Die Volksverschlüsselung®

Registrierung von Bürgern in den Meldeämtern

13.12.2017 - Bonn

Fraunhofer SIT

Partner in CRISP Center for Research in Security and Privacy

Inhalt

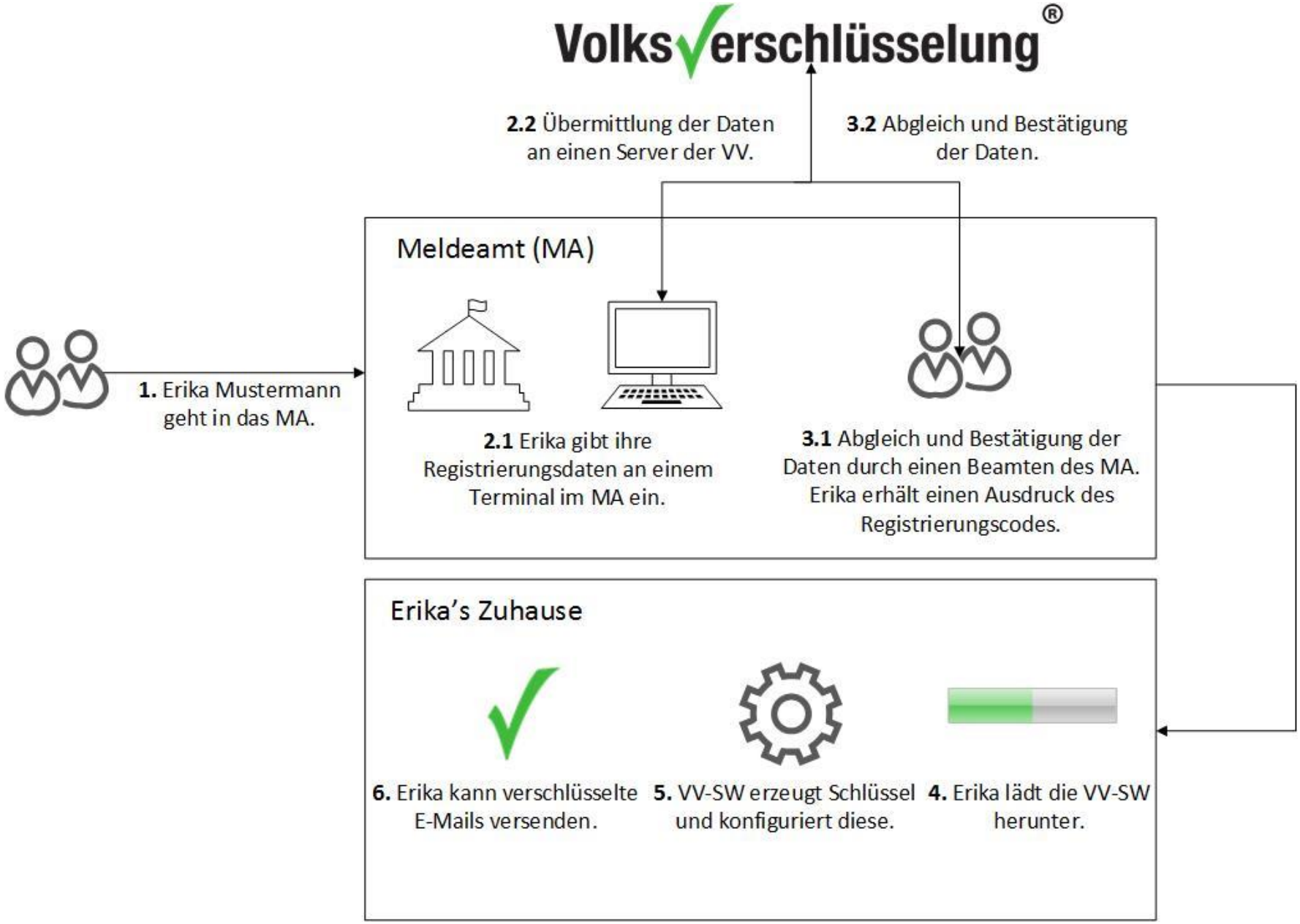
- Motivation
- Die Volksverschlüsselung
- Registrierungsprozess in den Meldeämtern
  - Organisatorischer Prozess (Meldeamt)
  - Technischer Prozess (eID/SID-Box)

