# Die Volksverschlüsselung®:

## Förderung vertrauenswürdiger Ende-zu-Ende-Verschlüsselung durch benutzerfreundliches Schlüssel- und Zertifikatsmanagement

Dominik Spychalski, Levona Eckstein, Michael Herfert, Daniel Trick, Tatjana Rubinstein

Informatik 2017, Chemnitz

26. September 2017

# INHALT

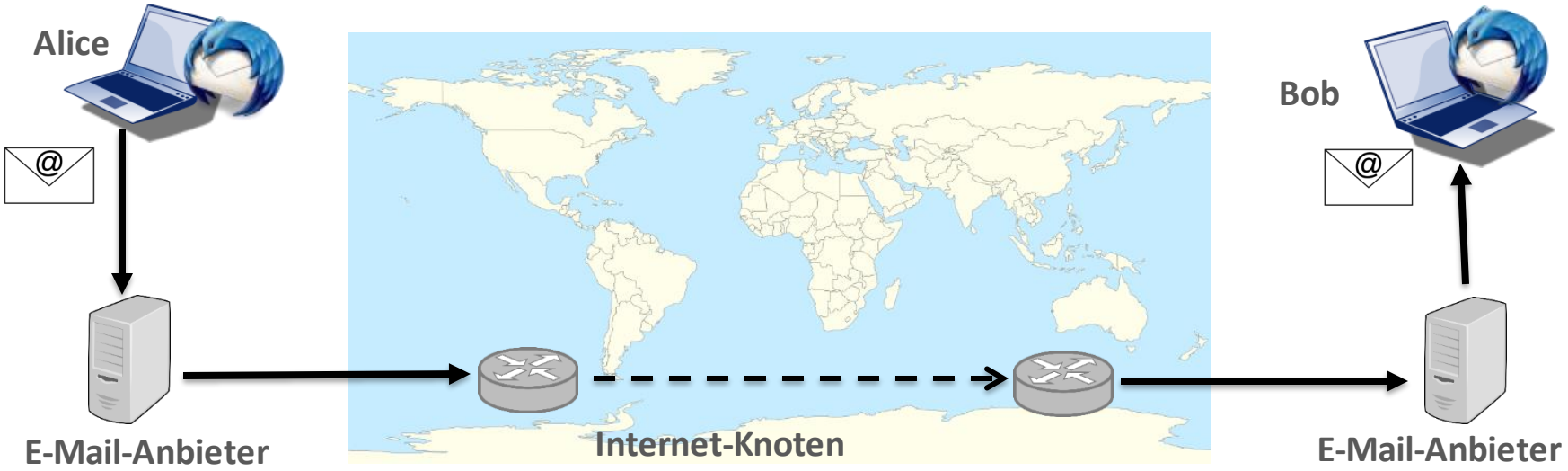
- Einführung und Motivation
- Ende-zu-Ende Verschlüsselung und Vertrauensmodelle
- Die Volksverschlüsselung
  - Projektziele
  - Architektur und Funktionsweise
  - Das Zertifizierungsmodell
  - Zertifikatsqualität durch Identitätsprüfung
  - Realisierungsdetails
- Fazit und Ausblick

# Einführung und Motivation

- Analyse der Beiden größten deutschen Anbieter für E-Mail[1]: 2016 Rekordjahr für E-Mail – ca. 625,8 Mrd
  - Einsatz in privatem und geschäftlichem Kontext
  - Seit 2010 verdoppet, ähnlicher Trend erwartet
- BITKOM Studie [2]: Nur etwa 15%der Nutzer in Deutschland verschlüsseln ihre E-Mails
- Mangelnde Benutzerfreundlichkeit wurde als Hauptgrund identifiziert

