Die Fraunhofer-Smartcard und ihre Anwendungen

Konzeption, Aufbau und Betrieb einer PKI am Beispiel der Fraunhofer Gesellschaft

GI SECMGT Workshop

„Digital Identitäten / Identitätsmanagement“

15. Juni 2012, Frankfurt

Uwe Bendisch

Fraunhofer-Institut SIT

Fraunhofer Competence Center PKI

Fraunhofer SIT

Inhalte und Gliederung

- Fraunhofer und das Fraunhofer Competence Center PKI
- Der Weg zur heutigen Fraunhofer-PKI
- Die Fraunhofer-Smartcard und ihre PKI-Anwendungen
- Zusammenfassung

Inhalte und Gliederung

- Fraunhofer und das Fraunhofer Competence Center PKI
- Der Weg zur heutigen Fraunhofer-PKI
- Die Fraunhofer-Smartcard und ihre PKI-Anwendungen
- Zusammenfassung

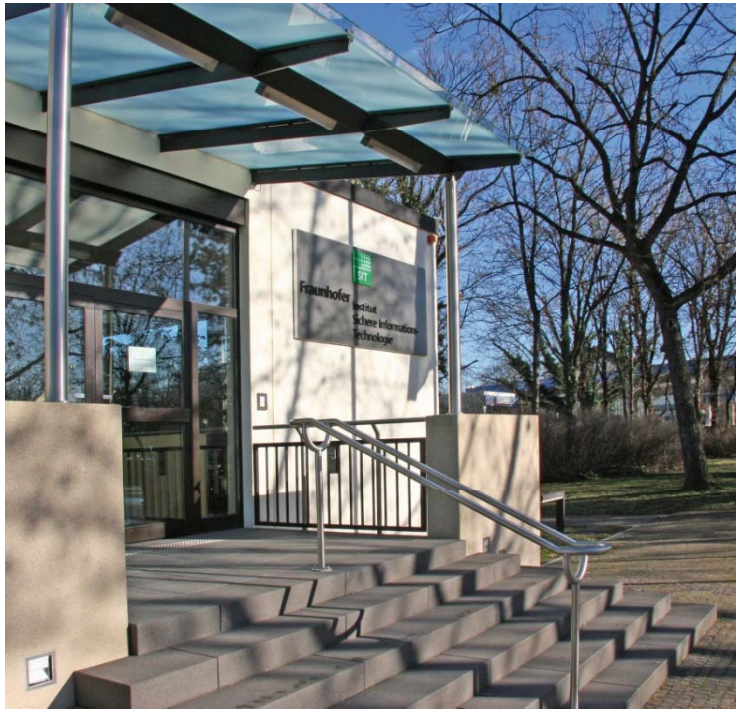
Fraunhofer SIT

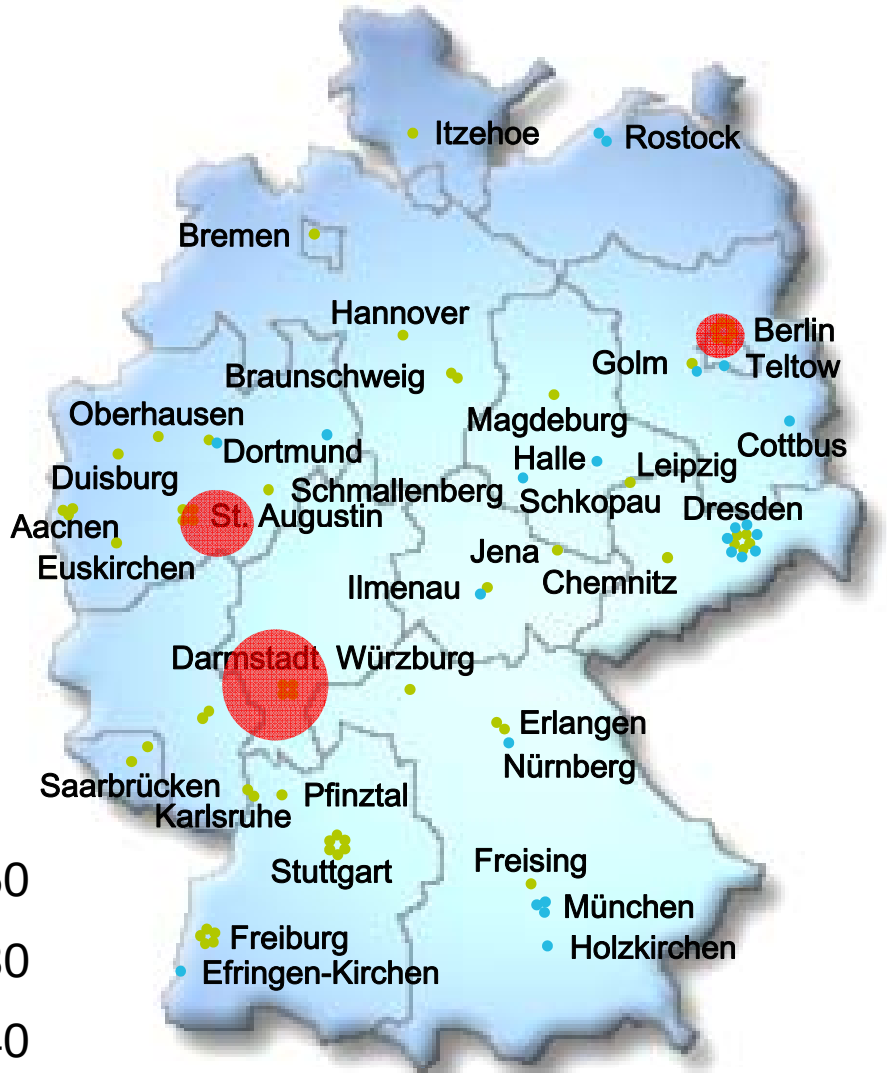
Fraunhofer-Gesellschaft

- Fraunhofer ist die führende Organisation für angewandte Forschung in Europa
- Sie betreibt anwendungsorientierte Forschung zum direkten Nutzen für Unternehmen und zum Vorteil der Gesellschaft
- 80 Forschungseinrichtungen weltweit (rund 40 Standorte in Deutschland)
- davon 60 Institute
- 20.000 Mitarbeiter
- Budget: 1,5 Mrd. €

Fraunhofer SIT

Fraunhofer-Institut für Sichere Informationstechnologie





- Leitung: Prof. Dr. Michael Waidner
  - Beschäftigte: 150
  - davon Wissenschaftler: 80
  - Wissenschaftliche Hilfskräfte: 40

Fraunhofer SIT

Fraunhofer Competence Center PKI (CC-PKI)

- Etabliert 2006 zur Einführung der neuen Fraunhofer-PKI / Smartcard
- Bündelung von Kompetenzen aus zwei Instituten
  - Fraunhofer SIT
  - Fraunhofer IOSB
- Zwei Standorte für Trustcenter
  - Sankt Augustin (SIT)
  - Karlsruhe (IOSB)
- Zentraler Ansprechpartner für die Fraunhofer-PKI