Motivation

- Unverschlüsselte E-Mails sind von allen mit Zugriff auf den Kommunikationskanal einsehbar
- Sichere kryptographische Ansätze existieren schon lange, scheidern aber an der Gebrauchstauglichkeit
- 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

Die Volksverschlüsselung

- Setzt den Fokus auf Gebrauchstauglichkeit / den Laien
- Erzeugt idenditätsgeprüfte Zertifikate zur Ende-zu-Ende Verschlüsselung und digitalen Signatur
  - Personalausweis (eID), Telekom Login, FhG SmartCard, Registrierungscode
- Funktioniert mit allen gängigen E-Mail-Clients (S/MIME)
- Betreibt eine eigenständige PKI / Server-Infrastruktur
- Bietet Windows-Anwendung (VV-SW) für Endnutzer
  - Automatisiert und unterstützt alle Prozesse so weit wie möglich
  - Erkennt installierte lokale Anwendungen und konfiguriert diese
    - Outlook, Thunderbird, Firefox, Chrome, IE, usw.
- Kostenlos für Privatanwender


Volksverschlüsselung®
2.2 Übermittlung der Daten an einen Server der VV.
3.2 Abgleich und Bestätigung der Daten.
Meldeamt (MA)
1. Erika Mustermann geht in das MA.
2.1 Erika gibt ihre Registrierungsdaten an einem Terminal im MA ein.
3.1 Abgleich und Bestätigung der Daten durch einen Beamten des MA. Erika erhält einen Ausdruck des Registrierungscodes.
Erika's Zuhause
6. Erika kann verschlüsselte E-Mails versenden.
5. VV-SW erzeugt Schlüssel und konfiguriert diese.
4. Erika lädt die VV-SW herunter.

Registrierungsprozess in den Meldeämtern
Allgemeiner Prozess - Zusammenfassung

- Bürger erfasst seine Registrierungsdaten an einem Terminal im Meldeamt
  - Vorname(n), Nachnamen, E-Mail Adresse, opt. akademischer Grad
  - Die Datenspeicherung erfolgt auf Servern der Volksverschlüsselung
  - Die Behörde und SIT haben einen Auftragsdatenverarbeitungsvertrag
- Bürger wendet sich an einen Mitarbeiter der Behörde und zeigt ihren Personalausweis vor. Autorisierte Mitarbeiter der Behörde können die Registrierungsdaten einsehen, abgleichen und bestätigen.
- Mitarbeiter der Behörde druckt den zeitlich limitierten Registrierungscode aus und überreicht ihn dem Bürger.
- Die Prozessbeteiligung des Meldeamtes ist beendet, es fallen keine administrative Aufgaben oder Verantwortlichkeiten an.