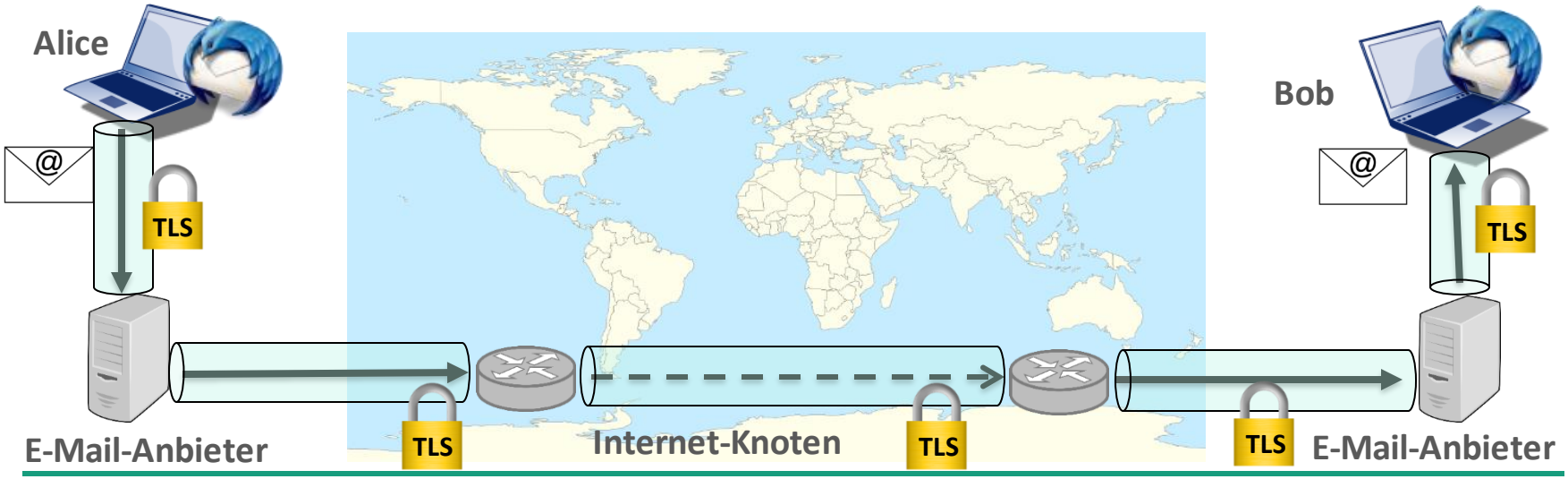
# Einführung und Motivation

- Ungeschützter Versand von E-Mails
- Inhalt der E-Mail auf kompletten Kommunikationspfad im Klartext
- Kommunikationsmetadaten ermöglichen Profilbildung durch unbefugte Dritte mit Zugriff auf den Kommunikationskanal