Fraunhofer SIT

Inhalte und Gliederung

- Fraunhofer und das Fraunhofer Competence Center PKI
- Der Weg zur heutigen Fraunhofer-PKI
- Die Fraunhofer-Smartcard und ihre PKI-Anwendungen
- Zusammenfassung

Fraunhofer SIT

Historie der Fraunhofer-PKI

- PKI ist seit über 15 Jahren in der FhG etabliert
  - zunächst auf PGP-Basis (ab ca. 1997)
  - seit 2003: eigene CA, die X.509-Softtoken für Mitarbeiter / Server ausstellt
  - Zunächst v. a. Zertifikate für Server, später Zertifikate für Mitarbeiter
- Stetig wachsende Anforderungen
  - Bessere Sicherheit, neue Technologien, mehr Anwendungsfälle und User
- Fortlaufenden Anpassung des PKI-Konzepts und der Technik
  - PKI ist gewachsen – mehrfach „umgebaut“ worden

Letzte Variante der „alten“ Fraunhofer-PKI (bis 2007)

- Zielgruppen:
  - Fraunhofer-Mitarbeiter (z. B. für sichere E-Mail)
  - **selbst beantragen** (dezentrale Schlüsselerzeugung, im Browser)
  - Server der Fraunhofer-Gesellschaft (z. B. Webserver)
  - Administratoren beantragen Zertifikate (**dezentrale Schlüsselerzeugung**)
- Sicherheitsniveau: mittel
  - Registrierungsstelle: Personen müssen persönlich erscheinen
  - **Softtoken**: Krypto-Schlüssel als Datei bei Benutzer/Server-Admin
  - gemeinsame Zertifizierungsstelle für Zertifikate von Mitarbeitern u. Servern
- Usability: verbesserbar
  - Wurzelzertifikat nicht standardmäßig im Browser/Betriebssystem enthalten
  - Signaturen/ Zertifikate nicht unmittelbar überprüfbar
  - Aufwand für FhG-externe Kommunikationspartner bei Signatur-Prüfung

Motivation der Fraunhofer-Gesellschaft

„Innensicht“

- Ziele der flächendeckenden PKI-Einführung:
  - "Elektronifizierung" von Geschäftsprozessen
  - starke Authentifizierung für Mitarbeiter-Portal
  - sichere elektronische Kommunikation
  - Minimierung von IT-Sicherheitsrisiken

„Außensicht“

- rechtliche Anforderungen
  - Datenschutz
  - Haftung
  - Revisionseignung der Verfahren
- Sensibilisierung durch Sicherheitsvorfälle
  - Trojaner-Attacken gegen öffentliche Einrichtungen
  - Informationsdiebstahl in Forschungseinrichtungen

Fraunhofer SIT

Ursachen für Sicherheitsprobleme

- Mangelnde Integration
- Security als Add-on statt Security Inside

- Mangelnde Usability
- Nutzung ist umständlich → Umgehen von Kontrollen

Fraunhofer SIT

Spannungsfeld Komplexität und Kosten einer PKI

- Komplexität einer PKI steigt, je…
  - **… heterogener das Umfeld** (technisch und organisatorisch)
  - FhG: Win, Unix, Mac; diverse Browser, Mail-Tools, Spezial-Anwendungen
  - Viele beteiligte Parteien mit komplexen Anforderungen
  - FhG: Zentrale, Institute aus unterschiedlichen Verbünden, Mitarbeiter, externe Kommunikationspartner
- Einsparpotential durch gute IST-Analyse
  - Schutzziele definieren
  - Anforderungen der beteiligten Parteien erheben und festlegen
  - **Nachträgliche Anpassungen** bedeuten **höhere Kosten**

Insbesondere…

„You can have easy, cheap or secure. Pick two …“

- Anwendungen mit mittleren bis hohen Sicherheitsanforderungen sind häufig
  - optimiert hinsichtlich Sicherheit und Kosten
  - optimierbar in ihrer Benutzerfreundlichkeit

Aber: Ziel muss die sinnvolle Gewichtung aller drei Anforderungen sein!

Fraunhofer SIT

Fraunhofer Anforderungen an eine neue PKI (2006)

Fraunhofer wählt fortgeschrittene Signaturen

- Hardwarebasiert
  - Multifunktionale Smartcards (Hybrid-Karten) und Lesegeräte für alle Institute & Mitarbeiter
- Sichere Registrierung
  - Prüfung von amtlichen Ausweisdokumenten
- Verlässliche ENTschlüsselung
  - Schlüsselhinterlegung (Key Recovery)
- Hohe Verfügbarkeit
  - Redundanz (Trustcenter an 2 Standorten)
- Integration mit bestehenden Anwendungen
  - Personalsystem, Corporate Directory
  - Jeder neue Mitarbeiter erhält „automatisch“ Smartcard
- Anerkennung im Außenraum

Fraunhofer SIT

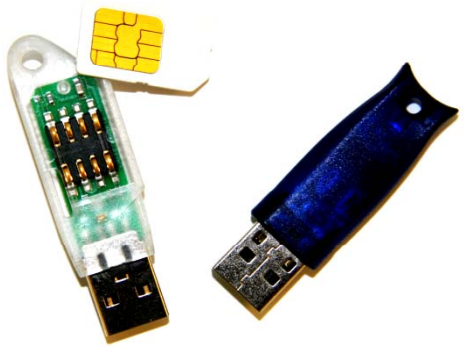
Vorstandsbeschluss: Einführung einer Smartcard

- Multifunktionskarte für ca. 20.000 User (Hybrid-Karte)
  - In allen Instituten und für alle Mitarbeiter
- PKI: 3 Schlüsselpaare und Zertifikate für
  - fortgeschrittene Signatur
  - Authentisierung
  - Verschlüsselung
- Mitarbeiterausweis im Corporate Design
- Sonderfunktionen in manchen Instituten
  - RFID, Magnetstreifen
  - Z. B. Zeiterfassung, Gebäudezugang, Bezahlen, Parken, Zugriffskontrolle…
- Einführung
  - Schrittweise in allen FhG Instituten und Einrichtungen (90% erreicht)

Fraunhofer SIT

Warum eine Smartcard-basierte Lösung / Hybrid-Karte?

- Hohe Sicherheit
  - Auslesen der Private Keys nicht möglich
    - → keine Gefahr von unberechtigter Nutzung
    - → in Softtoken gespeicherte Private Keys können kopiert werden
- Personalisierung im Batch-Betrieb möglich
  - Karten sind persönlich zuordenbar
    - → klare Verantwortlichkeit
- Eignung für optische Personalisierung
- Mobilität: durch USB-Leser + SIM-Plugin gewährleistet
- Integration verschiedener Technologien / Anwendungen
  - Nutzung bereits existierender Systeme
  - Steigerung der Benutzerakzeptanz
  - Karten werden häufiger benutzt, dadurch seltener vergessen
  - Vereinheitlichtes Management für Ausgabe, Einzug, Sperrungen etc. möglich



Fraunhofer SIT

Struktur der aktuellen Fraunhofer-PKI

- 10/2007: Zertifizierung durch T-Systems
  - Akzeptanz in gängigen Betriebssystemen/Browsern
  - deutliche Erleichterung bei Prüfung von Zertifikaten