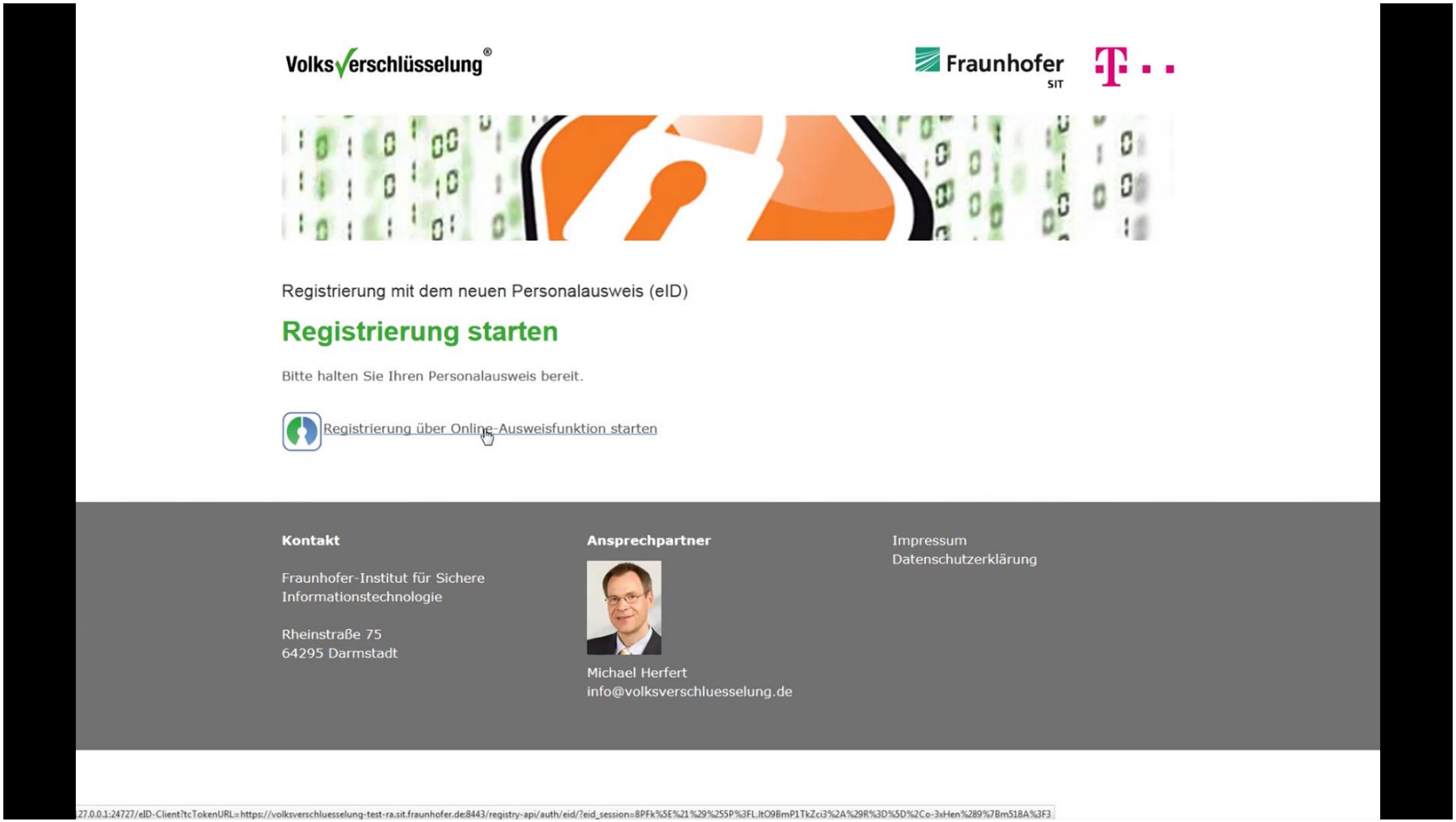
Registrierungsprozess in den Meldeämtern
Allgemeiner Prozess - Zusammenfassung

- Bürger bezieht Volksverschlüsselungs-Software (VV-SW) von Servern der Volksverschlüsselung
- Bürger Registriert sich mit zuvor auf dem Meldeamt erhaltenen Registrierungscode
- Die VV-SW…
  - erzeugt lokal kryptographsiche Schlüssel
  - zertifiziert diese zusammen mit Registrierungdaten
  - konfiguriert die detektierten und gewünschten Client-Anwendungen automatisch

