E-Mail-Verschlüsselung für Behörden und Unternehmen - Volksverschlüsselung und Ideen zum Schlüsseltausch

Ulrich Waldmann

Sommerakademie des ULD, Kiel
19. September 2016

Partner in

CRISP
Center for Research in Security and Privacy

Fraunhofer SIT

E-Mail-Verschlüsselung - wirklich?

- **Hintergrund**
  - Ende-zu-Ende-Verschlüsselung ist ein wirksames Mittel gegen die anlasslose Massenüberwachung.
  - **Zielsetzung: Verschlüsseln soll so selbstverständlich sein wie das Anschnallen im Auto.**

- **Konzepte und Programme**
  - Transportsicherung: E-Mail Made in Germany
  - Gesetzesbasiert: De-Mail
  - Software-Plugins: Enigmail, Mailvelope, pretty Easy privacy (p≡p), Gpg4win, ...
  - Zertifizierungsdienste: Commodo, Let's Encrypt, ...
  - Mail-Anbieter: Posteo, mailbox.org, ...

E-Mail-Verschlüsselung - weiteres Wachstum?

- Viele gute Initiativen
- Aber noch nicht für jeden beantwortet:

1. **Wie erhält man kryptografische Schlüssel für die Ende-zu-Ende-Verschlüsselung?**
2. **Wie kann man die Schlüssel nutzen, auch wenn man kein IT-Experte ist?**
3. **Wie können Firmen / Behörden Kunden und Bürger mit Schlüsseln versorgen? (um vertrauliche Mails zu senden)**
4. **Wie findet man die Schlüssel der Kommunikationspartner?**

Volksverschlüsselung® – Idee

1. **Wie erhält man kryptografische Schlüssel für die Ende-zu-Ende-Verschlüsselung?**
2. **Wie kann man die Schlüssel nutzen, auch wenn man kein IT-Experte ist?**

- **Lösungsansatz der Volksverschlüsselung (VV)**
  - Die **VV-Software** erzeugt Schlüssel und lässt sie zertifizieren.
  - Die **Telekom** betreibt die technische Infrastruktur der Volksverschlüsselung.
  - Die Verschlüsselung erfolgt mit den üblichen E-Mail-Anwendungen.
  - Die private Nutzung ist kostenlos.

Volksverschlüsselung® – Features

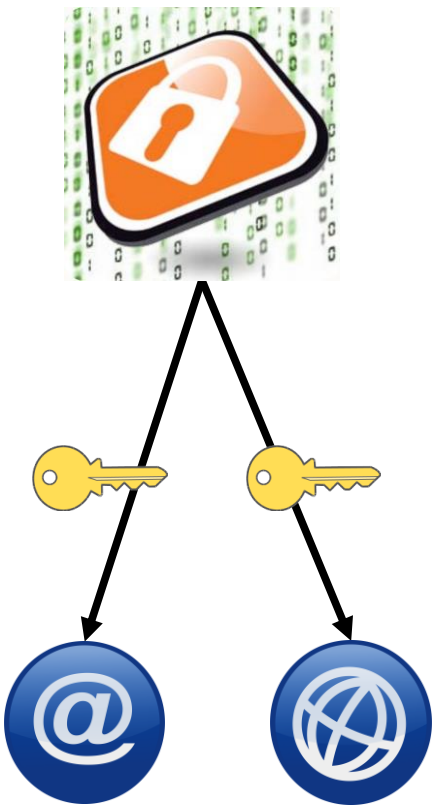
1. **VV-Software**
unterstützt Identifizierung
und erzeugt Schlüssel

Fraunhofer SIT

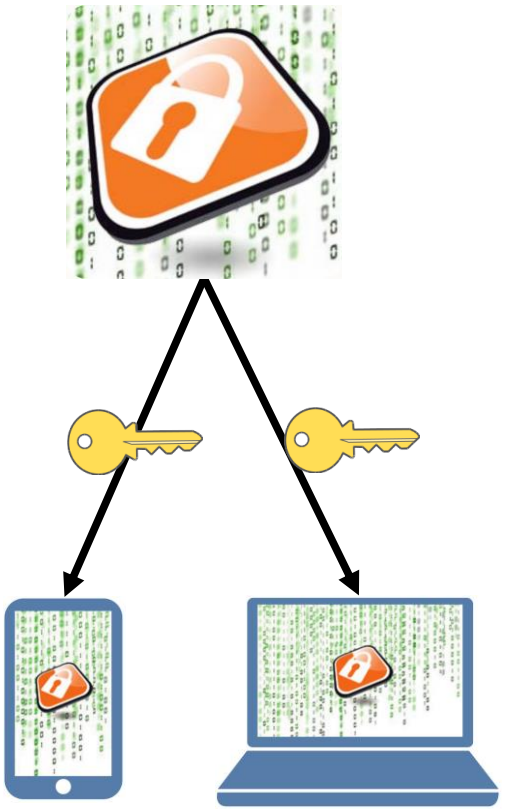
2. **VV-Software**
lässt die Schlüssel
zertifizieren