- T-Systems in Betriebssystemen/Browsern anerkannte Zertifizierungsstelle
  - in Windows XP, Windows Vista, Windows 7, Outlook, Outlook Express, Internet Explorer, Opera, Mozilla-Clients
- Auch Zertifikate der Fraunhofer PKI von Außenstehenden direkt überprüfbar
- Vertrauens-Anker ist selbst-signiertes Zertifikat von T-Systems

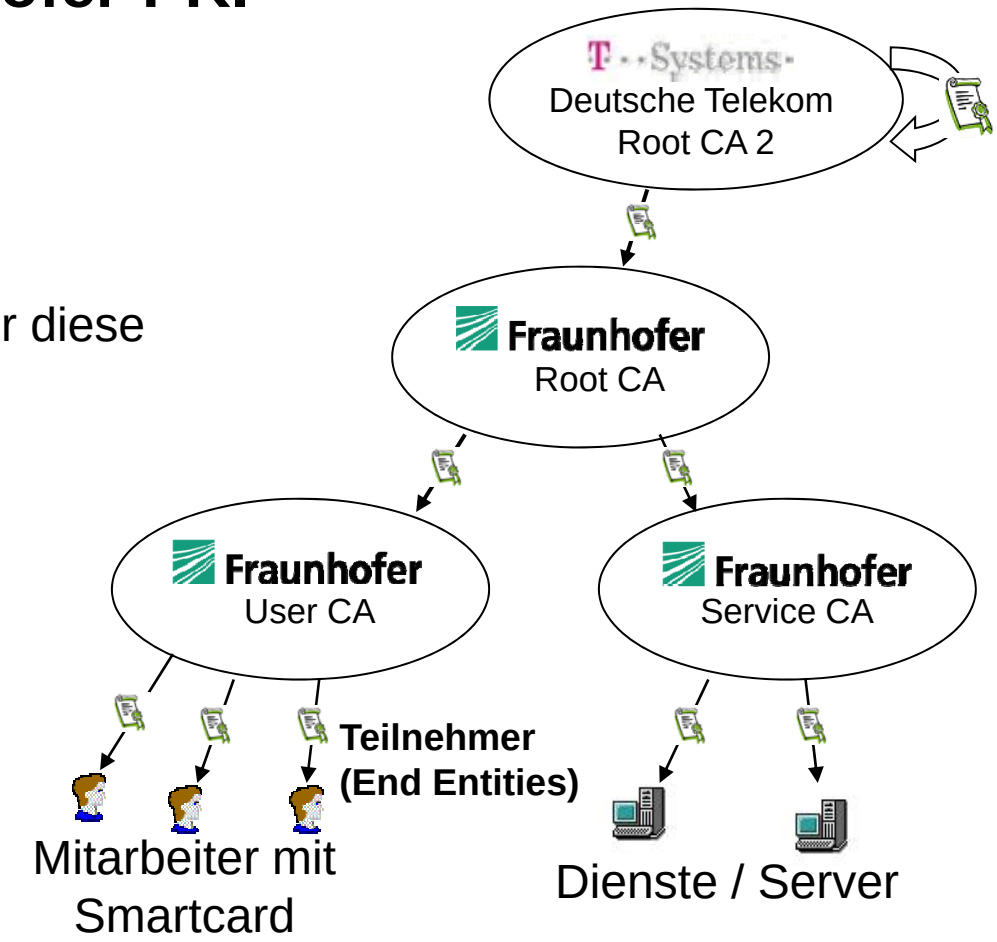
Die Hierarchie der Fraunhofer-PKI

Fraunhofer User CA
zertifiziert FhG-Mitarbeiter, gibt für diese Smartcards aus

Fraunhofer Service CA
Zertifikate für Server und Dienste (z. B. Mailinglisten)

Beide CAs sind Fraunhofer Root CA untergeordnet

Fraunhofer Root CA
ist wiederum Deutsche Telekom Root CA untergeordnet

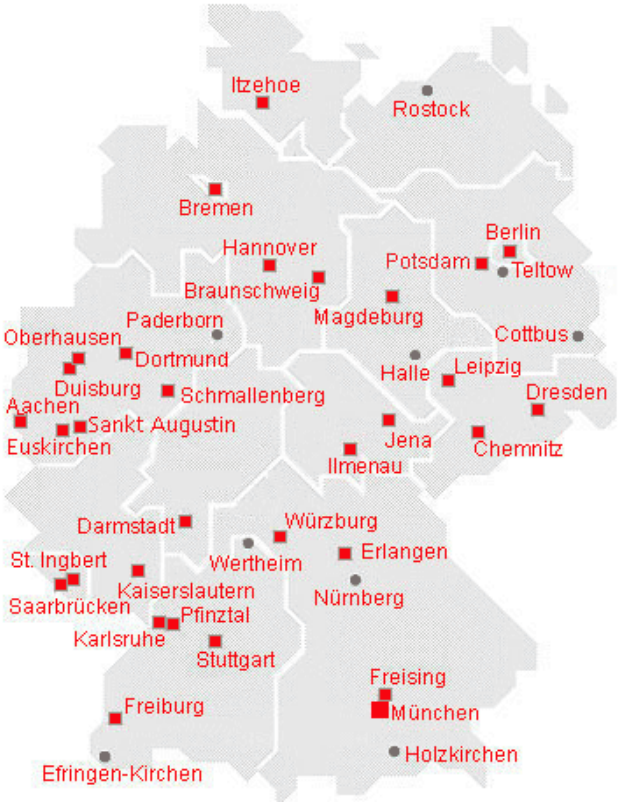


➡ Anerkennung der Zertifikate im Außenraum!

Fraunhofer SIT

Wie bekommt ein Mitarbeiter die Fraunhofer-Smartcard?

- Jeder Mitarbeiter bekommt automatisch eine Fraunhofer-Smartcard
- Die Smartcard wird von einer Ausgabestelle am Institut nur gegen Vorlage des Ausweises ausgegeben (Identitätsprüfung)
- Zusätzlich zur Smartcard werden Kartenleser ausgegeben
- Die PIN zur Nutzung der Smartcard wird in einem PIN-Brief persönlich an die Mitarbeiter gesendet