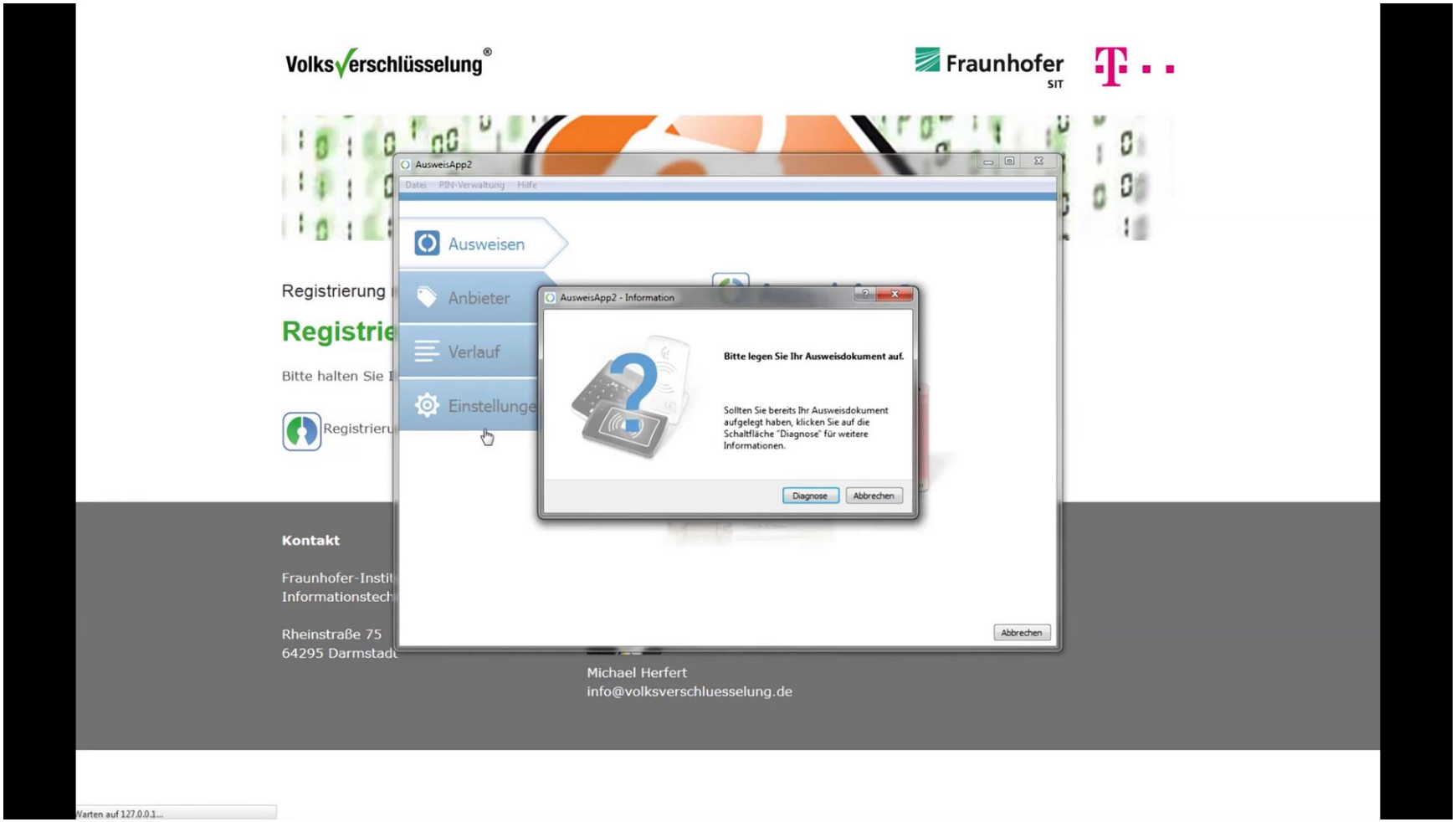
Registrierungsprozess in den Meldeämtern
Über die SID-Box und den nPA

- Web-Frontend zur Ausstellung von Registrierungscodes auf Basis des neuen Personalausweises
  - Wird z.B. auf SID-Box betrieben
- Registrierungscodes können als PDF herunter geladen werden (USB-Stick)
- Web-Frontend aktuell noch nicht online
- Demo / Screencast: Link