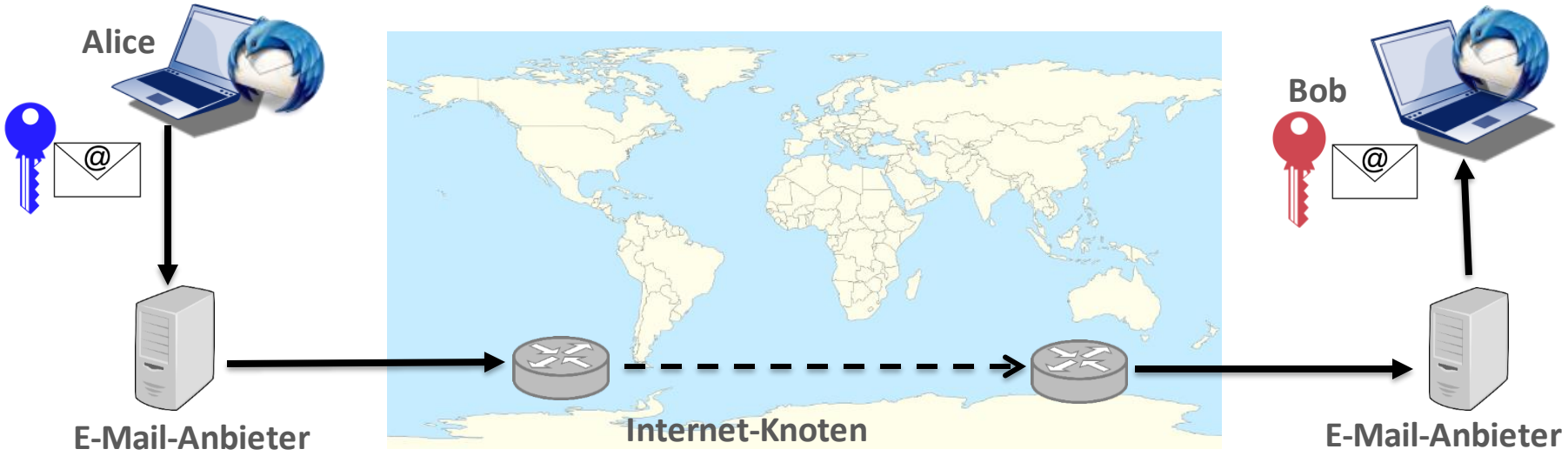
# Einführung und Motivation

- Provider-seitiger Schutzmechanismus: Transportwegsicherung – TLS/SSL
- Inhalt und Kommunikationsmetadaten nur durch Servie Provider und auf Knotenpunkten einsehbar



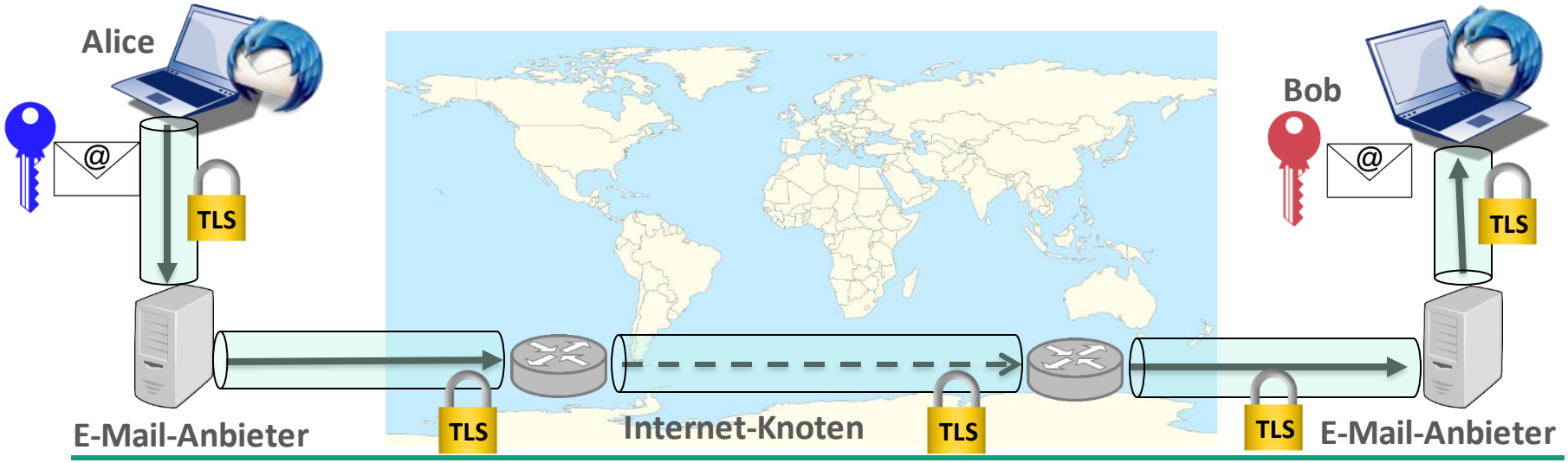
# Einführung und Motivation

- Ende-zu-Ende verschlüsselte E-Mails: Klartext nur durch Kommunikationspartner einsehbar
- Kommunikationsmetadaten ermöglichen Profilbildung durch unbefugte Dritte mit Zugriff auf den Kommunikationskanal



# Einführung und Motivation

- Ideal: Kombination der provider-seitigen und client-seitigen Schutzmechanismen
- Inhalte nur durch Kommunikationspartner einsehbar
- Kommunikationsmetadaten nur durch Service Provider einsehbar