Fraunhofer SIT

Datenflüsse und Abhängigkeiten

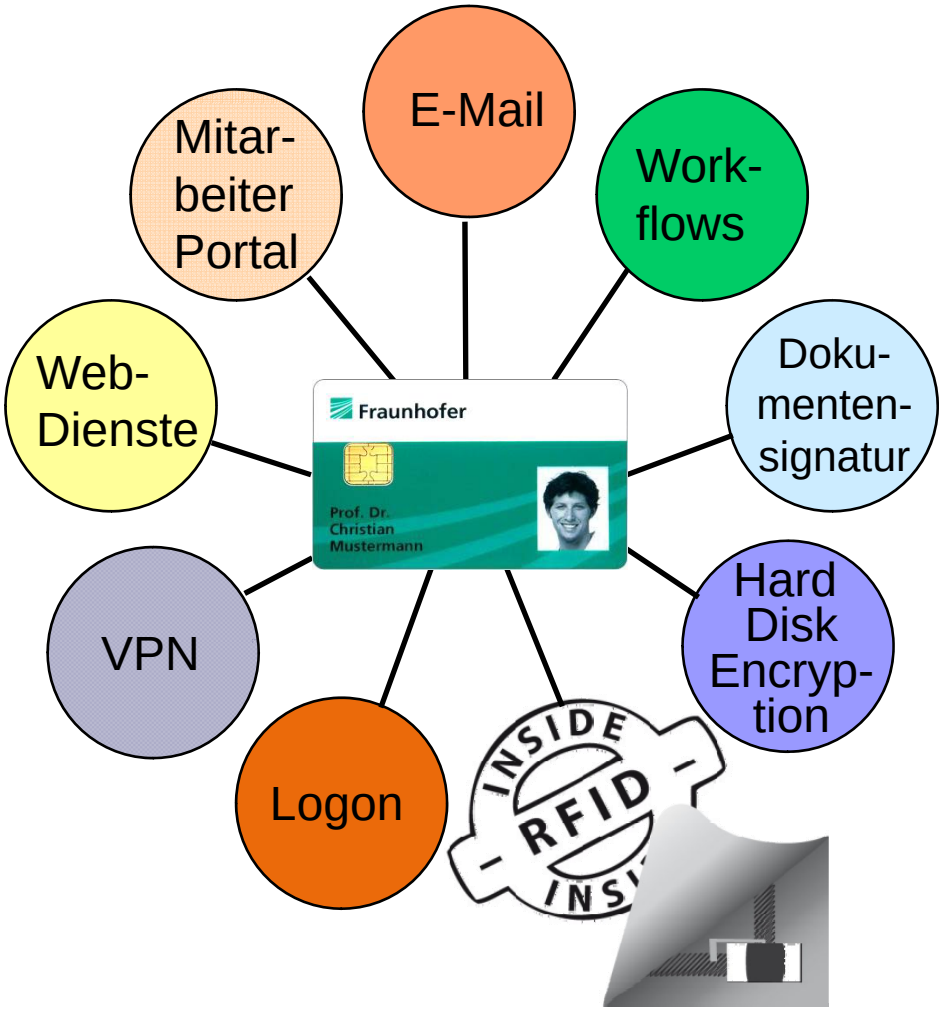
Fraunhofer SIT

Inhalte und Gliederung

- Das Fraunhofer Competence Center PKI
- Der Weg zur heutigen Fraunhofer-PKI
- Die Fraunhofer-Smartcard und ihre PKI-Anwendungen
- Zusammenfassung

Fraunhofer SIT

Anwendungen der Fraunhofer-Smartcard



Fraunhofer SIT

Die Fraunhofer-Smartcard als …
Sichtausweis

- Betriebsausweis / Mitarbeiterausweis
  - Trägt Name, Vorname und Bild des Mitarbeiters sowie das Institutslogo des Fraunhofer-Instituts bzw. der Gesellschaft

    → Sichtkontrolle beim Betreten der Einrichtungen
    → Nachweis der Zugehörigkeit zu Fraunhofer gegenüber Dritten

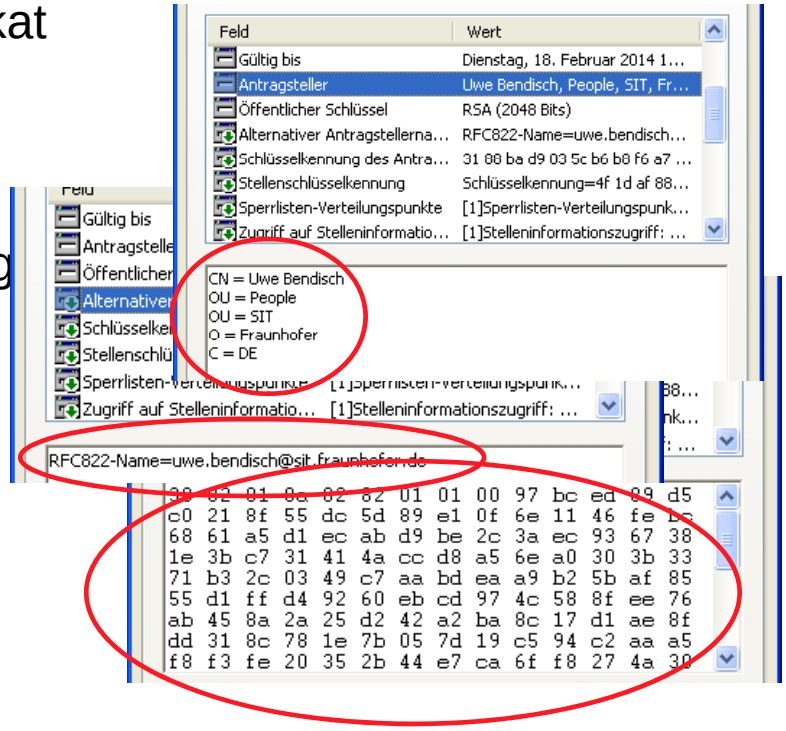
Fraunhofer SIT

Die Fraunhofer-Smartcard als …
Schlüsselkarte (PKI-Karte)

- Krypto-Chip mit persönlichen, geheimen Schlüsseln und den zugehörigen Zertifikaten (Philips Smart MX P5CC072, STARCOS 3.0/3.2)
  - Authentisierung
    → Eigene Identität gegenüber Anwendungen / Servern ausweisen
  - Verschlüsselung
    → Für mich verschlüsselte Daten lesbar machen
  - (Fortgeschrittene) Signatur
    → Daten elektronisch unterschrieben

Die Fraunhofer-Smartcard als … Schlüsselkarte (PKI-Karte)

- Zu jedem geheimen Schlüssel ein Zertifikat
  - Name, Institut, E-Mail Adresse
  - Öffentlicher Schlüssel (public key)
  - Beglaubigt (signiert) von Zertifizierung
- Zertifikate sind öffentlich
  - Authentisierungszertifikat:
    Mit versendet bei Serveranmeldung
  - Verschlüsselungszertifikate weltweit über LDAP abrufbar
  - Signaturzertifikat: in jeder Signatur



Fraunhofer SIT

Die Fraunhofer-Smartcard als …
Multifunktionskarte

- RFID-Chip (Mifare DESFire 4K, Legic Advant 2048) und Magnetstreifen (HICOM)
  - Gebäude-Zugang
  - Zeiterfassung
  - Bezahlung (Kantine, Parkhaus, etc.)
  - Secure Follow-Me Printing