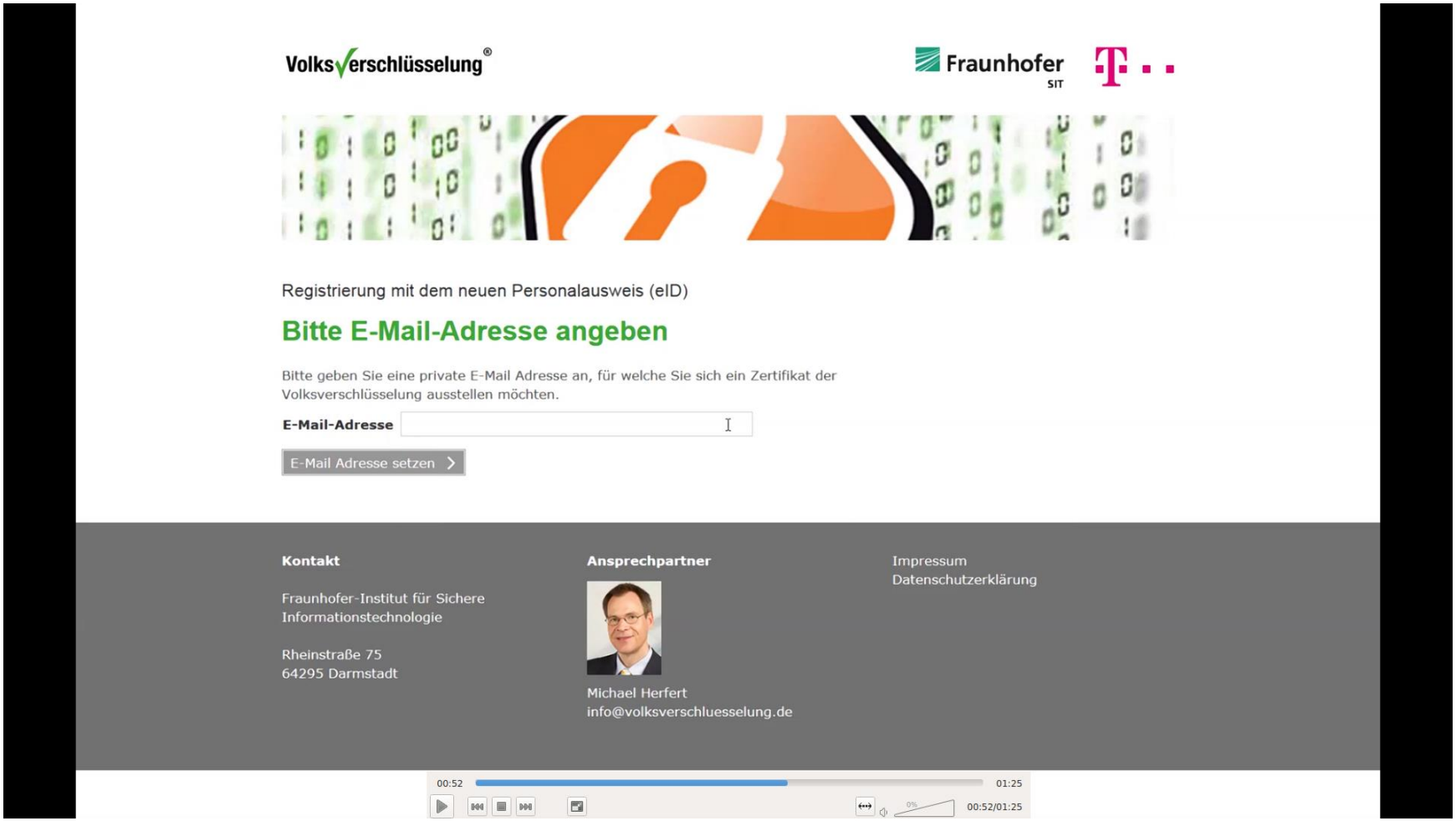
Registrierungsprozess in den Meldeämtern
Über die SID-Box und den nPA



