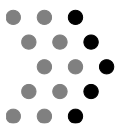

E-Mail-Verschlüsselung für Behörden und Unternehmen - Volksverschlüsselung und Ideen zum Schlüsseltausch

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?**



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.

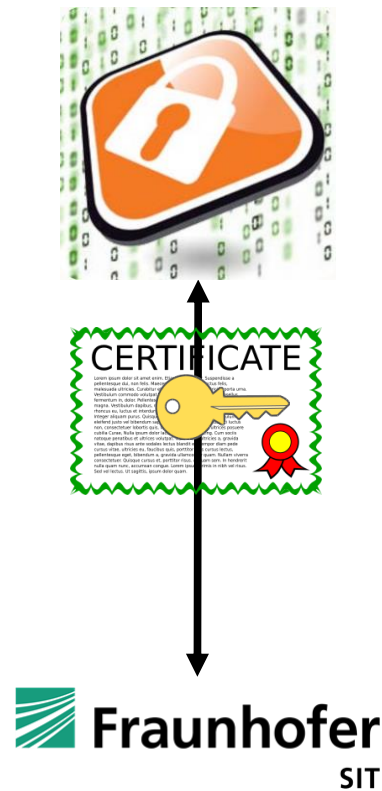


Volksverschlüsselung[®] – Features

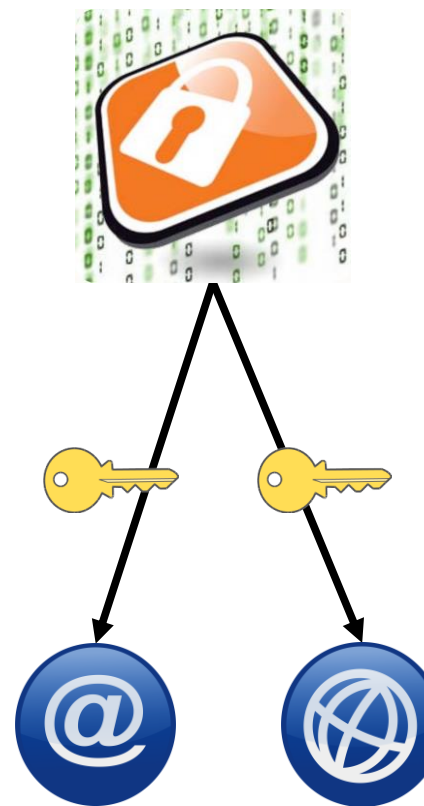
1. **VV-Software** unterstützt Identifizierung und erzeugt Schlüssel



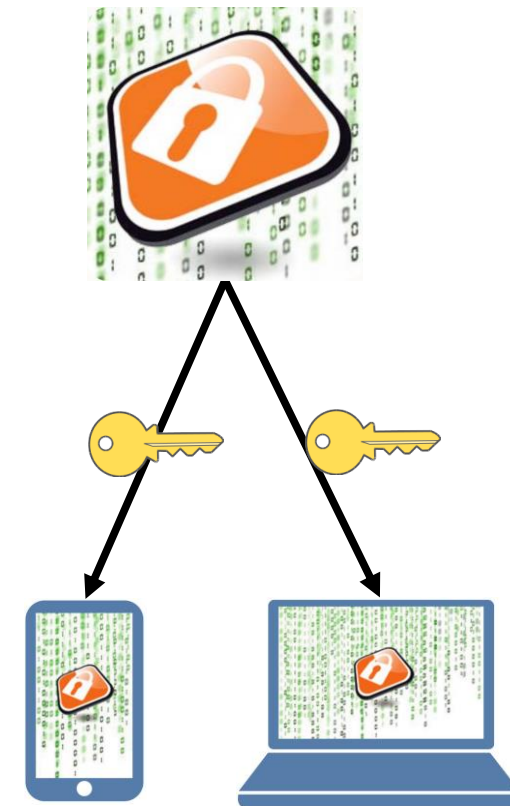
2. **VV-Software** lässt die Schlüssel zertifizieren



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



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



Volksverschlüsselung[®] – Hauptmenü

The screenshot shows the main menu of the Volksverschlüsselung application. The window title is 'Volksverschlüsselung' and the menu item is 'Hauptmenü'. The interface includes a sidebar with navigation icons (Home, Hauptmenü, Application Start, Action Selection, Settings, Help, Refresh, Info) and a main content area with a welcome message and three action buttons: 'Neues Zertifikat', 'Computer konfigurieren', and 'Zertifikatsverwaltung'. A notification bar indicates that the user has 4 certificates. The footer contains logos for Fraunhofer SIT and the copyright notice '© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie'.

Volksverschlüsselung

Hauptmenü

Herzlich willkommen! Möchten Sie jetzt ein neues Zertifikat beantragen, Ihre lokalen Anwendungen zur Nutzung Ihres Zertifikats konfigurieren oder Ihre vorhandenen Zertifikate verwalten?

Hinweis: Sie verfügen bereits über 4 Zertifikat(e). Ihre lokalen Zertifikate können jetzt eingerichtet oder verwaltet werden...