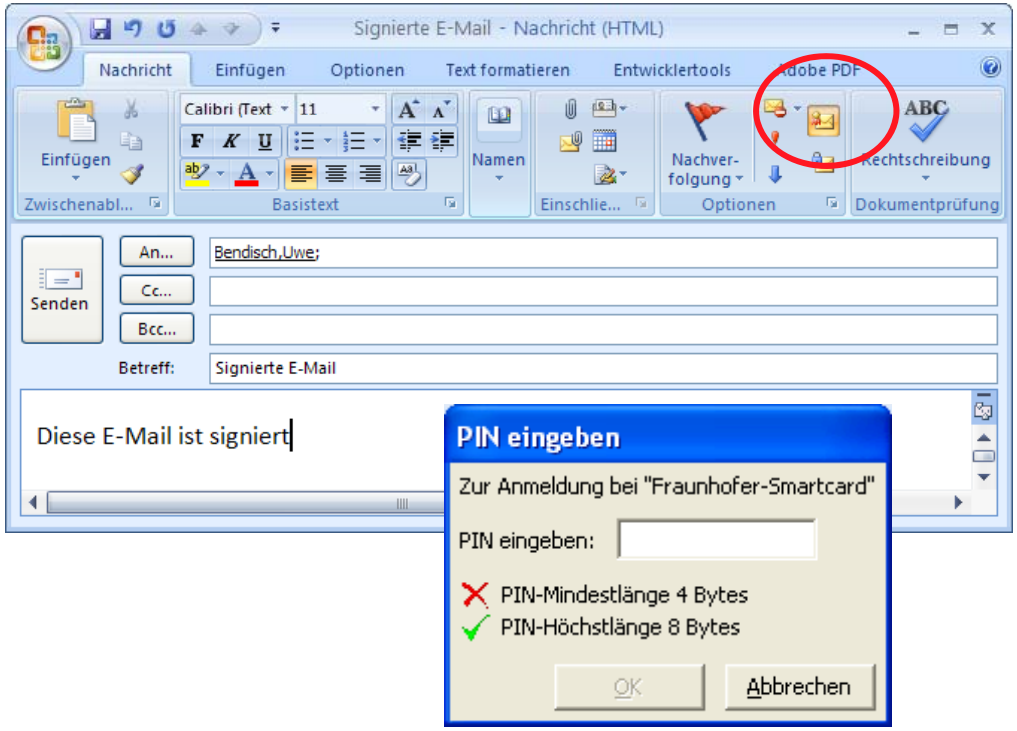
Fraunhofer SIT

System-Logon

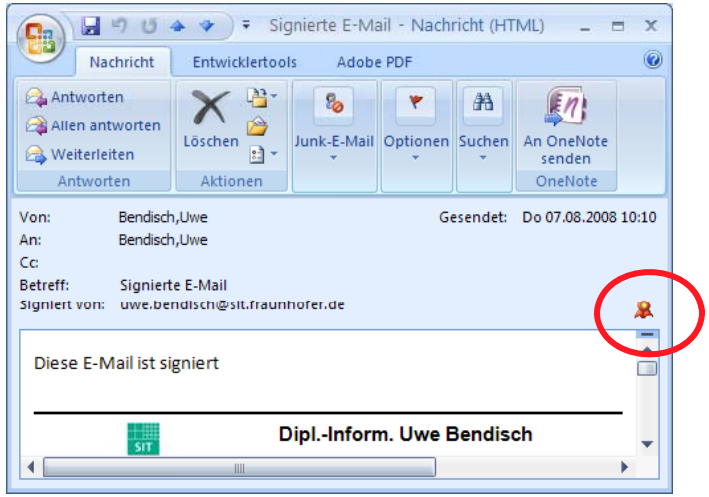
- Smartcard als Alternative oder Ersatz für Benutzername/Passwort
- Auch unter Linux / MacOS X nutzbar

Fraunhofer SIT

E-Mail-Signatur (mit Outlook)



- Signieren, um Schreiben verbindlich zu machen
- Gebrochene Signatur beim Empfänger deutet hin auf geänderten Inhalt oder falschen Absender



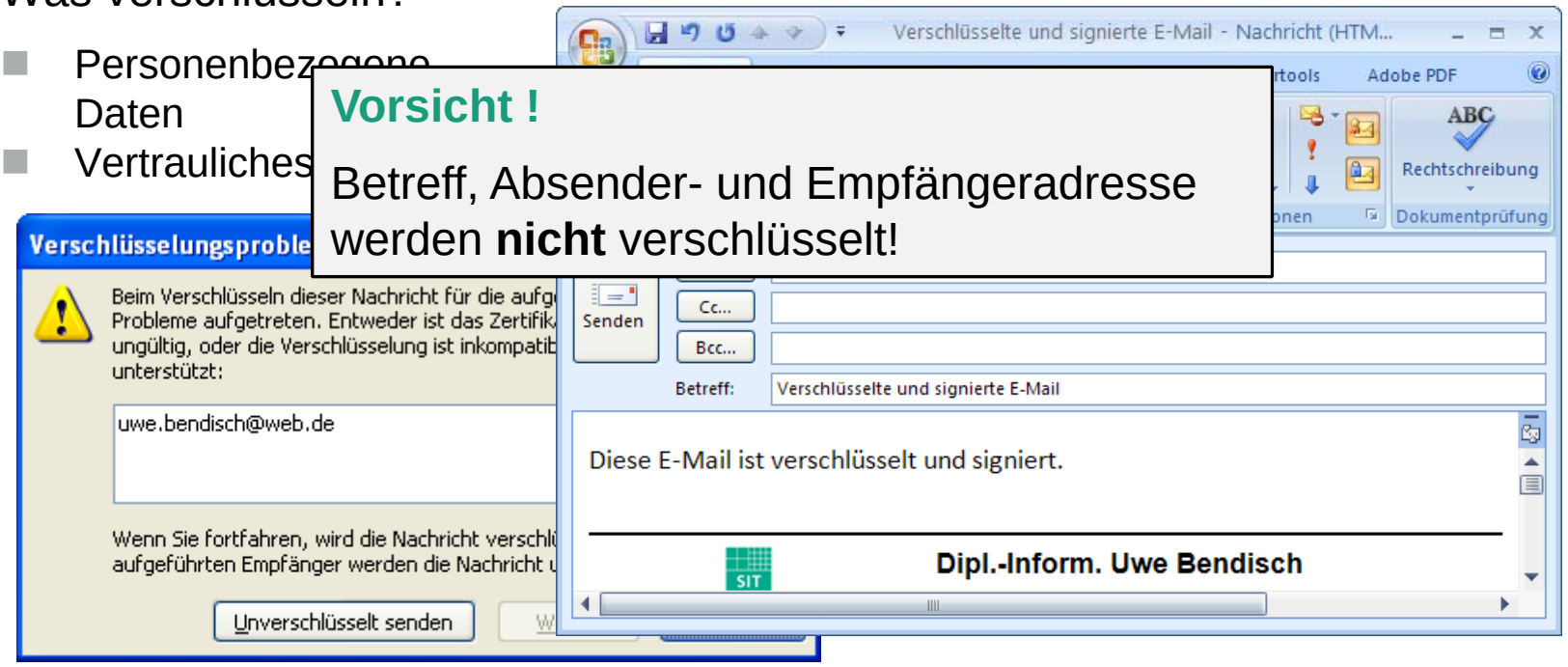
Fraunhofer SIT

E-Mail-Verschlüsselung mit Outlook

- Verschlüsselung benötigt Zertifikat des Empfängers
  - Fraunhofer-Mitarbeiter: im Fraunhofer Directory
  - Externe: Signierte E-Mail zusenden lassen und ins Adressbuch übernehmen
  - Externe können auch bei Fraunhofer (Software-)Zertifikate erhalten
- Was verschlüsseln?
  - Personenbezogene Daten
  - Vertrauliches

Vorsicht !