Fraunhofer SIT

3. **VV-Software**
verteilt Schlüssel
an lokale Anwendungen

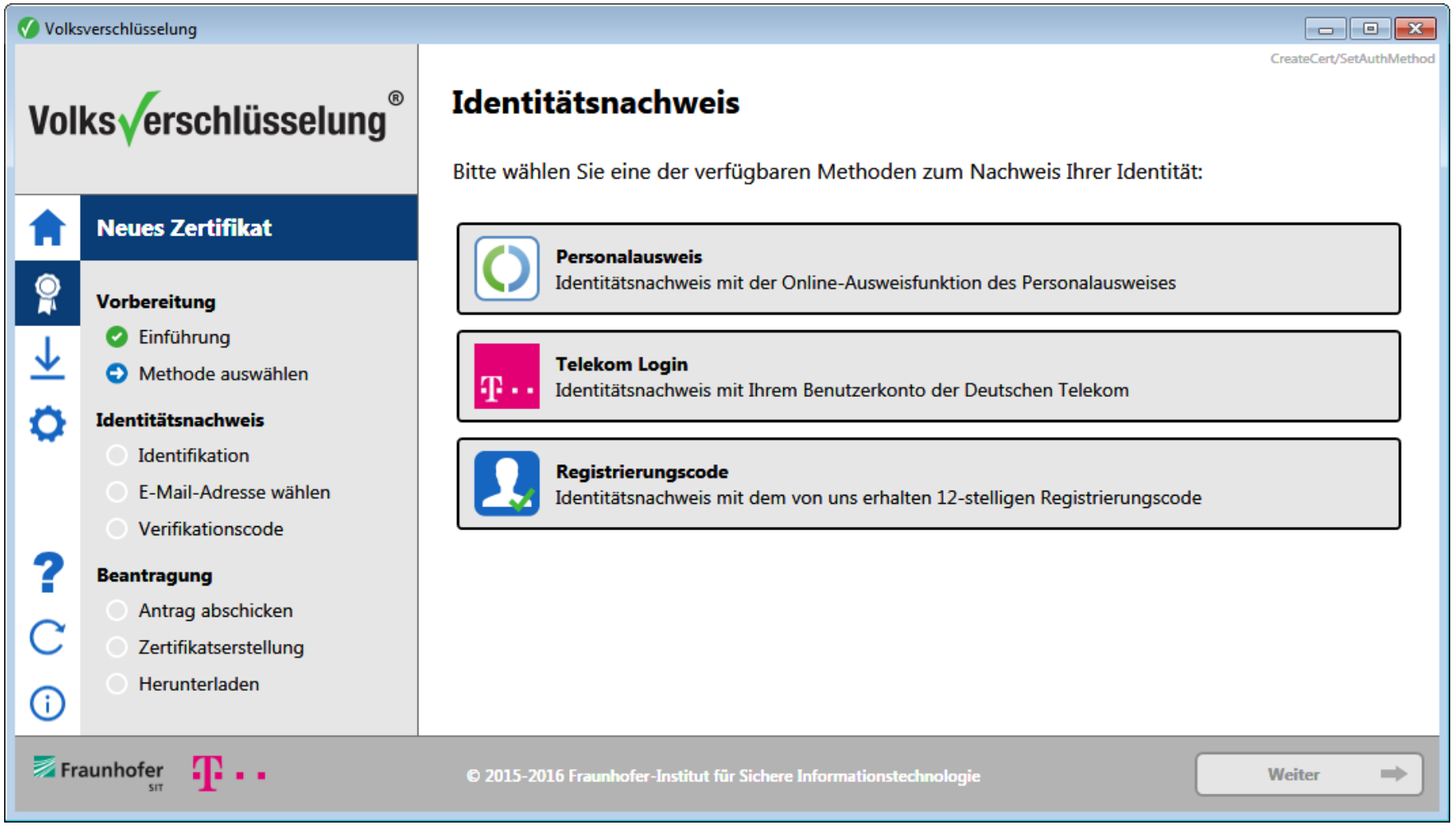


4. **VV-Software**
verteilt Schlüssel
an weitere Geräte

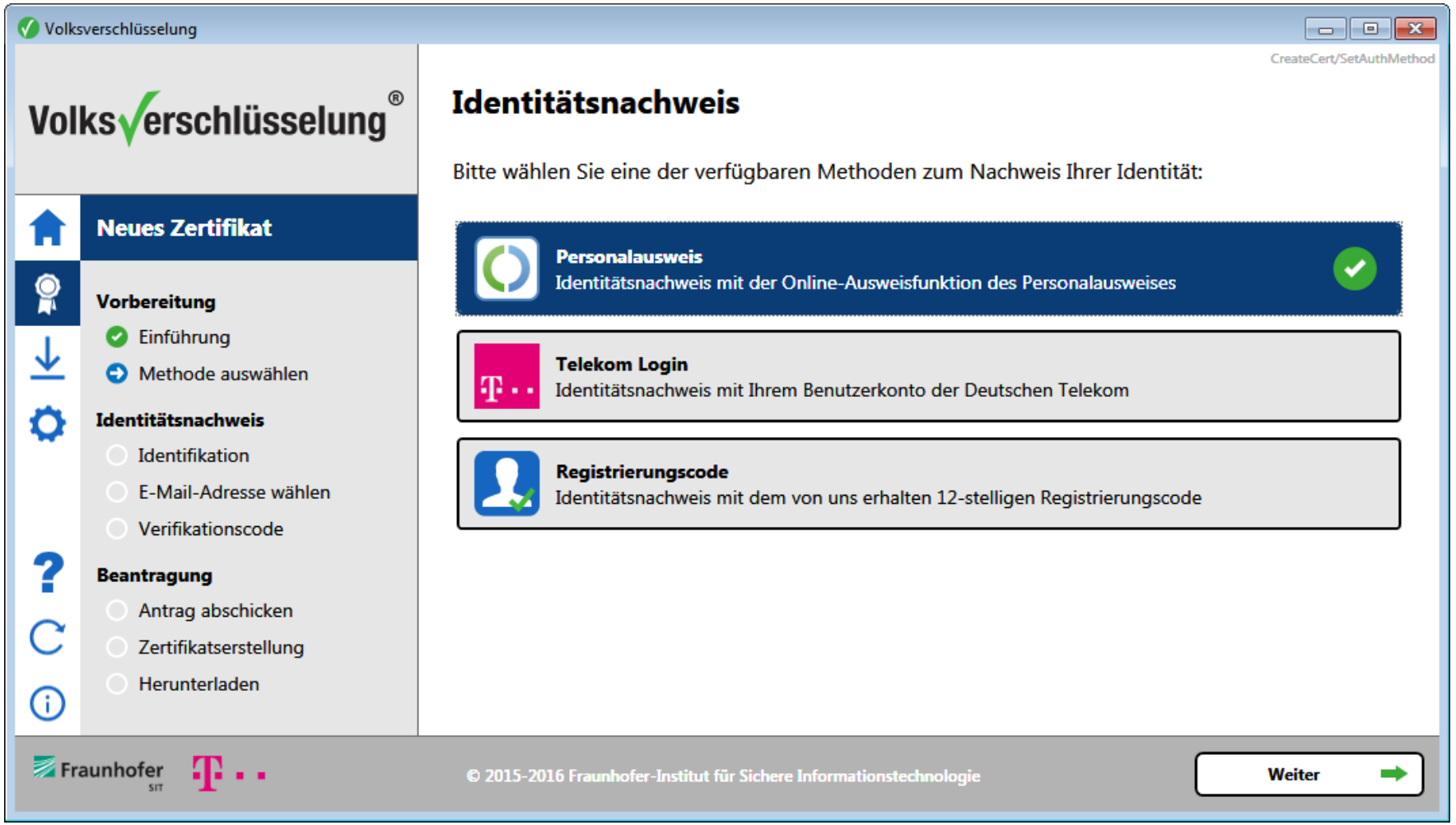


Volksverschlüsselung® – Hauptmenü

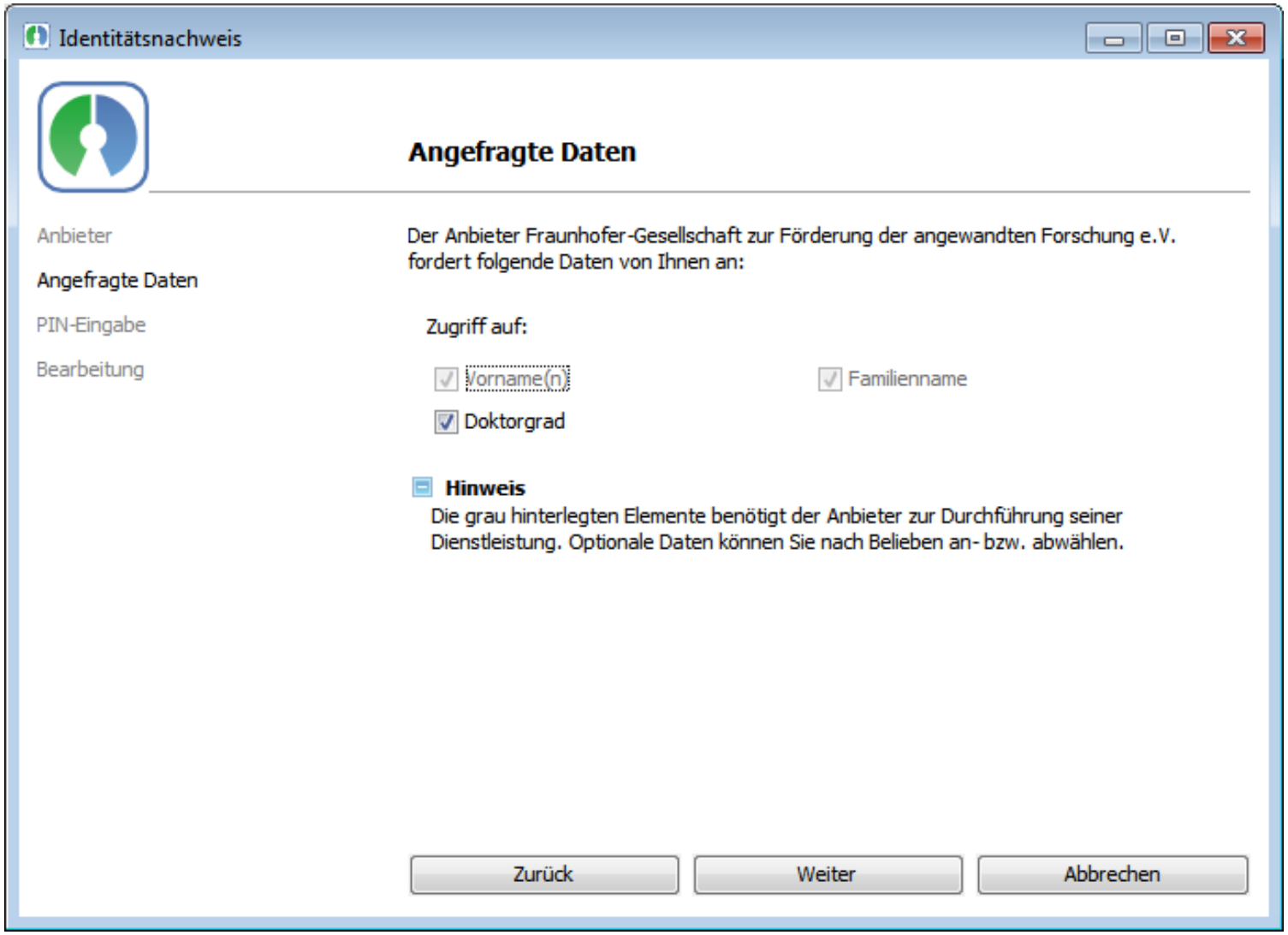
Volksverschlüsselung® – Identitätsprüfung