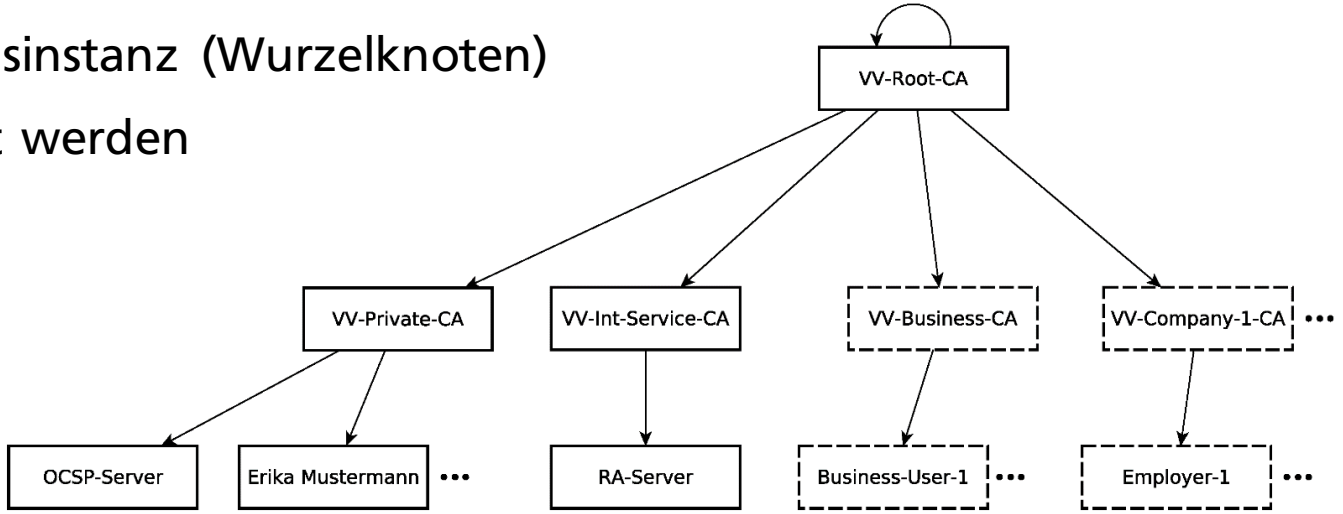


# Ende-zu-Ende Verschlüsselung

- Asymmetrische Kryptographie: Schlüsselpaar bestehend aus privatem Schlüssel $sk$ und öffentlichem Schlüssel $pk$
  - Basierend auf mathematischem Referenzproblem
  - Kryptographische Algorithmen und Verfahren sind kommutativ
- Ver-/Entschlüsselung $\mathrm{c} \leftarrow enc_{pk}\ (m)$ $\mathrm{m} \coloneqq dec_{sk}(c)$
  - Schutz der Vertraulichkeit
- Digitale Signatur $\sigma \leftarrow sig_{sk}(m)$ $b \coloneqq vf_{pk}(m, \sigma),\ b \in \{1,0\}$
  - Schutz der Integrität und Authentizität
- Verschiedene Vertrauensmodelle zur Bescheinigung der Authentizität eines kryptographischen Schlüssels
- Digitale Zertifikate zur Schlüsselverteilung und Bescheinigen der Subjekt ↔ Objekt($pk$) Bindung

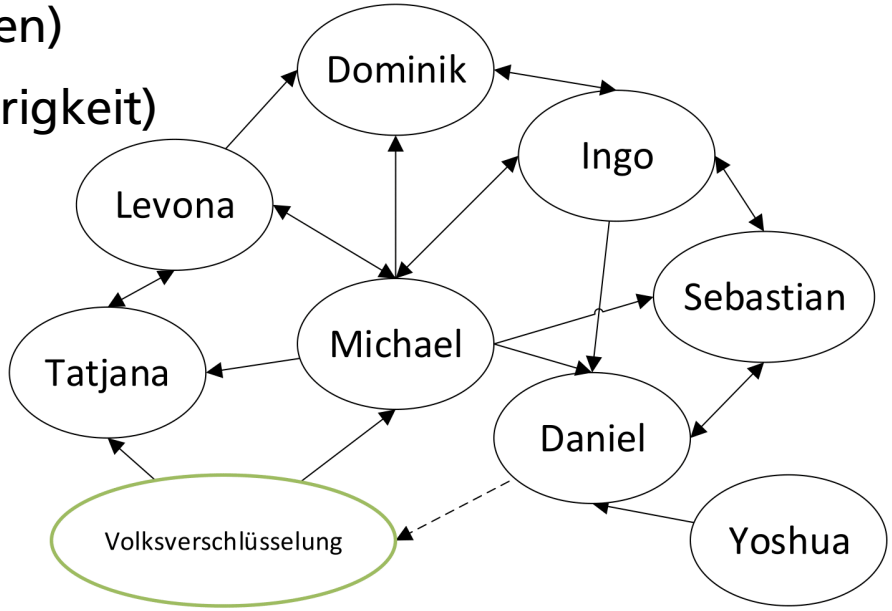
# Ende-zu-Ende Verschlüsselung
## Vertrauensmodelle – S/MIME