Bitte die gewünschte Aktion auswählen:

- Neues Zertifikat**
Einen neues Zertifikat beantragen oder eine laufende Beantragung fortsetzen
- Computer konfigurieren**
Richtet die Anwendungen auf dem Computer zur Verwendung Ihres Zertifikats ein
- Zertifikatsverwaltung**
Zertifikate Importieren bzw. Exportieren (Backup) oder ein Zertifikat widerrufen

Fraunhofer SIT

© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie

Weiter →

The screenshot shows a web browser window titled "Volksverschlüsselung" with a "CreateCert/SetAuthMethod" tab. The main content area is titled "Identitätsnachweis" and contains the instruction: "Bitte wählen Sie eine der verfügbaren Methoden zum Nachweis Ihrer Identität:". Three options are presented in grey boxes:

- Personalausweis**: Identitätsnachweis mit der Online-Ausweisfunktion des Personalausweises
- Telekom Login**: Identitätsnachweis mit Ihrem Benutzerkonto der Deutschen Telekom
- Registrierungscode**: Identitätsnachweis mit dem von uns erhalten 12-stelligen Registrierungscode

The left sidebar contains a navigation menu with the following items:

- Home icon: **Neues Zertifikat**
- Checkmark icon: **Vorbereitung**
 - ✓ Einführung
 - ➔ Methode auswählen
- Gear icon: **Identitätsnachweis**
 - Identifikation
 - E-Mail-Adresse wählen
 - Verifikationscode
- Question mark icon: **Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

The footer of the application window includes the Fraunhofer SIT logo, the text "© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie", and a "Weiter" button with a right-pointing arrow.

The screenshot shows a web browser window titled "Volksverschlüsselung" with a sub-header "CreateCert/SetAuthMethod". The main content area is titled "Identitätsnachweis" and contains the instruction: "Bitte wählen Sie eine der verfügbaren Methoden zum Nachweis Ihrer Identität:". Three options are listed in a vertical stack:


- Personalausweis**: Identitätsnachweis mit der Online-Ausweisfunktion des Personalausweises. This option is highlighted with a blue background and a green checkmark icon.
- Telekom Login**: Identitätsnachweis mit Ihrem Benutzerkonto der Deutschen Telekom.
- Registrierungscode**: Identitätsnachweis mit dem von uns erhalten 12-stelligen Registrierungscode.

The left sidebar contains a navigation menu with the following items:

- Home icon: **Neues Zertifikat**
- Medal icon: **Vorbereitung**
 - Einführung
 - Methode auswählen
- Download icon: **Identitätsnachweis**
 - Identifikation
 - E-Mail-Adresse wählen
 - Verifikationscode
- Question mark icon: **Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

The footer of the application window includes the Fraunhofer SIT logo, the text "© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie", and a "Weiter" button with a right-pointing arrow.

Identitätsnachweis



Angefragte Daten

Anbieter: Der Anbieter Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. fordert folgende Daten von Ihnen an:

Angefragte Daten

PIN-Eingabe

Bearbeitung

Zugriff auf:

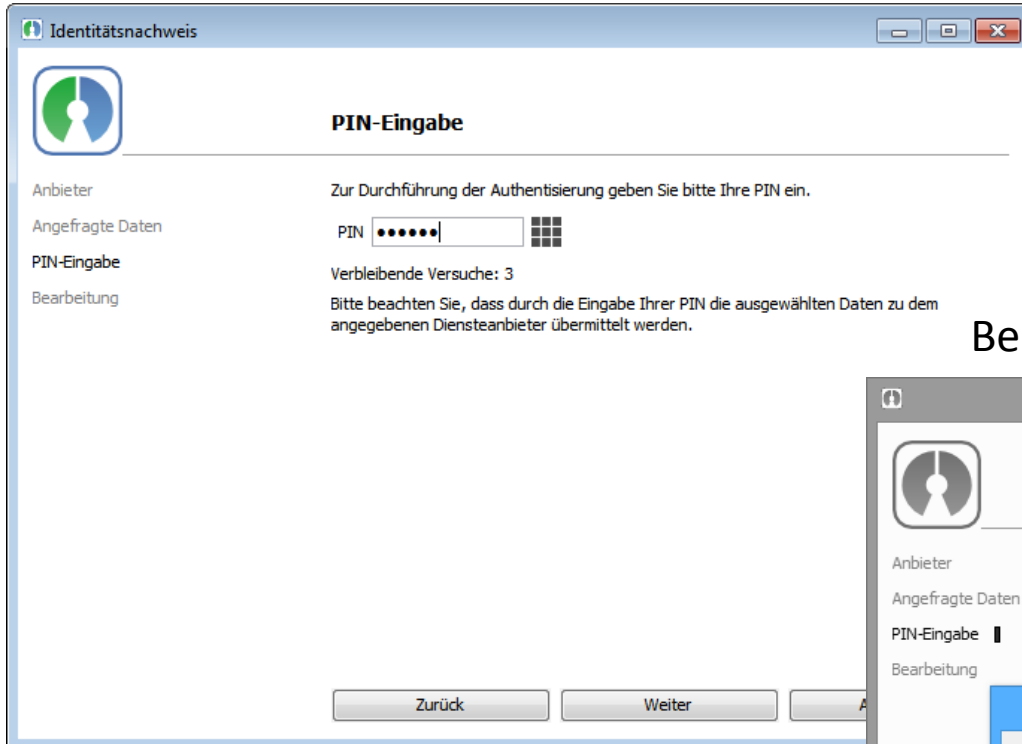
Vorname(n) Familienname

Doktorgrad

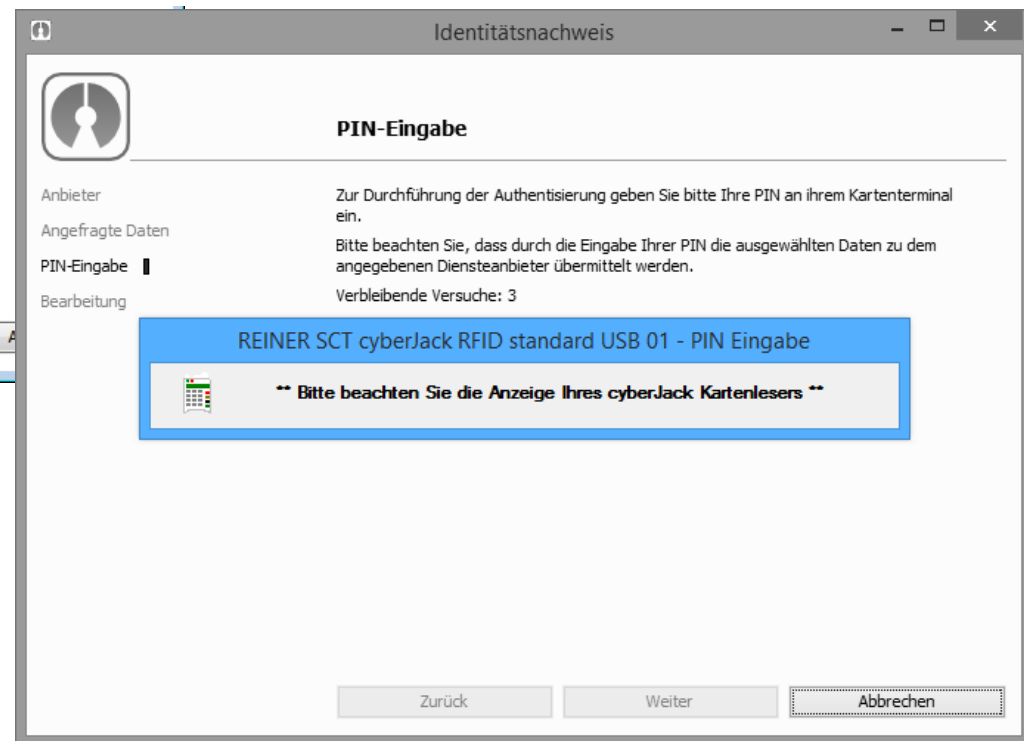
Hinweis
Die grau hinterlegten Elemente benötigt der Anbieter zur Durchführung seiner Dienstleistung. Optionale Daten können Sie nach Belieben an- bzw. abwählen.

Zurück Weiter Abbrechen

Bei Nutzung eines Basislesers (ohne Tastatur)



Bei Nutzung eines Standardlesers (mit Tastatur)



The screenshot shows a web browser window titled "Volksverschlüsselung". The main content area is titled "Identitätsnachweis" and contains the instruction: "Bitte wählen Sie eine der verfügbaren Methoden zum Nachweis Ihrer Identität:". There are three selection options:

- Personalausweis**: Identitätsnachweis mit der Online-Ausweisfunktion des Personalausweises
- Telekom Login**: Identitätsnachweis mit Ihrem Benutzerkonto der Deutschen Telekom (This option is highlighted in blue and has a green checkmark icon on the right).
- Registrierungscode**: Identitätsnachweis mit dem von uns erhalten 12-stelligen Registrierungscode

The left sidebar contains a navigation menu with the following items:

- Home icon: **Neues Zertifikat**
- Medal icon: **Vorbereitung**
 - Einführung
 - Methode auswählen
- Download icon: **Identitätsnachweis**
 - Identifikation
 - E-Mail-Adresse wählen
 - Verifikationscode
- Question mark icon: **Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

At the bottom of the window, there are logos for Fraunhofer SIT and Deutsche Telekom, the copyright notice "© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie", and a "Weiter" button with a right-pointing arrow.