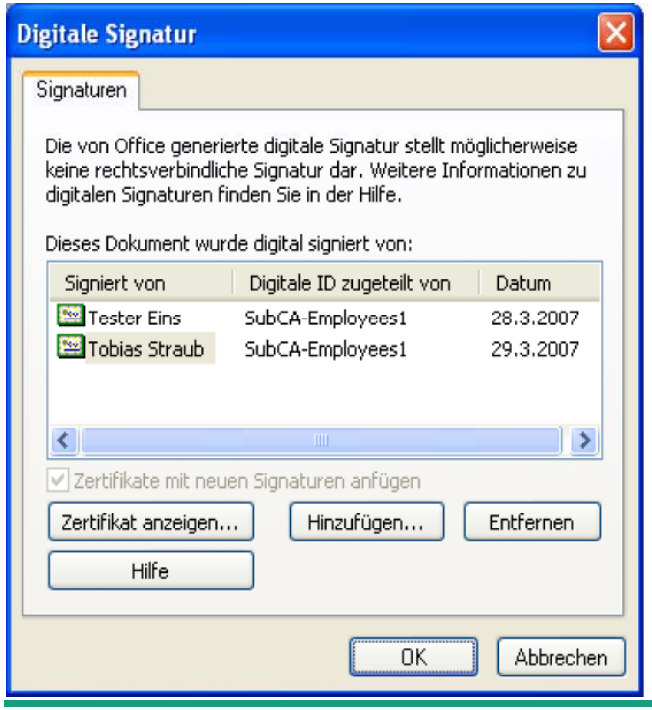
Betreff, Absender- und Empfängeradresse werden **nicht** verschlüsselt!



Fraunhofer SIT

Elektronische Workflows / Dokumentensignatur

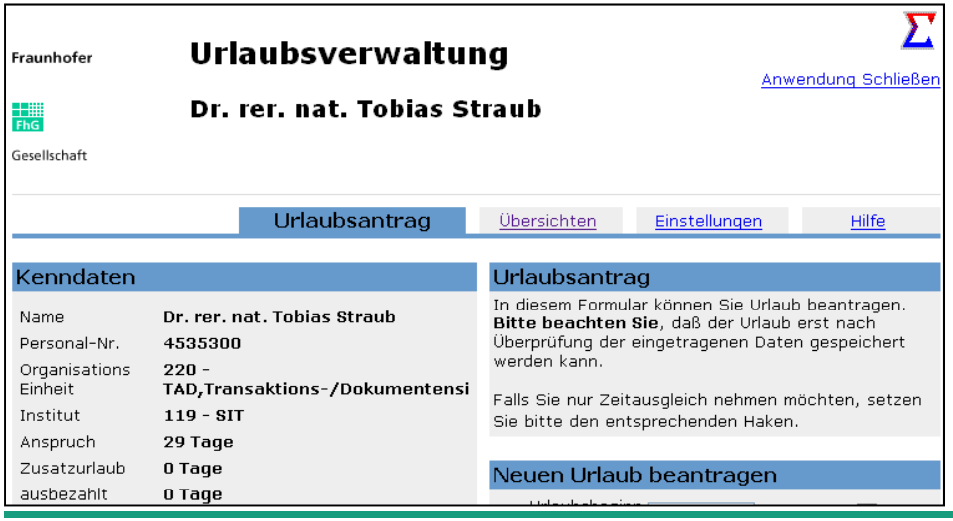
- Standard-Funktionalität in Microsoft-Office oder Adobe Acrobat
- Dokumente lassen sich mehrfach signieren, Reihenfolge/Zeitpunkt ist dokumentiert

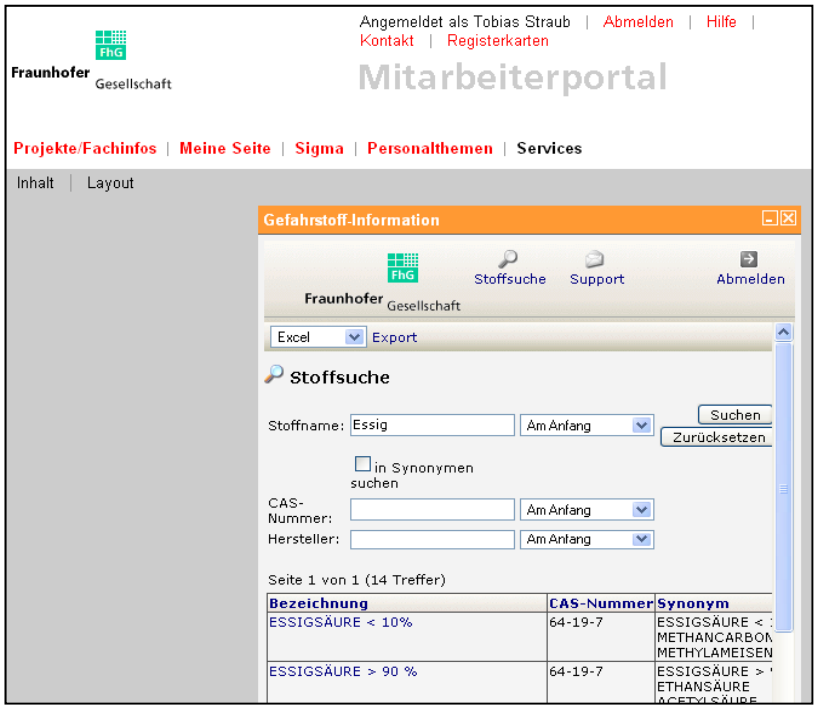


Fraunhofer SIT

HTTPS mit Client-Auth – Zugang zum Fraunhofer-Portal

- u.a.
  - Urlaubsverwaltung (Web-Urlaub)
  - Gefahrstoff-Datenbank (GEVIS)
  - WEB-Zeiterfassung
- Zugang auch zu anderen FhG-Servern