- Zentrales und hierarisches Vertrauensmodell: Public Key Infrastructure
- Fast alle Mail-Clients unterstützen S/MIME nativ, einfache Nutzbarkeit
- Aktuell keine Unterstützung für Webmailer
- X.509-Zertifikate werden durch Zertifizierungsinstanz ausgestellt
  - Prozessregelung/-definition durch Zertifizierungsrichtlinien
- Zertifizierungsinstanz (Wurzelknoten) muss vertraut werden



# Ende-zu-Ende Verschlüsselung
## Vertrauensmodelle - PGP

- Installation von Plugins und Zusatzsoftware notwendig, dann auch mit Unterstützung von Webmailern
- Dezentrales Vertrauensmodell: Nutzer bescheinigen gegenseitug die Gültigkeit eines Schlüssels mittels digitaler Signaturen
  - Owner Trust (Signaturverhalten)
  - Key Validity (Schlüsselzugehörigkeit)
- Es muss auf die Fahigkeit und Sorfalt der Signierenden Vertraut werden
  →Signaturen nicht äquivalent



# Die Volksverschlüsselung

- Initiative des Fraunhofer SIT zur Verbreitung der vertrauenswürdigen Ende-zu-Ende Verschlüsselung für die E-Mail Kommunikation
- Stellt Klasse 3 Zertifikate basierend auf einer starken Identitätsprüfung aus
- Kostenlos für Privatanwender
- Fokus auf Gebrauchstauglichkeit
  - Z.B. durch die automatisierte Konfiguration etablierter Client-Anwendungen wie Outlook, Thunderbird, Firefox, Chrome, usw.
  - Wurde durch diverse Studien und Arbeiten evaluiert und verbessert (z.B. durch die Universität der Künste Berlin)
- Setzt auf etablierte Standards und Technologien → Interoperabilität

