHLÜSSELUNG

Vor- und Nachteile

- Einfache Verbreitung von Schlüsseln (Keyserver)
- Keine zentrale Stelle zur Signierung von Schlüsseln
    - gut für private Anwendung
    - kann in Firmen zu Problemen führen
- Verschlüsselung gilt als „military grade“
- Erfordert Zusatzprogramme
- Viele Implementierungen sind „Open Source“ und gut untersucht

PGP SCHLÜSSEL

Anzahl Schlüssel auf Keyserver



IV

FAZIT ANPACKEN

FAZIT WAS IST ZU TUN?

Sicherheit erfordert Kenntnisse über die Technologie, Scheinsicherheit hilft niemals dem Anwender.

Je vebreiteter die Anwendung, desto besser dokumentiert und umkomplizierter wird die Verschlüsselung und der Schlüsselaustausch.

Ohne grundlegende Sicherheit des benutzten Sender- und Absender-Systems nützt die Verschlüsselung der E-Mail nicht viel.

VIELEN DANK

für die Aufmerksamkeit

nach kurzer Pause der nächste Vortrag...

KNF KONGRESS 2013

E-Mail im NSA-Zeitalter

Bildverzeichnis

Bildverzeichnis, Creative Commons Lizenzen

Scott Ableman (CC BY-NC-ND 2.0) getting searched at airport security
Schub@ (CC BY-NC-SA 2.0) Postbox
Christian Pop (CC BY-NC-SA 2.0) Schnaps
Francesco Adorisio (CC BY-NC-ND 2.0) old mailboxes
Nate Bolt (CC BY-SA 2.0) (afe with pirate symbols
Tom Ellefsen (CC BY-NC-SA 2.0) locked store
Steven Tom (CC BY-ND 2.0) locks
Sugree Phatanapherom (CC BY-SA 2.0) network switch with cables
UK Ministry of Defence (CC BY-SA 2.0) GCHQ building
Drake Goodman (CC BY-NC-SA 2.0) Feind hört mit
Sandia Labs (CC BY-SA 2.0) blue dell servers
Thomas Hawk (CC BY-NC 2.0) Adobe
Sean MacEntee (CC BY 2.0) cables
Bryn Salisbury (CC BY-NC-SA 2.0) enigma
JD Hancock (CC BY 2.0) hard at work
Jan H. - applejan (CC BY-NC-SA 2.0) reading
Neptune Canada (CC BY-NC-SA 2.0) beehive canada
Victor Bayon (CC BY-NC-SA 2.0) insecure laptop
Carl Guderian (CC BY-NC-SA 2.0) 4677 C-446 A
Patricia Espedal (CC BY 2.0) spiderweb
Duncan Hull (CC BY-SA 2.0) questions