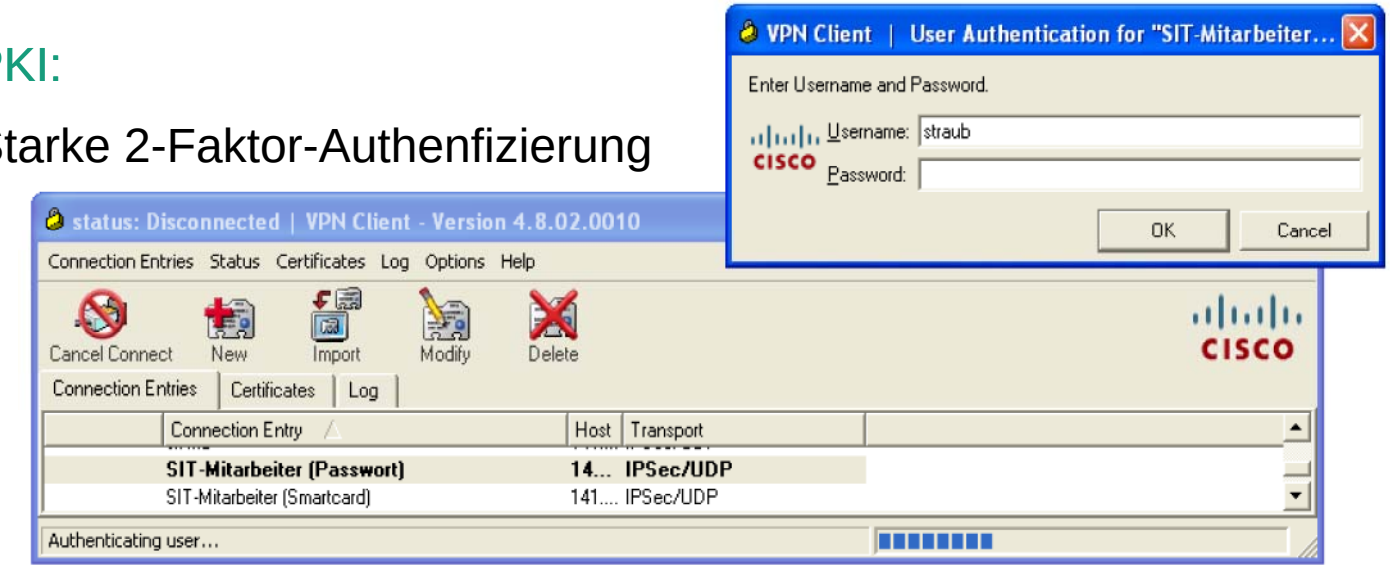




Fraunhofer SIT

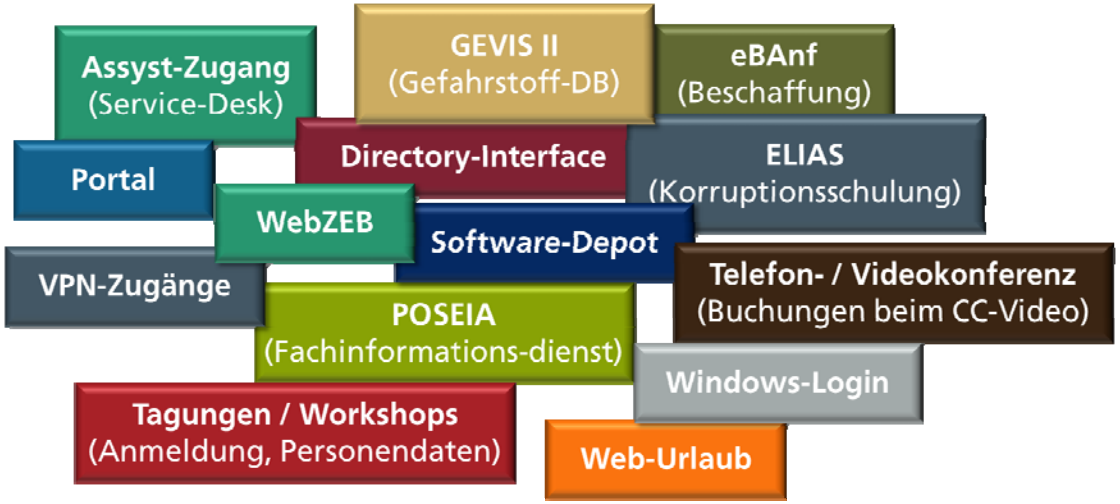
VPN

- Typische Konfiguration der CISCO-Firewall:
  - Benutzername/Passwort (Aber Bill Gates 2004: „Das Passwort ist tot.“)
  - Shared-Key-Verfahren: Alle Clients haben denselben Schlüssel, bei Kompromittierung muss dieser überall geändert werden
- Mit PKI:
  - Starke 2-Faktor-Authenfizierung



Fraunhofer SIT

Weitere Anwendungen der Smartcard



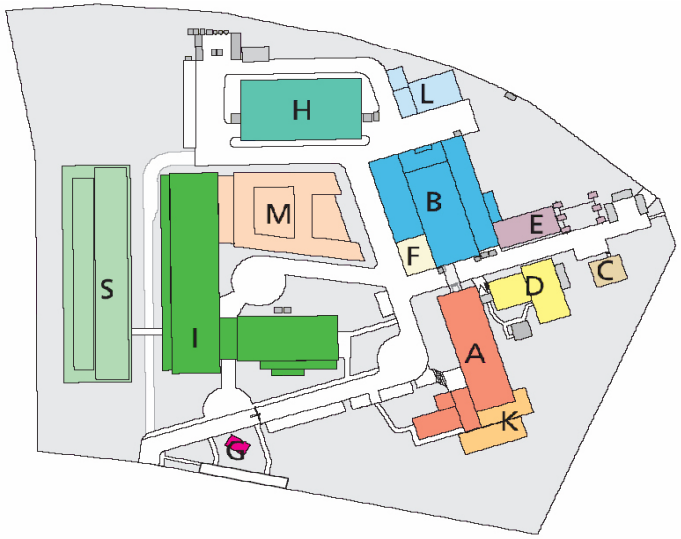
- Zentraler Service Desk (Ticket-System)
- Elektronische Bestellanforderungen
- Lernplattformen
- Authentisierung am Fraunhofer-Directory (Erweiterte Pflegemöglichkeiten)
- Softwaredepot
- Anmeldungen für Tagungen / Workshops
- Buchung von Telefon-/Videokonferenzen
- …

Fraunhofer SIT

Anwendungsbeispiel zur Multifunktionskarte

Fraunhofer WKI, IST (Braunschweig)

- Campus: Zwei Institute – eine Verwaltung
- Angestrebt: Harmonisierung / Vereinheitlichung der Dienste (Server-Sharing)