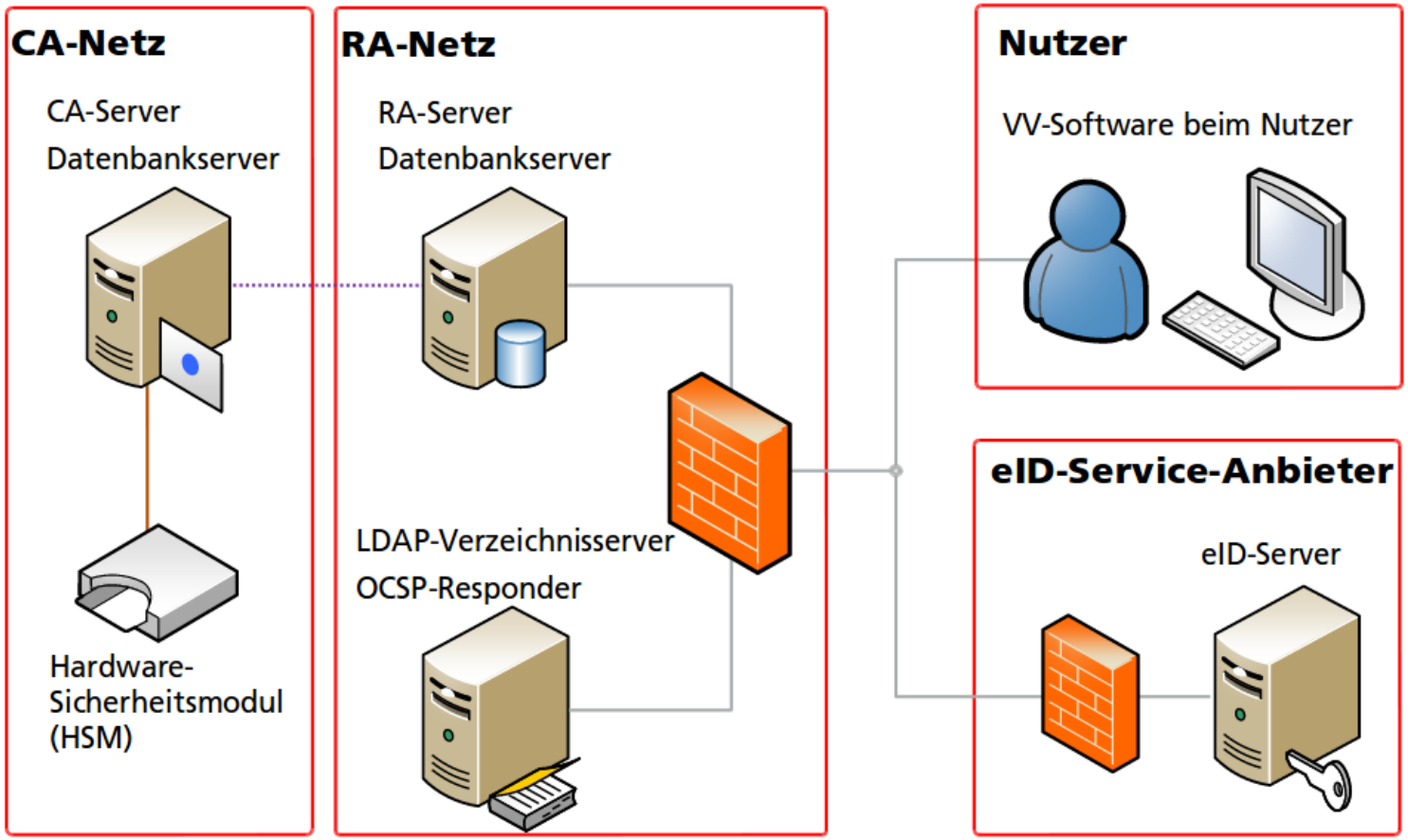
# Die Volksverschlüsselung
## Projektziele

- Gebrauchstauglichkeit
- Identifizierende Schlüssel
- Offene Schnittstellen
- Verwendung von Verschlüsselungsstandards
- Datenschutz und Datensparsamkeit
- Transparenz
- Keine Kosten für Privatanwender

# Die Volksverschlüsselung
## Architektur und Funktionsweise

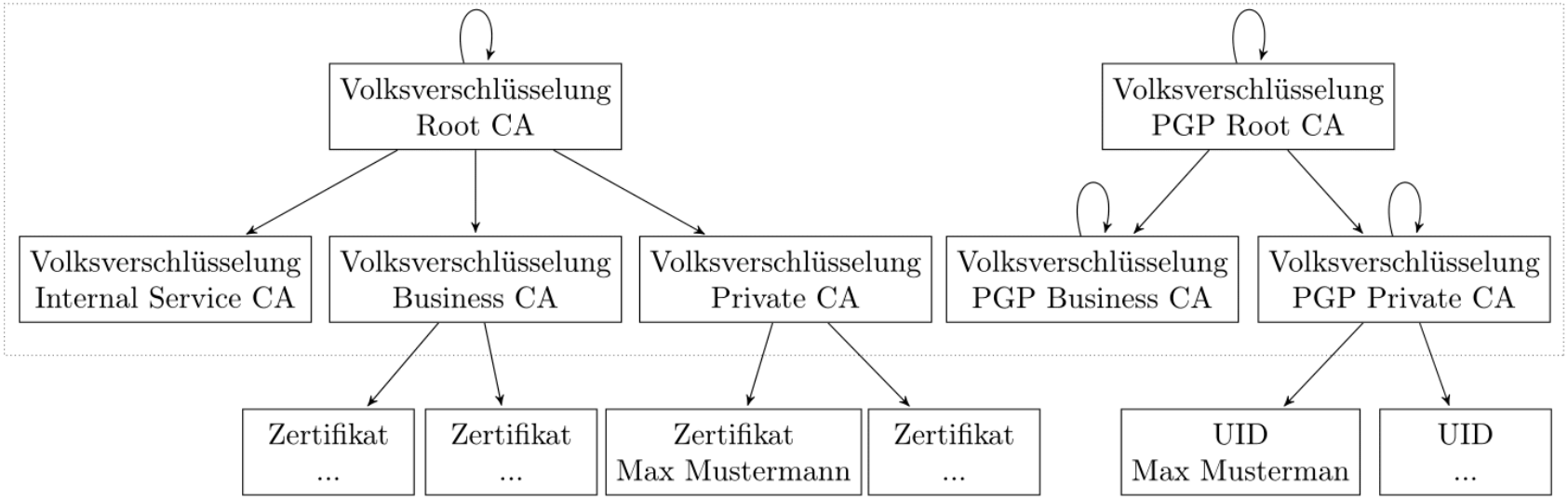
- Client-Anwendung (VV-SW): Unterstützt Anwender bei Authentifizierung, Schlüsselerzeugung und Konfiguration der lokalen Anwendungen
  - Automatisiert alle möglichen Prozesse so weit wie möglich
  - Quellcode ist veröffentlicht → Transparente Erzeugung der Schlüssel
  - Client-Konfiguratoren modular erweiterbar (Plug-in Mechanismus)
  - Aktuell nur für Windows verfügbar
- Server-Seite: Stellt Zertifikate und Signaturen aus
  - Öffentliche REST-Schnittstelle
  - Bietet weitere Dienste (z.B. OCSP, LDAP)
- Entwicklungs- und Zertifizierungsverantwortung bei SIT, Betrieb in Rechenzentrum der Deutschen Telekom AG