Volksverschlüsselung® – Personalausweis

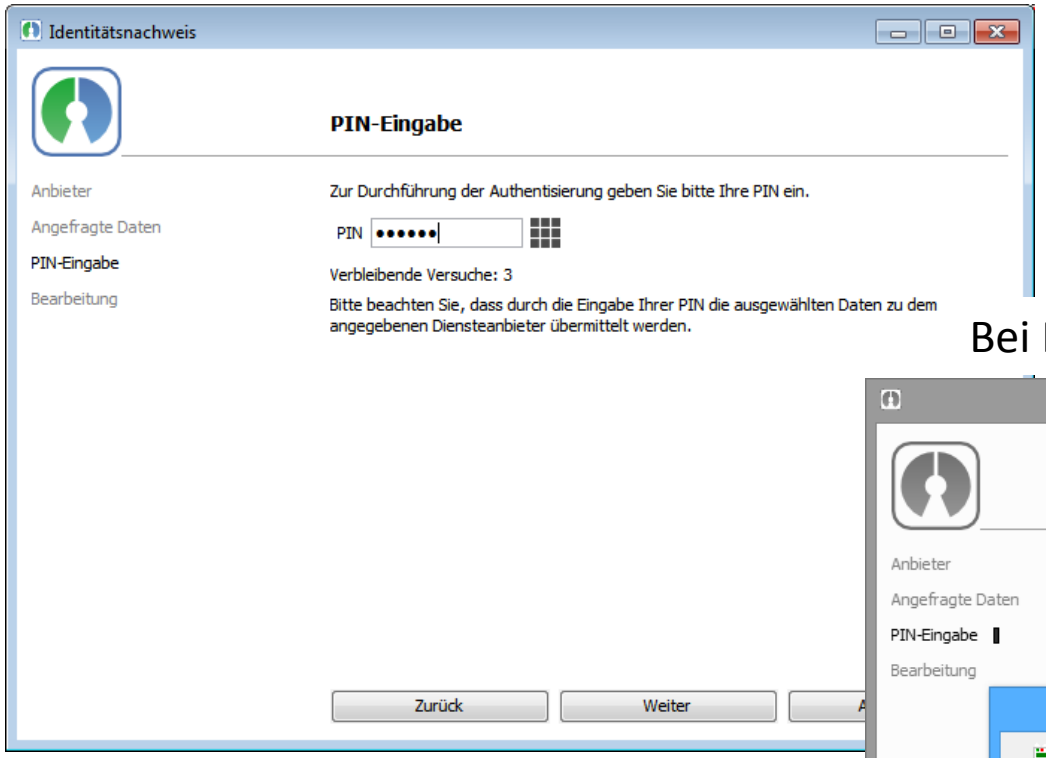


VolksVerschlüsselung® – Personalausweis

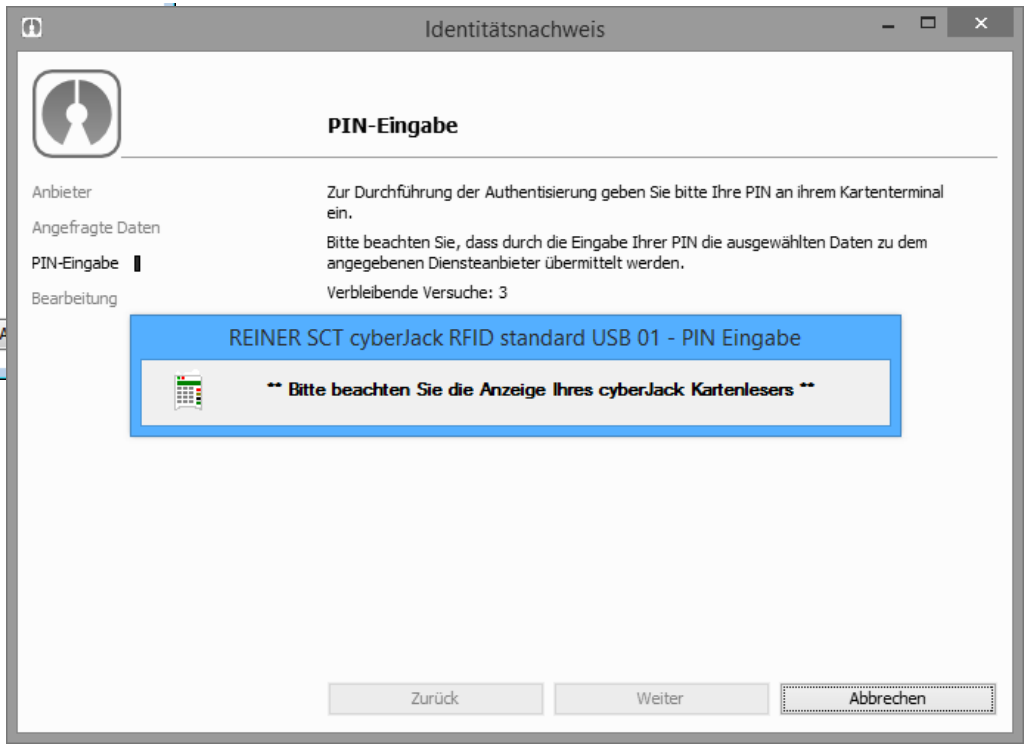


VolksVerschlüsselung® – Personalausweis

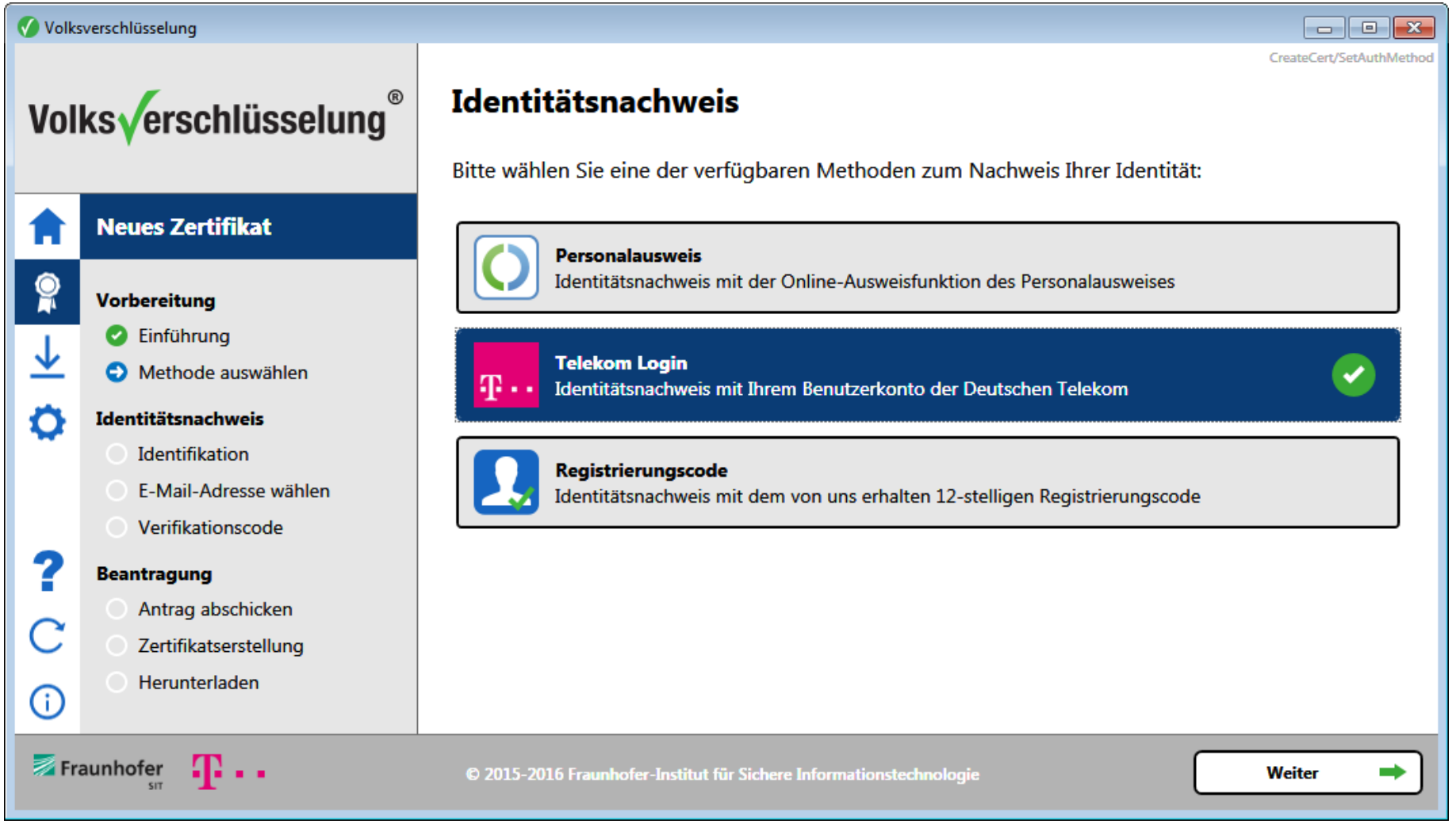
Bei Nutzung eines Basislesers (ohne Tastatur)