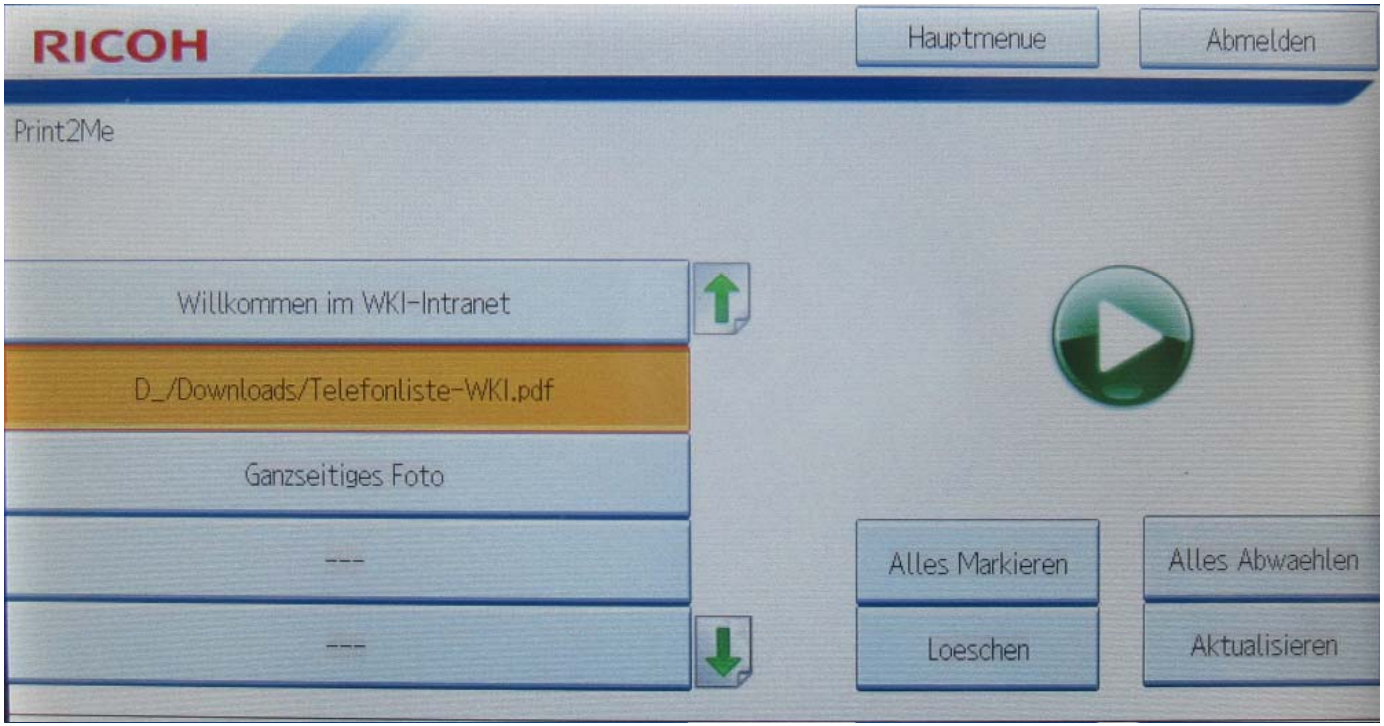
Nutzung der Smartcard u. a. für

- Gebäude-Zugang
- Secure Follow-Me Printing

Source: L. Reckemeyer (Fraunhofer WKI, IST)

Fraunhofer SIT

Fraunhofer WKI, IST - Kopierer Menüansicht



Source: L. Reckemeyer (Fraunhofer WKI, IST)

Fraunhofer SIT

Weitere Kartentypen

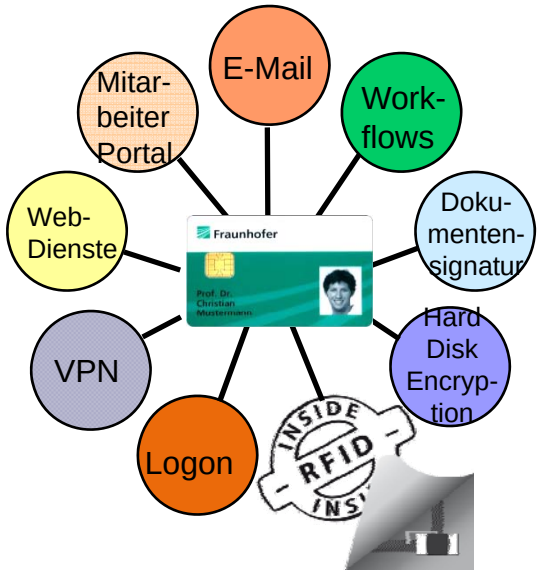
- Nebenkarten
  - Enthält identischen Verschlüsselungsschlüssel, aber andere Signatur- und Authentifizierungsschlüssel
  - Anwendungsfälle:
    - Simultanes Arbeiten an mehreren PCs
    - im SIM-Format für Geräte mit Windows Mobile, RIM Blackberry
- Vertreterkarten
  - Z.B. für Sekretariate
  - Enthalten nur Verschlüsselungsschlüssel
- Backup-Karten
  - Enthalten nur Verschlüsselungsschlüssel
- Notfallkarten
  - Wie Backup-Karte, aber Karte befindet sich nicht im Besitz des Karteninhabers

Inhalte und Gliederung

- Fraunhofer und das Fraunhofer Competence Center PKI
- Der Weg zur heutigen Fraunhofer-PKI
- Die Fraunhofer-Smartcard und ihre PKI-Anwendungen
- Zusammenfassung

Die Fraunhofer-Smartcard als Sicherheitsanker

- Die Fraunhofer-Smartcard sichert IT-Anwendungen
- Wer Karte hat und PIN kennt, kann sie missbrauchen
  - Im Namen des Fraunhofer Mitarbeiters unterschreiben
  - Auf für den Mitarbeiter verschlüsselte Daten zugreifen
  - Unberechtigt Zugang zu Computern und Portal erhalten



- … und die Mitarbeiter werden in ihrer Arbeit von der Karte abhängig
  - je nach Anwendungen ist ohne Karte die Nutzung eingeschränkt oder gar nicht möglich

PKI-Einführung: Was ist zu beachten?

- Aufwand
  - PKI kostet Zeit & Geld
  - Organisatorische Maßnahmen und Betrieb teurer als Technik und Einführung
- Integration in Prozesse des Unternehmens
  - Business Case klar definieren
    - Prozessorientierte Integration ist aufwändiger wenn Prozess/Business-Case schlecht oder gar nicht modelliert wurde
    - Prozess-Optimierungen sollten nicht gleichzeitig mit PKI eingeführt werden – Aufgaben sind dadurch häufig zu komplex
  - Gute IST-Analyse für Einführung
  - Veränderte Arbeitsabläufe
    - Z. B. neu: Registrierung und Ausgabe von Zertifikaten und Schlüsseln
    - Z. B.: Veränderte Workflows durch digitale Signatur statt auf Papier
    - E-Mail-Verteilerlisten: Ggfs. zusätzliche Server-Lösung erforderlich

PKI-Einführung: Was ist zu beachten?

- Komplexität
  - Mangelnder Akzeptanz / Sicherheitsbewusstein bei Mitarbeitern vorbeugen
    - Schulung und Awareness-Maßnahmen notwendig (Flyer, Vorträge etc.)
  - Übertriebene Sicherheitsanforderungen wg. Angst vor Haftung und Missbrauch vermeiden
- Stellvertreterproblem bei verschlüsselten Daten
  - Lösung durch technische und/oder organisatorische Maßnahmen
- Schlüsselhinterlegung
  - löst Message / Data Recovery Problem
- Sichere Kommunikation mit Geschäftspartnern
  - Erfordernis
  - Kompatibilität
- Richtige Gewichtung von Usability – Sicherheit – Kosten

PKI-Einführung: Was ist zu beachten?

- Mobilität der Nutzer
  - Hardwaretoken vs. Softtoken als Schlüsselträger
- keine unveränderliche Infrastruktur
  - Neue Anforderungen müssen umgesetzt werden (können)
  - Beispiel Fraunhofer
    - Export von Verschlüsselungs-Token
    - Problematik realer Namen im DN
- (Neue) Sicherheitsprobleme
  - Bei Ende-zu-Ende Verschlüsselung können am Sicherheitsgateway keine Pakete geprüft werden – Clients müssen ggf. zusätzlich gesichert werden

Kontakt

Fraunhofer-Institut für
Sichere Informationstechnologie SIT

Abteilung Security Management (SMA)

Institutszentrum Schloss Birlinghoven

Uwe Bendisch

Schloss Birlinghoven

53757 Sankt Augustin

Telefon: +49 2241 14-3122

Fax: +49 2241 14-43122

E-Mail: uwe.bendisch@sit.fraunhofer.de

Internet: http://www.sit.fraunhofer.de

Fraunhofer SIT