The screenshot shows a web browser window titled 'Volksverschlüsselung' with a sub-header 'Auth/Telekom'. The main heading is 'Identitätsnachweis mit Telekom-Login'. Below the heading, there is a paragraph: 'Bitte geben Sie zu diesem Zweck den Login-Namen sowie das zugehörige Passwort Ihres Telekom-Kontos ein. Hierbei kann ausschließlich der jeweilige Hauptbenutzer akzeptiert werden!' followed by a 'Hinweis: Im Rahmen des Identitätsnachweises werden ausschließlich Anrede, Vor- und Nachname sowie ggf. die E-Mail-Adresse aus Ihrem Telekom-Kundenkonto an uns übermittelt.' The form contains two input fields: 'Login-Name eingeben:' with the value 'ulrich.waldmann@t-online.de' and 'Passwort eingeben:' with masked characters. A 'Vergessen?' link is next to the password field. A 'Weiter' button with a right arrow is at the bottom right. A sidebar on the left shows navigation options: 'Neues Zertifikat', 'Vorbereitung' (with 'Einführung' and 'Methode auswählen' checked), 'Identitätsnachweis' (with 'Identifikation' selected), and 'Beantragung' (with 'Antrag abschicken', 'Zertifikatserstellung', and 'Herunterladen' as options). The footer includes the Fraunhofer SIT logo and copyright information '© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie'.

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

The screenshot shows a web browser window titled "Volksverschlüsselung". The main content area is titled "Identitätsnachweis" and contains the instruction: "Bitte wählen Sie eine der verfügbaren Methoden zum Nachweis Ihrer Identität:". There are three selection options:

- Personalausweis**: Identitätsnachweis mit der Online-Ausweisfunktion des Personalausweises
- Telekom Login**: Identitätsnachweis mit Ihrem Benutzerkonto der Deutschen Telekom
- Registrierungscode**: Identitätsnachweis mit dem von uns erhaltenen 12-stelligen Registrierungscode (This option is highlighted with a blue background and a green checkmark icon).

The left sidebar contains a navigation menu with the following items:

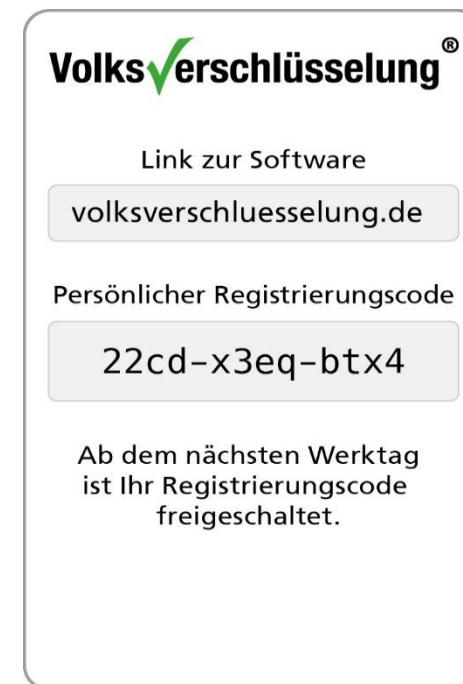
- Home icon
- Neues Zertifikat**
- Vorbereitung**
 - Einführung
 - Methode auswählen
- Identitätsnachweis**
 - Identifikation
 - E-Mail-Adresse wählen
 - Verifikationscode
- Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

The footer of the application window includes the logos for Fraunhofer SIT and Deutsche Telekom, the copyright notice "© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie", and a "Weiter" button with a right-pointing arrow.

Volksverschlüsselung[®] – Registrierungscode

- **Ausgabe des Registrierungscode**
 - 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



The screenshot shows a web browser window titled "Volksverschlüsselung" with a "Auth/FaceToFace" indicator in the top right corner. The main heading is "Identitätsprüfung mittels Registrierungscode". Below this, instructions state: "Schließen Sie die Vor-Ort Identitätsprüfung durch das Einlösen Ihres Registrierungscode ab. Bitte geben Sie zu diesem Zweck Ihren zwölfstelligen Registrierungscode, der sich auf der Rückseite Ihrer Registrierungskarte befindet, sowie die dazugehörige E-Mail-Adresse ein!".

The left sidebar contains a navigation menu with the following items:

- Home icon
- Neues Zertifikat**
- Vorbereitung**
 - Einführung
 - Methode auswählen
- Authentifizierung**
 - Identifikation
 - E-Mail-Adresse wählen
 - Verifikations-Code
- Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

The main content area features a small image of the registration card, a text input field for the "E-Mail-Adresse eingeben:" containing "ulrich.waldmann.01@vv.sit.fraunhofer.de", and a registration code input field for "Registrierungscode eingeben:" containing "VZ26 - SWNI - 5CMW". A prominent instruction reads: "Klicken Sie auf 'Weiter', um dem Registrierungscode einzulösen!". A "Weiter" button with a right-pointing arrow is located at the bottom right of the interface.