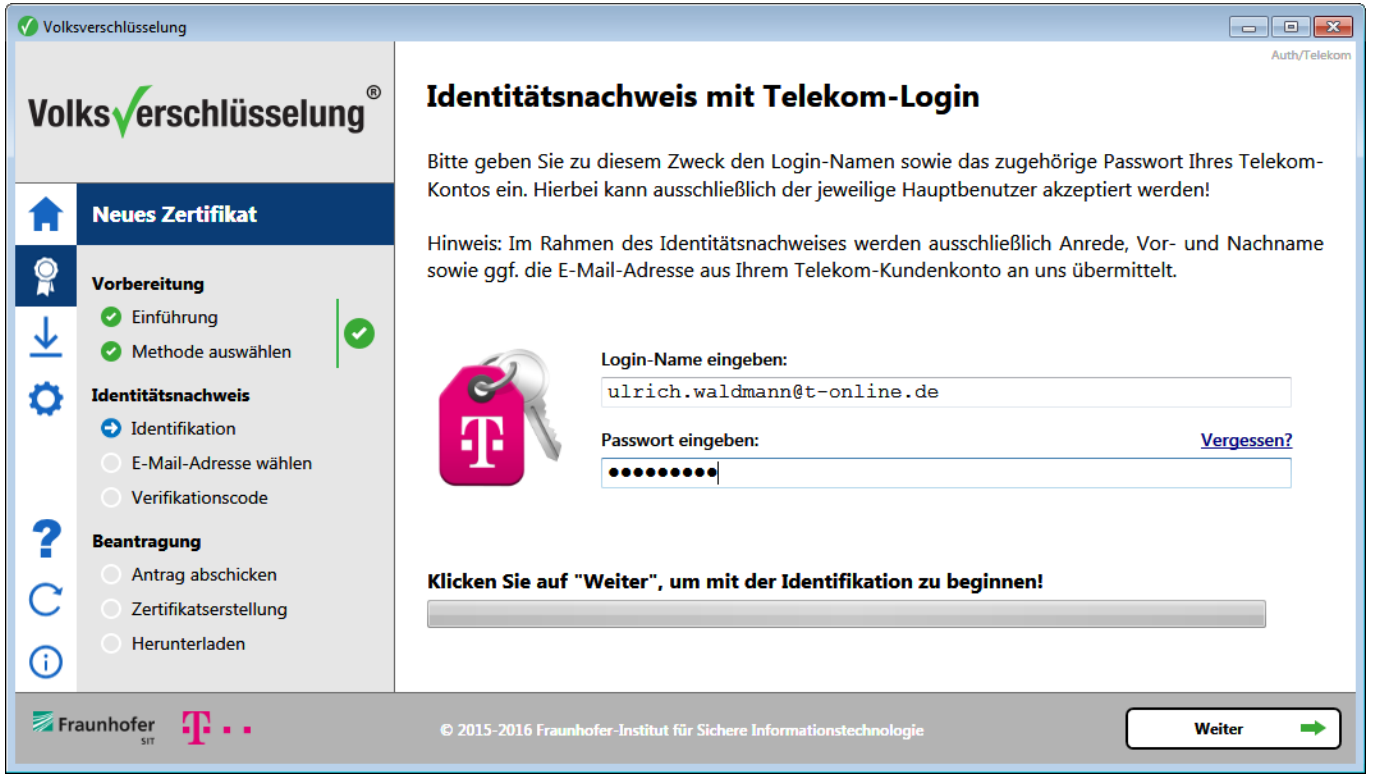
Bei Nutzung eines Standardlesers (mit Tastatur)



Volksverschlüsselung® – Telekom-Login

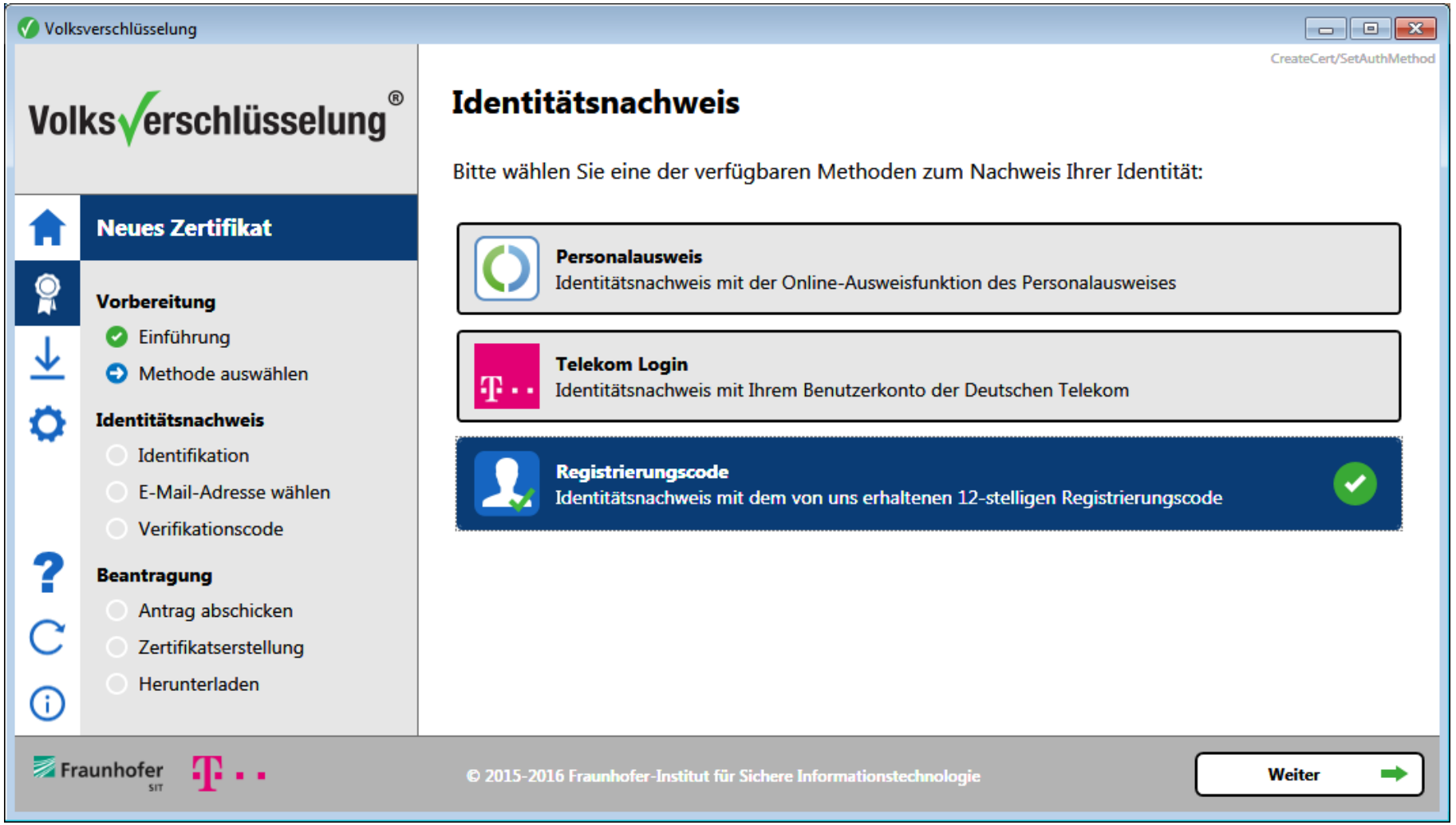


Volksverschlüsselung® – Telekom-Login



- Ausschließlich für Telekom-Festnetzkunden
  - VV-Software verbindet sich mit Telekom-Identitätsmanagement-Server
  - Telekom sendet JSON-Web-Token mit Vorname, Nachname, E-Mail-Adresse