# Die Volksverschlüsselung
## Architektur und Funktionsweise



# Die Volksverschlüsselung
## Das Zertifizierungsmodell

- Wurzelknoten der Volksverschlüsselung ist selbstsigniert
  - Nicht per default in den Truststores (Browser, OS)
  - Installation erfolgt während Client-Konfiguration in VV-SW



# Die Volksverschlüsselung
## Zertifikatsqualität durch Identitätsprüfung

- Starke Identitätsprüfung elementar: Klasse-3 Zertifikate/Signaturen
- Umgesetzte Authentifizierungsmethoden
  - Online-Ausweisfunktion des Personalausweises
  - Kundenkonto der Deutschen Telekom AG
  - Registrierungscode
  - SmartCard der FhG


# Die Volksverschlüsselung
## Realisierungsdetails

- Einsatz von OpenSource Technologien unter Berücksichtigung des Sicherheitsnivaus bevorzugt (EJBCA, OpenLDAP)
- Verzeichnisdienst (OpenLDAP)
  - Anonymer Zugriff → Jeder kann das Verzeichnis nutzen
  - Datenschuzkontzept per Overlay-Plugin durchgesetzt (C)
    - Suche nur auf Basis einer expliziten E-Mail-Adresse
- VV-SW (C# & WPF) nutzt etablierte Drittbibliotheken z.B. Bouncy Castle
- RA-Server verwendet das Play-Framework (Java)

# Die Volksverschlüsselung
## Fazit und Ausblick

- Die Volksverschlüsselung ist eine Initiative mit dem Ziel, kryptographische Schlüssel benutzerfreundlich an Nutzer zu verteilen
- Förderung des Selbstdatenschutzes
- Kooperationen und Multiplikatoren
- Weitere Authentifizierungsverfahren
- Plattformunabhängigkeit
- Einsatz in einem geschäftlichen Kontext (Backup, Schlüsselverteilung)

Fraunhofer SIT


## Dominik Spychalski

**Fraunhofer-Institut für Sichere Informationstechnologie SIT**

Cloud Computing, Identity & Privacy

Rheinstraße 75, 64295 Darmstadt

E-Mail dominik.spychalski@sit.fraunhofer.de

Telefon +49 6151 869 249


www.sit.fraunhofer.de

www.volksverschluesselung.de

# Quellen

[1] https://newsroom.web.de/2017/02/13/2016-rekordjahr-fuer-e-mail/

[2] https://www.bitkom.org/Presse/Presseinformation/Verschluesselung-von-E-Mails-kommt-nur-langsam-voran.html