Volksverschlüsselung[®] – Auswahl der E-Mail-Adresse

The screenshot shows the 'Volksverschlüsselung' web application interface. The title bar reads 'Volksverschlüsselung' and 'CreateCert/SelectEmail'. The main heading is 'E-Mail-Adresse'. Below it, the text says: 'Bitte wählen Sie jetzt Ihre E-Mail-Adresse, für die Sie ein neues Zertifikat beantragen möchten.' The section 'E-Mail-Adresse auswählen:' contains a list of email addresses with selection radio buttons:

- ulrich.waldmann.01@vv.sit.fraunhofer.de**
Ulrich Waldmann 01
- ulrich.waldmann.02@vv.sit.fraunhofer.de**
Waldmann, Ulrich
- ulrich.waldmann@sit.fraunhofer.de**
Ulrich Waldmann
- ulrich.waldmann.03@vv.sit.fraunhofer.de**
Waldmann, Ulrich

Below the list is a link: 'Eine andere E-Mail-Adresse verwenden (manuelle Eingabe)'. The left sidebar shows the progress: 'Neues Zertifikat' (selected), 'Vorbereitung' (Einführung, Methode auswählen), 'Authentifizierung' (Identifikation, E-Mail-Adresse wählen, Verifikations-Code), and 'Beantragung' (Antrag abschicken, Zertifikatserstellung, Herunterladen). The bottom footer includes the Fraunhofer SIT logo, copyright '© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie', and a 'Weiter' button with a right arrow.

Volksverschlüsselung[®] – Prüfung der E-Mail-Adresse

The screenshot shows a web browser window titled "Volksverschlüsselung" with a sub-tab "CreateCert/ValidateEmail". The main heading is "Verifikations-Code". The text explains that a verification code has been sent to the user's email and that they should enter it in the provided field. Below the text is a text input field containing the code "OV7UK".

Verifikations-Code

Ein Verifikations-Code wurde an Ihre E-Mail-Adresse gesendet. Sobald Sie die Bestätigungs-Mail erhalten haben, geben Sie den 5-stelligen Code in das Eingabefeld ein.

Falls Sie die Bestätigungs-Mail nicht innerhalb von 5 Minuten erhalten, überprüfen Sie bitte die angegebene E-Mail-Adresse und sehen Sie auch in Ihrem „Spam“ Ordner nach.

Verifikations-Code eingeben:

OV7UK

Neues Zertifikat

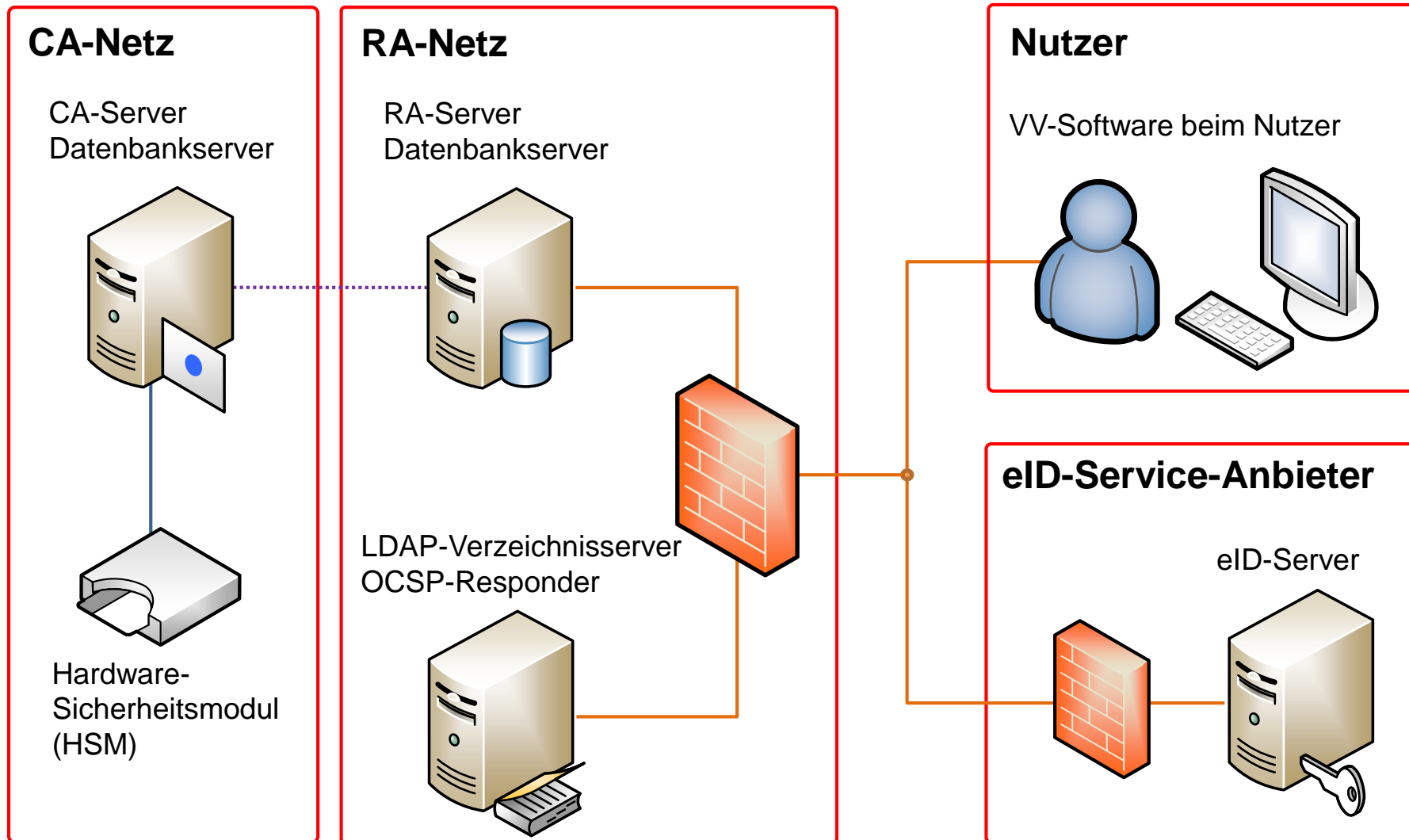
- Vorbereitung**
 - ✓ Einführung
 - ✓ Methode auswählen
- Authentifizierung**
 - ✓ Identifikation
 - ✓ E-Mail-Adresse wählen
 - ➔ Verifikations-Code
- Beantragung**
 - Antrag abschicken
 - Zertifikatserstellung
 - Herunterladen