Volksverschlüsselung® – Registrierungscode

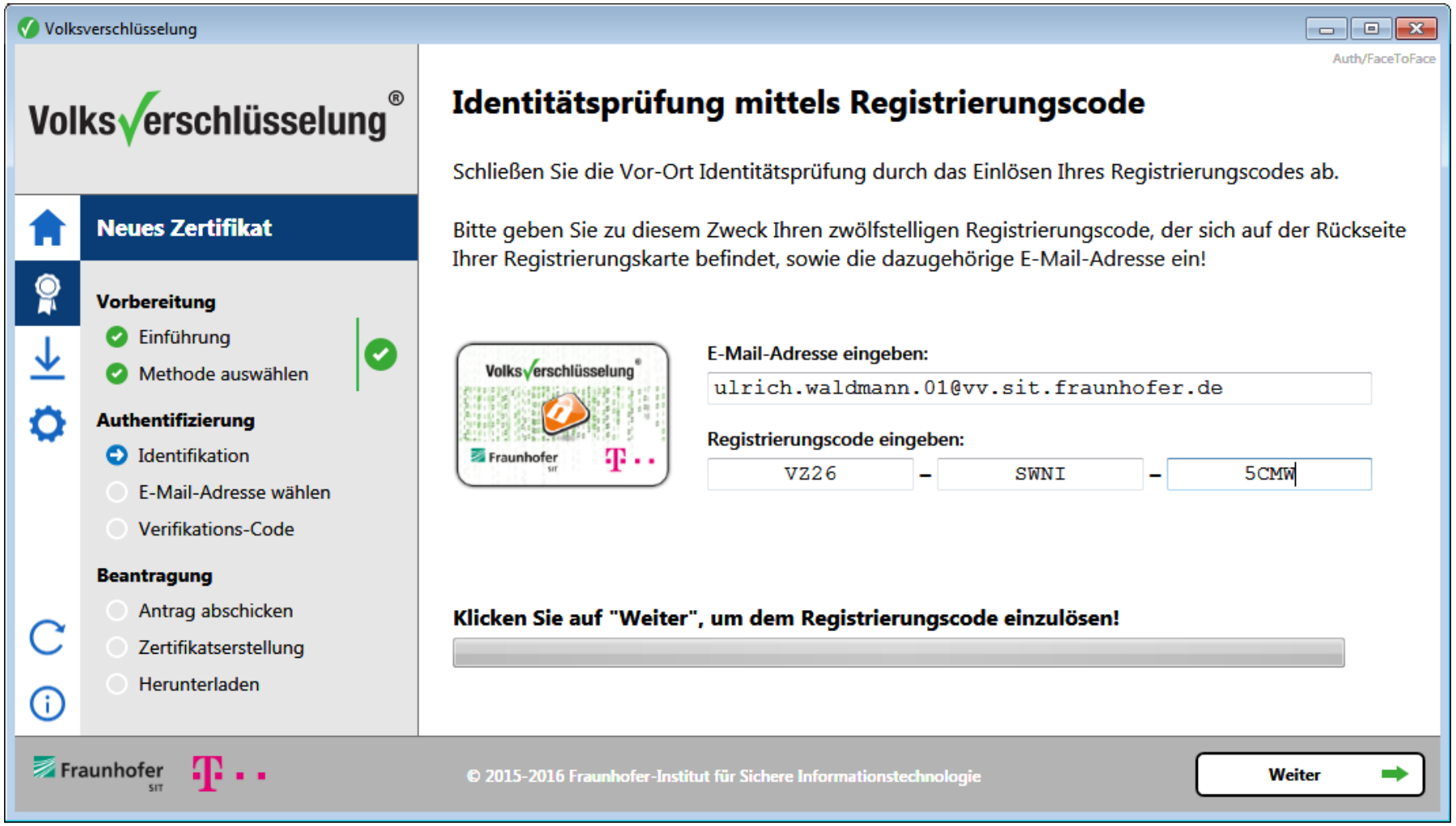


Volksverschlüsselung® – Registrierungscode

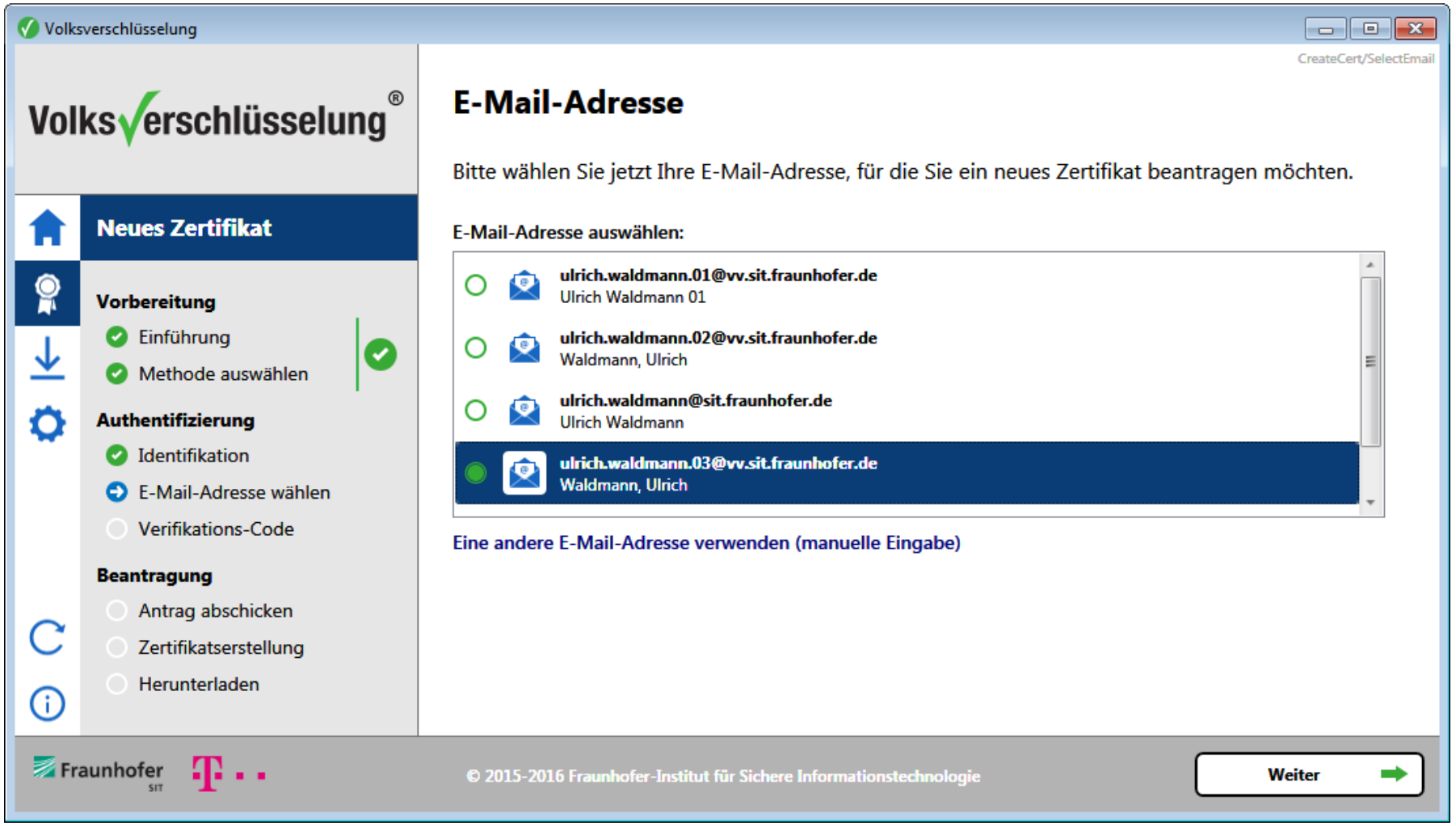
- **Ausgabe des Registrierungscodes**
  - Zukünftiger Nutzer trifft Fraunhofer SIT auf öffentlicher Veranstaltung
  - SIT identifiziert die Person anhand des Personalausweises
  - Person erhält Registrierungscode
  - Registrierungscode ist Authentifizierung in der VV-Software