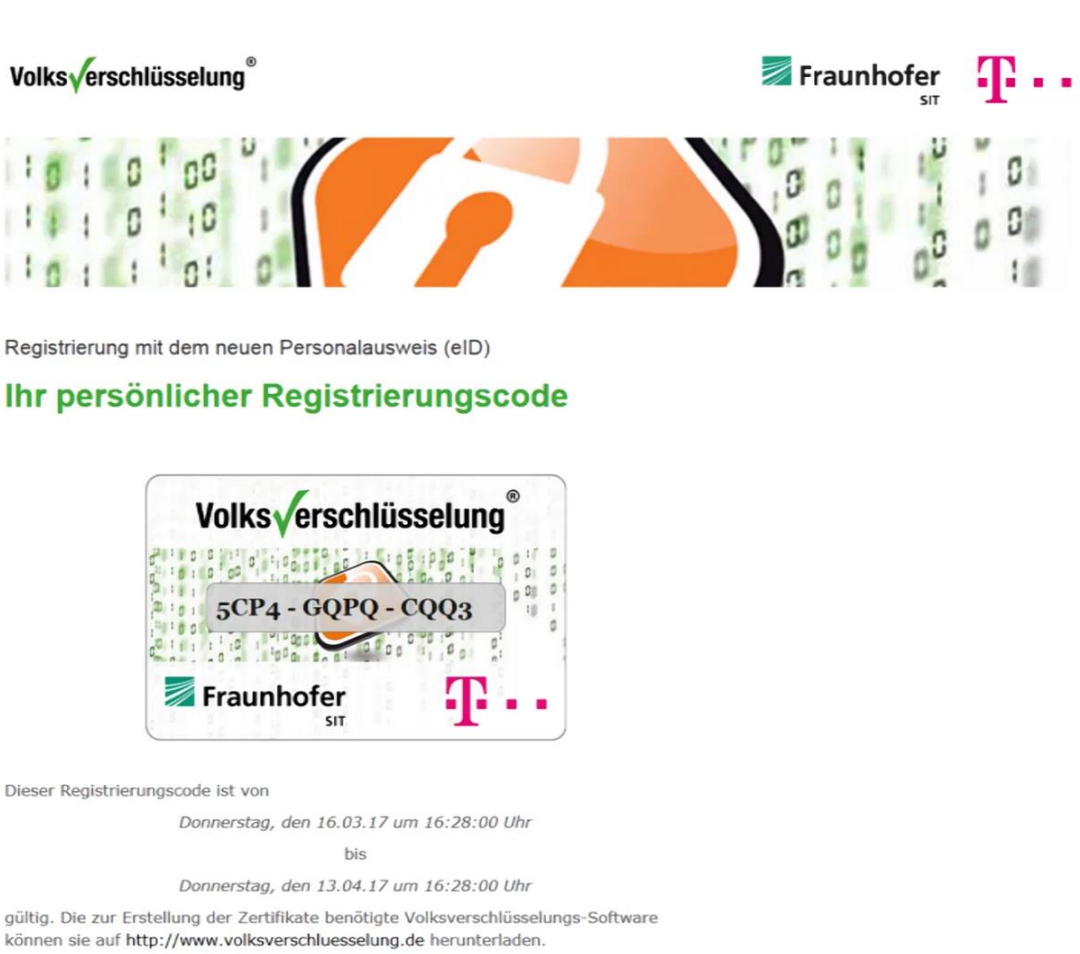
Registrierungsprozess in den Meldeämtern
Über die SID-Box und den nPA



Registrierungsprozess in den Meldeämtern
Über die SID-Box und den nPA



Registrierungsprozess in den Meldeämtern
Über die SID-Box und den nPA



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

Abgrenzung zu De-Mail

- De-Mail-Anbieter müssen akkreditiert sein
- De-Mail authentifiziert die Teilnehmer bevor sie an De-Mail teilnehmen dürfen
- Zusätzlich: De-Ident, De-Safe
- Kanalverschlüsselung zwischen den Anbietern
- De-Mail-Gesetz
  - Rechtsverbindliche Kommunikation
- Versandoptionen wie bei Briefen möglich
  → Ersatz für Briefe
- Einmalige Einrichtegebühr + Versandkosten je nach Versandoption
- Konfliktfreie Ko-Existenz mit Volksverschlüsselung