Fraunhofer SIT © 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie Weiter

Volksverschlüsselung[®] – Auswahl der Anwendungen

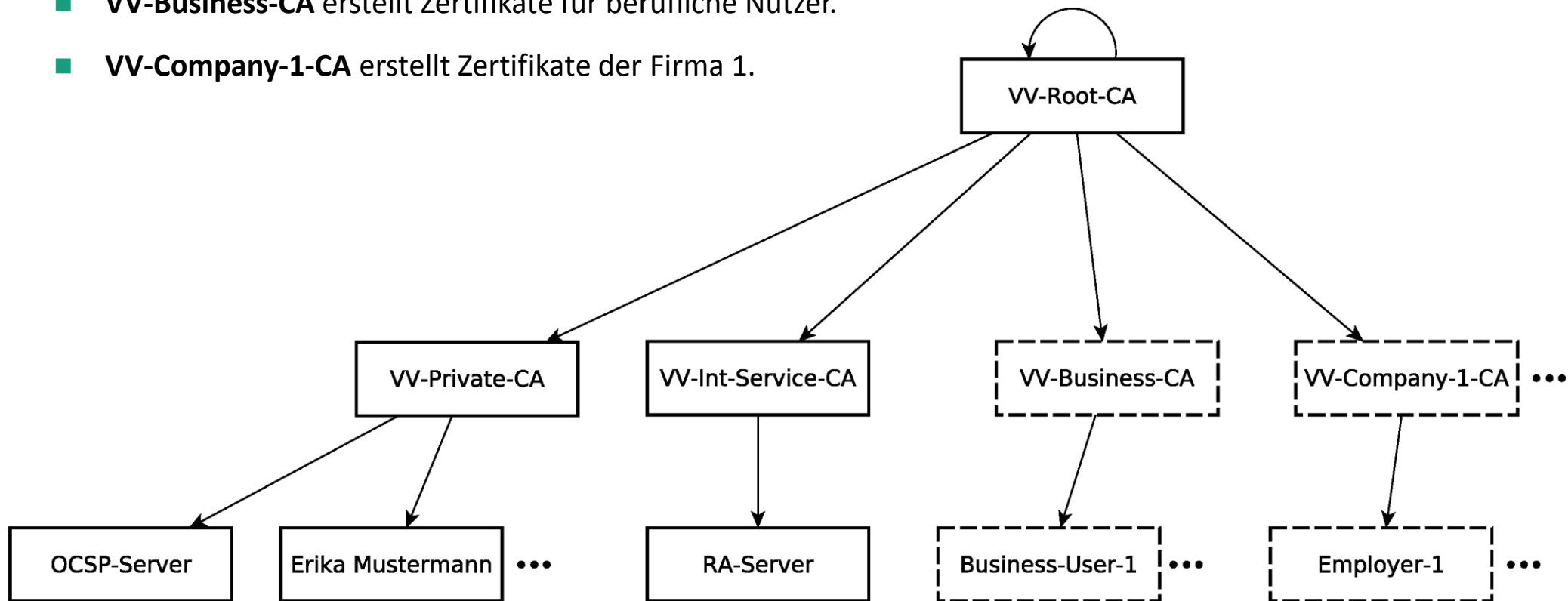
The screenshot shows a software window titled "Volksverschlüsselung" with a sub-window "SetupPC/Step1/ChooseApps". The main heading is "Anwendungen auswählen". Below it, a message reads: "Bitte wählen Sie die Programme aus, in denen Sie Ihr Zertifikat verfügbar machen möchten." A green progress bar indicates that 6 supported applications have been found. The interface is divided into three columns: "E-Mail-Programme:", "Web-Browser:", and "Web-Mail-Dienste:". Under "E-Mail-Programme:", there are three items: "Microsoft Outlook", "Mozilla Thunderbird", and "SeaMonkey Suite", each with a checked checkbox. Under "Web-Browser:", there are three items: "Google Chrome", "Internet Explorer", and "Mozilla Firefox", each with a checked checkbox. The "Web-Mail-Dienste:" column is empty and contains a placeholder message: "Wird demnächst verfügbar sein." At the bottom of the application selection area, there are links for "Alle auswählen" and "Keine auswählen", and a status indicator "6/6 Programme gewählt". A "Weiter" button with a right-pointing arrow is located at the bottom right of the window. The left sidebar contains navigation icons and the text "Computer einrichten" and "Zertifikate installieren". The footer of the window includes the Fraunhofer SIT logo, the copyright notice "© 2015-2016 Fraunhofer-Institut für Sichere Informationstechnologie", and the Fraunhofer logo.