- **Ziel**: Schlüssel für Menschen, die weder Online-Ausweisfunktion des Personalausweises noch Telekom-Account haben

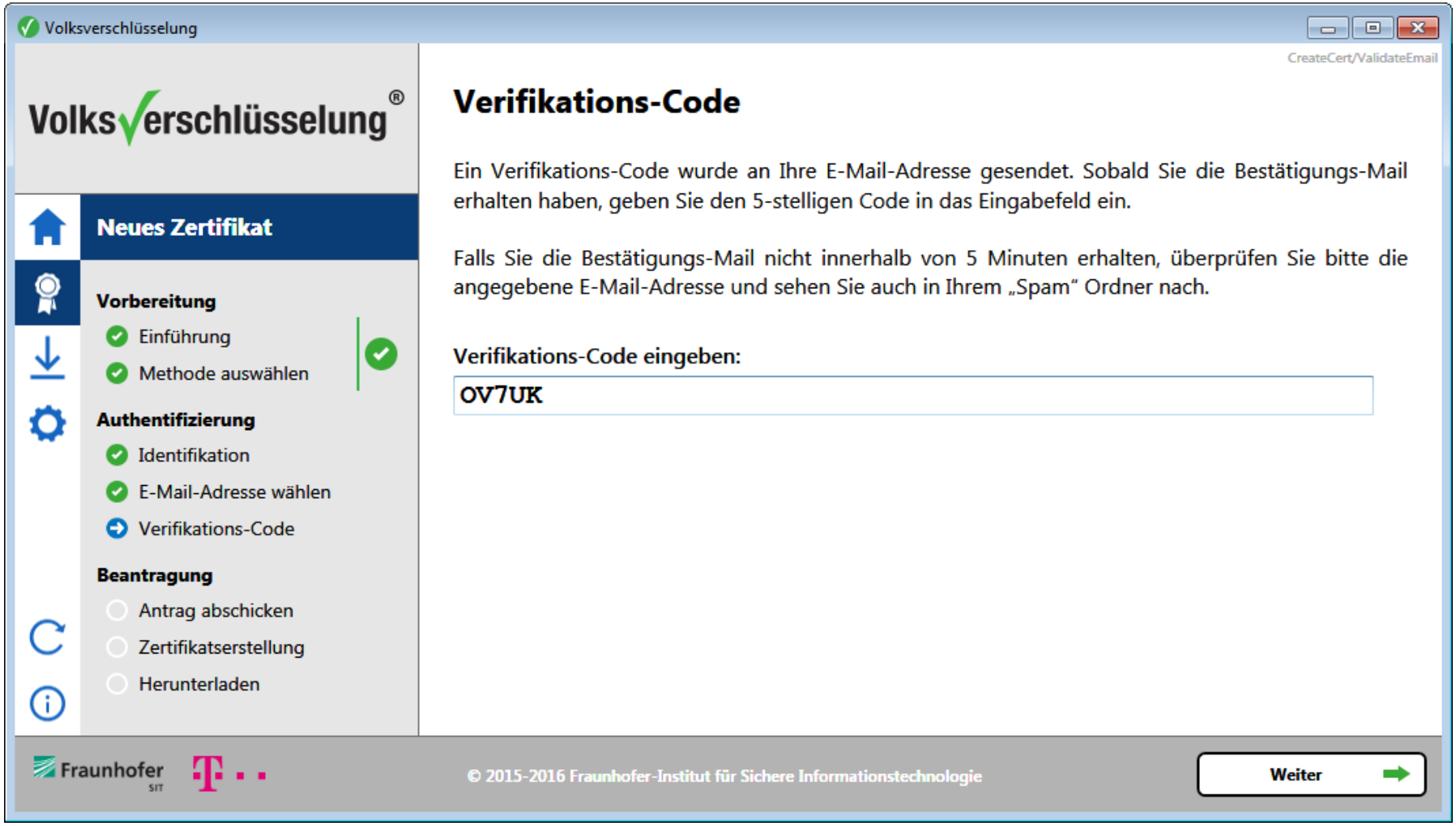
Volksverschlüsselung® – Registrierungscode



Volksverschlüsselung® – Auswahl der E-Mail-Adresse

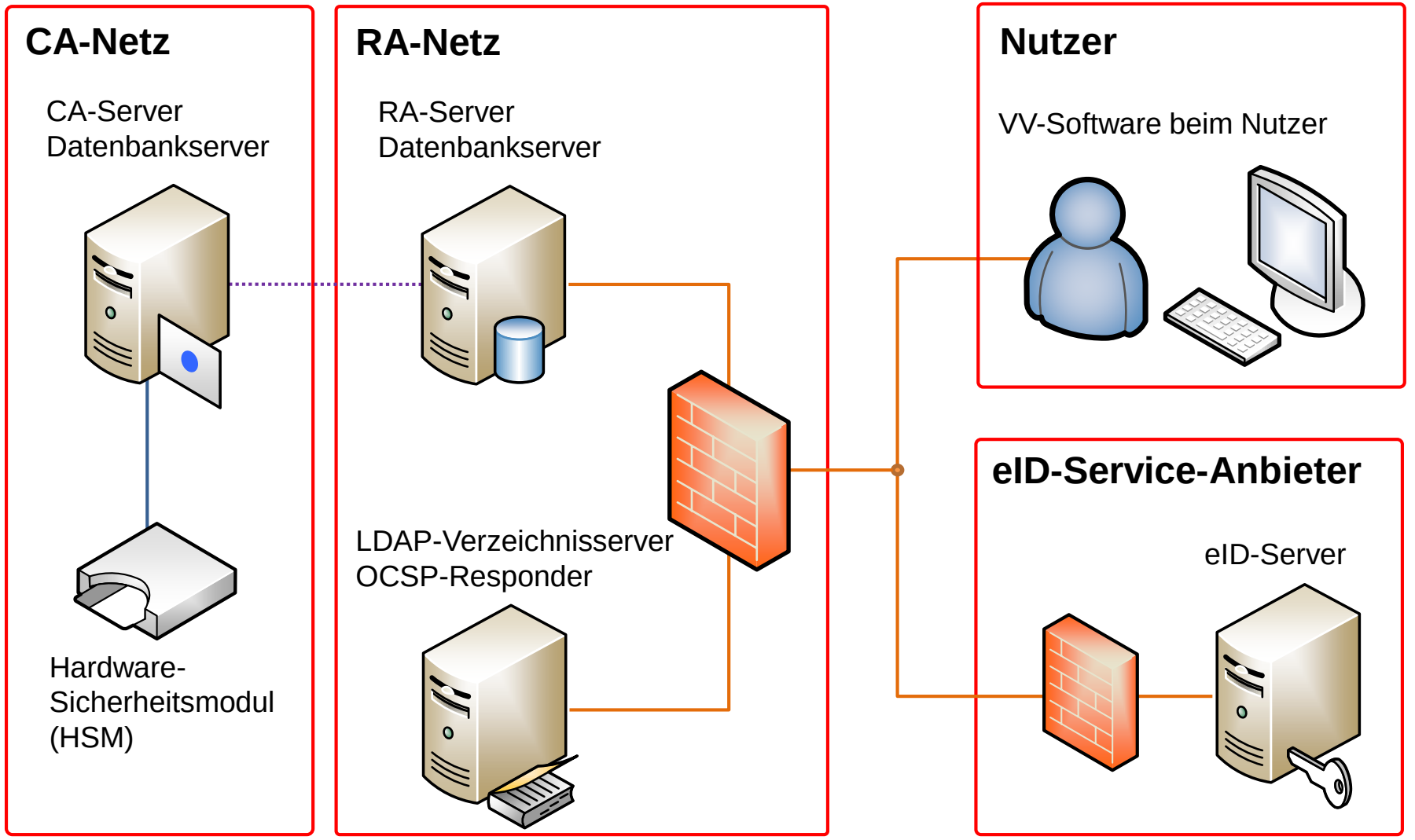


Volksverschlüsselung® – Prüfung der E-Mail-Adresse



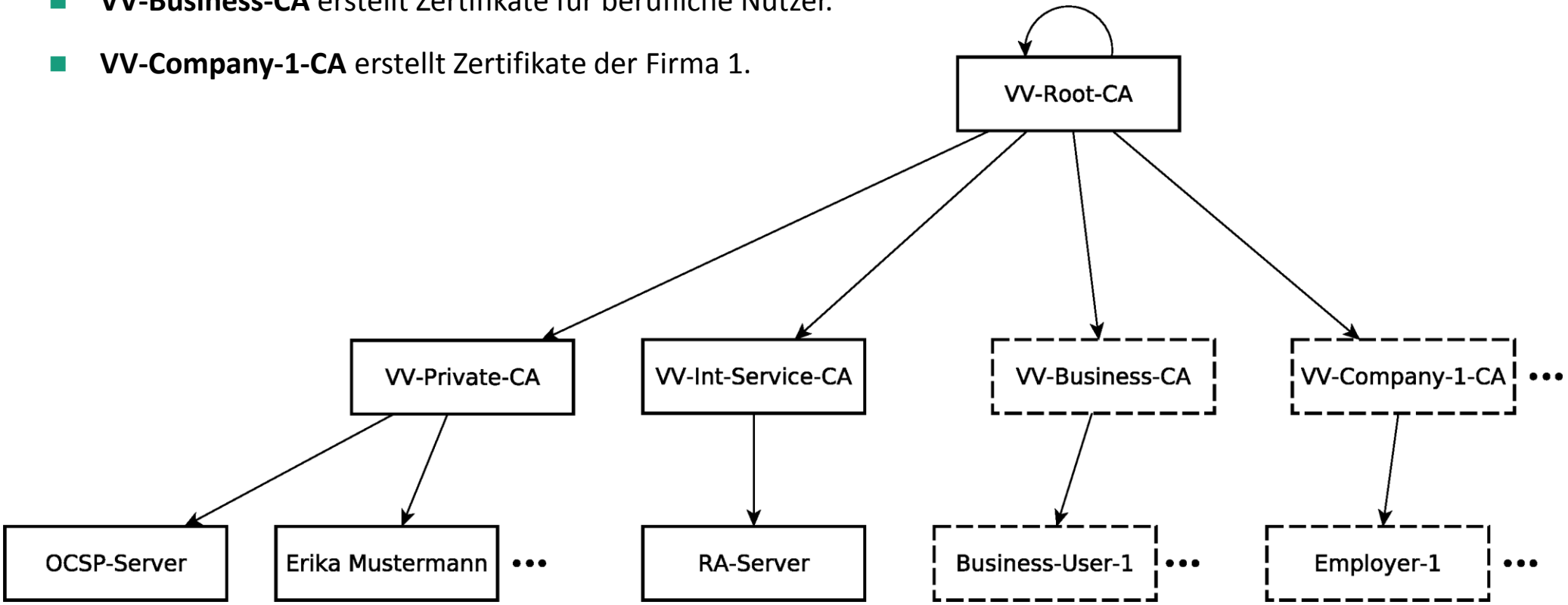
Volksverschlüsselung® – Auswahl der Anwendungen

VolksVerschlüsselung® – Infrastruktur



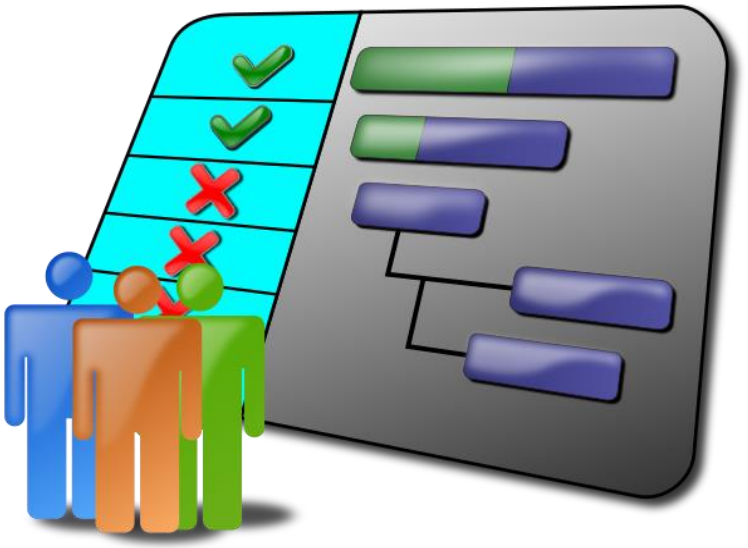
Volksverschlüsselung® – Zertifizierungshierarchie

- **VV-Root-CA** in den Anwendungen NICHT vorinstalliert.
- **VV-Private-CA** erstellt Zertifikate für Privatnutzer.
- **VV-Int-Service-CA** erstellt Zertifikate für techn. Komponenten.
- **VV-Business-CA** erstellt Zertifikate für berufliche Nutzer.
- **VV-Company-1-CA** erstellt Zertifikate der Firma 1.



Volksverschlüsselung® – Weitere Schritte

- Integration von OpenPGP und WebMail
- Identifikation mit existierenden Schlüsseln
- Identifikation über ein Bezahlsystem
- Registrierung in Telekom-Shops
- Versionen für Mac OS X, Linux, iOS, Android



- **Schlüsselgenerierung**
  - PGP-Schlüssel sollen in VV-Software erzeugt oder alternativ aus anderer Quelle bezogen werden:
    - aus einer Datei oder
    - aus beliebigem Schlüsselbund oder
    - aus Enigmail oder Mailvelope, ...

- **Konfiguration der Anwendungen**
  - Die PGP-Schlüssel müssen beim Export mit privatem PGP-Schlüssel signiert werden.
  - Die Schlüssel sollen um VV-Signatur ergänzt werden.
  - Die Schlüssel sollen in Enigmail, Mailvelope, ... importiert werden.

Volksverschlüsselung® – Initiative

- Offener Quelltext
- Offenes Kommunikationsprotokoll
- Offen für weitere Krypto-Applikationen
- Offen für Kooperationen mit anderen PKIs
- Offen für kostenlosen privaten Gebrauch
- Offen für Business-Optionen

3. Wie können Firmen / Behörden Kunden und Bürger mit Schlüsseln versorgen?

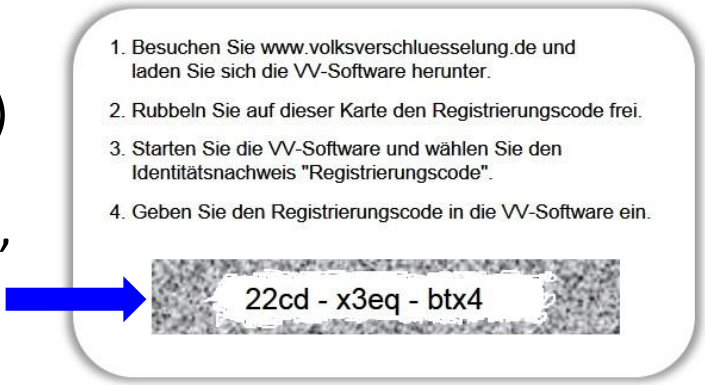
- **Lösung durch Volksverschlüsselung**

  (1) Firma erhält *n* Registrierungscodes,
  ergänzt Mail-Adresse und Name des Kunden.
  (optional: VV übermittelt Mail-Adresse an Firma)

  (2) Firma sendet Registrierungscode an den Kunden,
  z. B. über Kundenportal oder Brief.

  (3) Kunde nutzt VV-Software und authentisiert
  sich dazu über Registrierungscode.