Volksverschlüsselung[®] – Infrastruktur

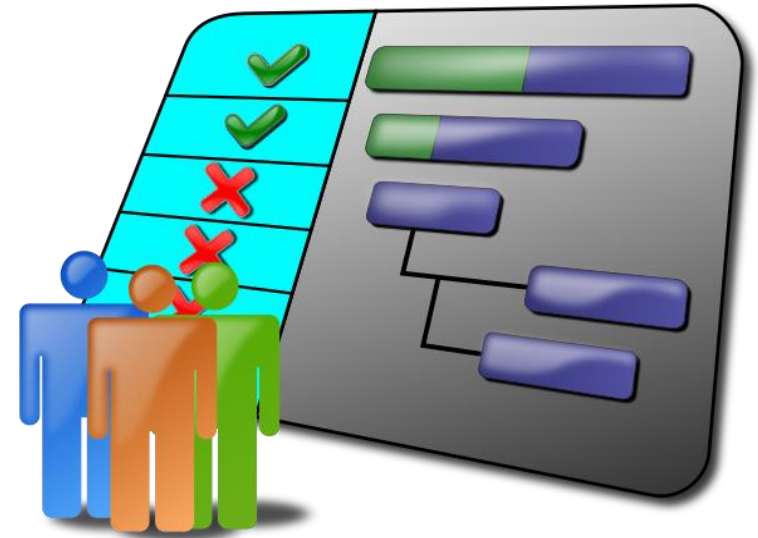


Volksverschlüsselung[®] – Zertifizierungshierarchie

- **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.



- Integration von OpenPGP und WebMail
- Identifikation mit existierenden Schlüsseln
- Identifikation über ein Bezahlungssystem
- 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.

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

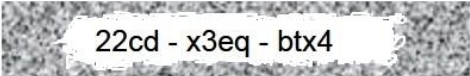



3. Wie können Firmen / Behörden Kunden und Bürger mit Schlüsseln versorgen?

■ Lösung durch Volksverschlüsselung

- (1) Firma erhält n Registrierungscode, 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.

1. Besuchen Sie www.volksverschlueselung.de und laden Sie sich die VV-Software herunter.
2. Rubbeln Sie auf dieser Karte den Registrierungscode frei.
3. Starten Sie die VV-Software und wählen Sie den Identitätsnachweis "Registrierungscode".
4. Geben Sie den Registrierungscode in die VV-Software ein.