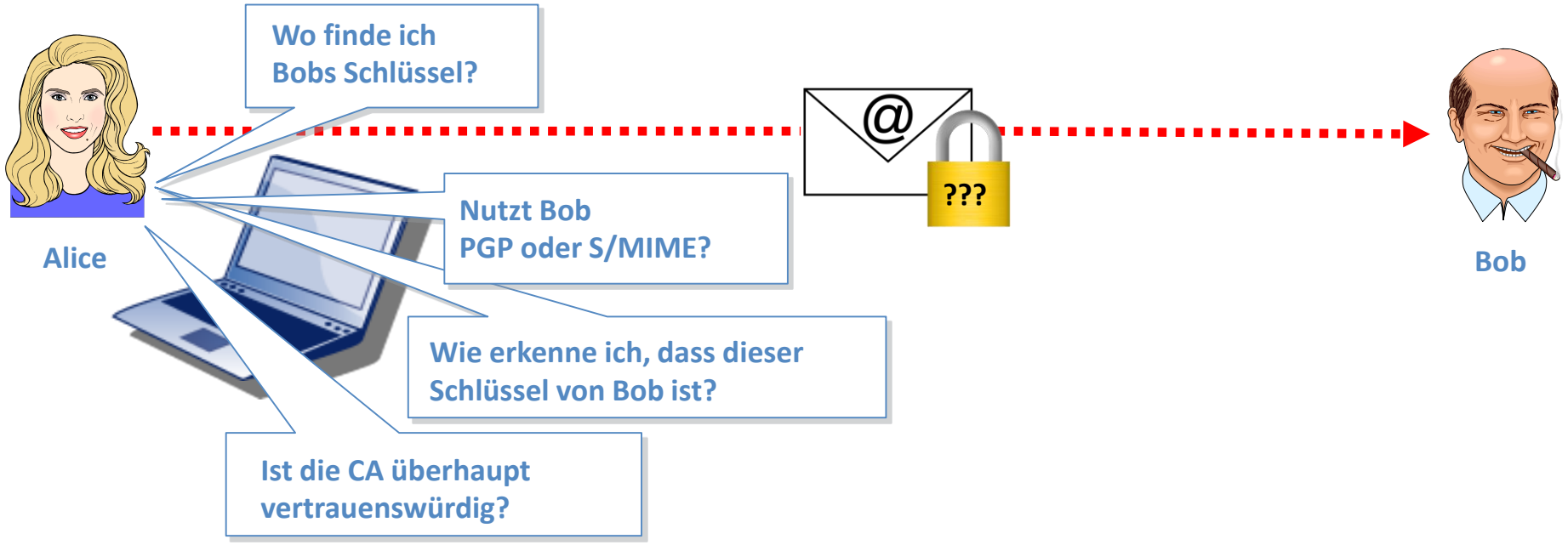
  (4) Firma nutzt VV, um eigene Schlüssel zu erwerben und
  den Schlüssel des Kunden zu finden.



Ideen zum Schlüsseltausch

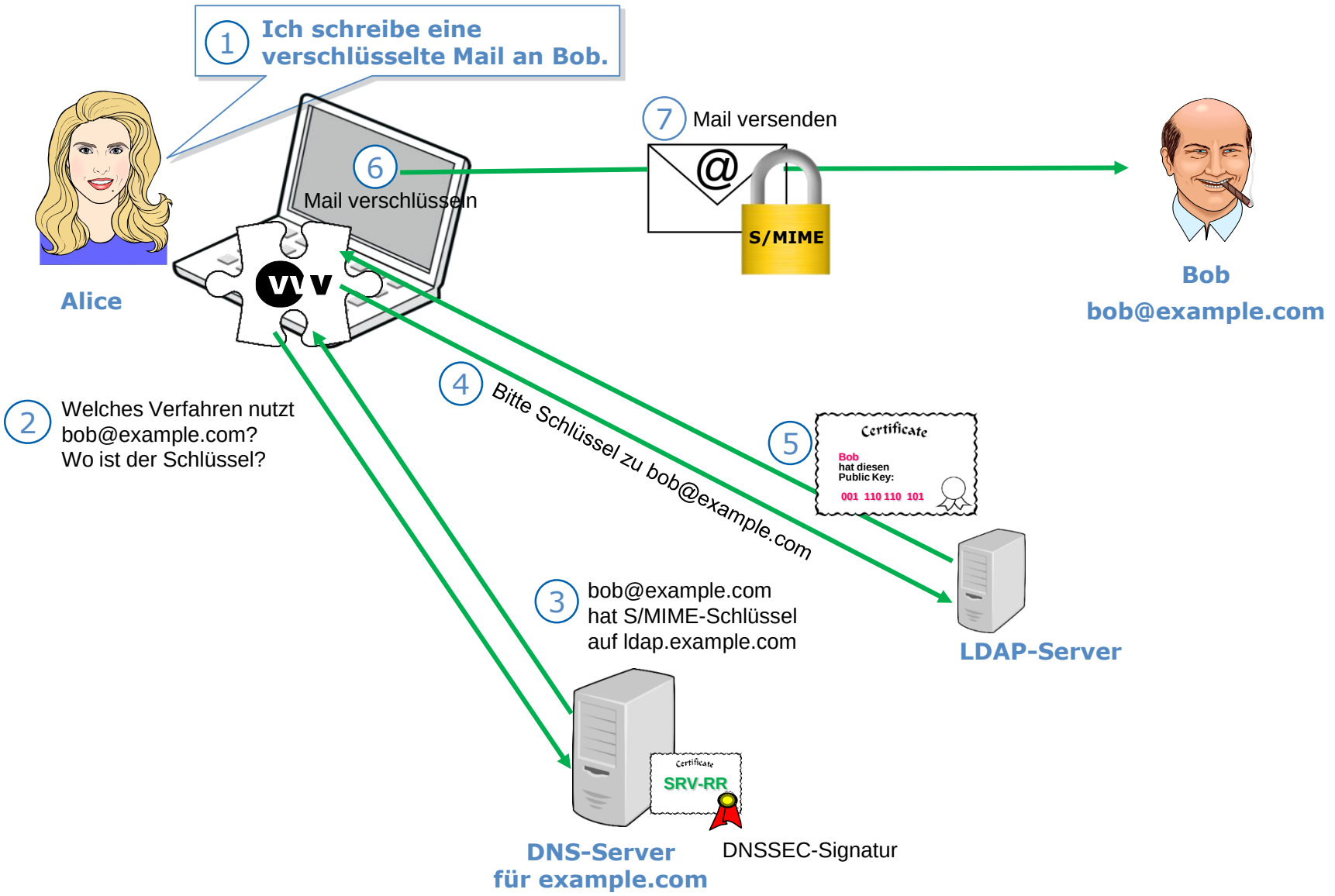
4. Wie findet man die Schlüssel der Kommunikationspartner?

(deren Schlüssel nicht von der Volksverschlüsselung zertifiziert sind)



- **Lösungsansatz**
  - Der Mail-Provider veröffentlicht einen Schlüssel auf Weisung des Nutzers.
  - Der DNS-Server der Mail-Domain sagt authentisch, wo der Schlüssel veröffentlicht ist.

Ideen zum Schlüsseltausch



Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

- **Laufzeit** April 2016 bis April 2018 (2 Jahre)
- **Schwerpunkt** Selbstbestimmt und sicher in der digitalen Welt
- **Konsortium** UdK Berlin, Fraunhofer SIT, mailbox.org, Uni Kassel, ULD

Gefördert vom Bundesministerium für Bildung und Forschung

Design Research Lab

Fraunhofer SIT

mailbox.org damit Privates privat bleibt

provet Projektgruppe verfassungsverträgliche Technikgestaltung

ULD

- **Lösungsanforderungen** (Auswahl)
  - Einfachheit: Die Kenntnis der E-Mail-Adresse soll ausreichen.
  - Privatsphäre: Nur die absolut notwendigen Daten sollen vorgehalten werden.
  - Authentizität: Die DNSSEC-Infrastruktur soll genutzt werden.

Fazit

- Die Verschlüsselung macht Fortschritte.
- Mangelnde Benutzbarkeit wurde als Haupthinderungsgrund erkannt.
- Es gibt viele Initiativen, alle sind gut.
- Die weitere Verbreitung von Ende-zu-Ende Verschlüsselung ist notwendig.

Volksverschlüsselung®

- **Volksverschlüsselung (VV)** hilft bei der eigenen Schlüsselgenerierung und Integration in die Anwendungen.

- **Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln (VVV)** wird bei der Suche nach Schlüsseln der Kommunikationspartner helfen.

Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Cloud Computing, Identity & Privacy
Rheinstraße 75, 64295 Darmstadt

Ulrich Waldmann

E-Mail ulrich.waldmann@sit.fraunhofer.de
Telefon +49 6151 869 222

www.sit.fraunhofer.de
www.volksverschluesselung.de
www.keys4all.de

CRISP
Center for Research
in Security and Privacy

Fraunhofer
SIT