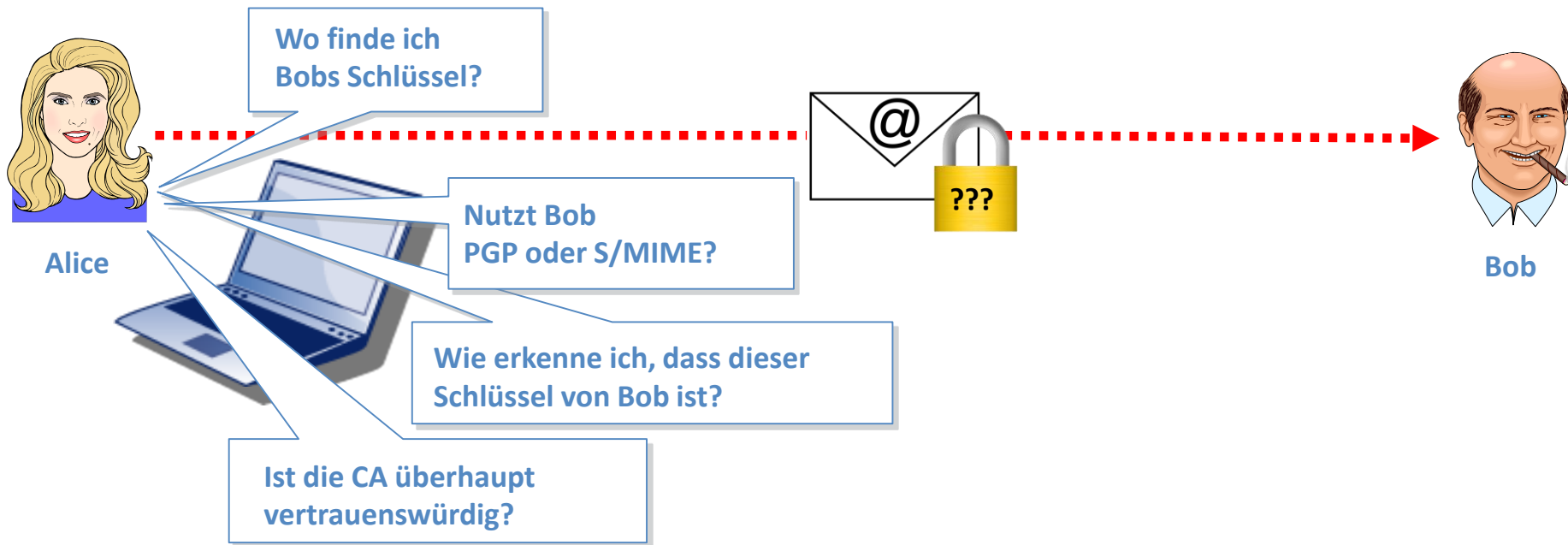


22cd - x3eq - btx4

Ideen zum Schlüsseltausch

4. Wie findet man die Schlüssel der Kommunikationspartner?

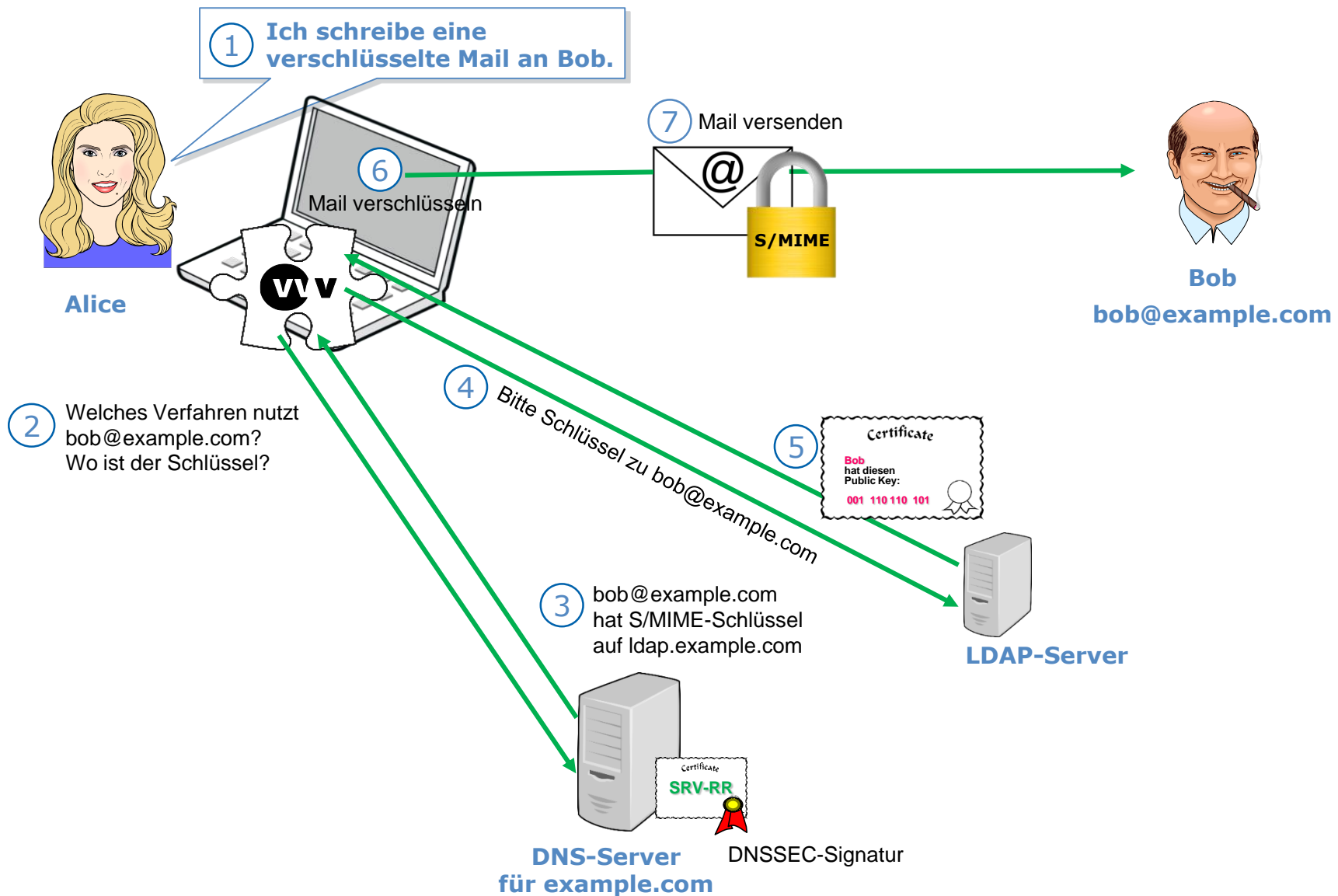
(deren Schlüssel nicht von der Volksverschlüsselung zertifiziert sind)



■ 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



Design
Research
Lab



■ 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.

Volks✓verschlüsselung[®]

- **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