

Pilotprojekt „Digitaler Dienstausweis“



Dr. Andreas Wiemers, BSI
40. Erfahrungsaustausch des KoopA ADV
25./26.3.03 in Potsdam

Pilotprojekt „Digitaler Dienstausweis“



Zur Entwicklung des Pilotvorhabens

- Anfang 1999: Konzeptpapiere einer BMI-Arbeitsgruppe „Einsatz multifunktionaler Chipkarten als Haus- und Dienstausweis“
- Jahr 2000: EU-weite Ausschreibung für ein Pilotprojekt „Digitaler Dienstausweis“
- Ziel des Piloten: Erfahrungen machen mit digitalem Dienstausweis; Risiken und Aufwände erkennen; Informationen für andere Behörden zur Verfügung stellen (detaillierter Abschlussbericht)

Pilotprojekt „Digitaler Dienstausweis“



Vorgaben für die Ausschreibung

- Fälschungssicherer Kartenkörper
- qualifizierte elektronische Signaturen nach SigG; d.h. Zertifizierungsdienstleistung nach SigG und Chipkarte als sichere Signaturerstellungseinheit
- Chipkarte realisiert kryptographische Grundfunktionen: Digitale Signatur; Verschlüsselung, Authentisierung
- Zutrittskontrolle/Zeiterfassung durch zweiten kontaktlosen Chip auf der Karte
- Anbindung an Sphinx (E-Mail-Absicherung mittels Signatur und Verschlüsselung)

Pilotprojekt „Digitaler Dienstausweis“



Zur Entwicklung des Pilotvorhabens

- Arbeitsteilung zwischen Chipkarte und Hintergrundsystem auf Basis der TeleTrust-Chipkartenspezifikation „German Office Identity Card“
- Weitere Funktionen im Piloten unter Realisierungsvorbehalt
 - Zugriff auf Daten über Netze
 - Zugangskontrolle an Rechnern
 - Ausweisdaten werden digital abgelegt auf Chipkarte

Pilotprojekt „Digitaler Dienstausweis“



Zum technischen Hintergrund:

- Symmetrische Kryptographie seit Jahrhunderten benutzt
- Digitale Signaturen basieren auf asymmetrischer Kryptographie
- Asymmetrische Kryptographie: Trenne Verschlüsselung und Entschlüsselung mit jeweils anderen Schlüsseln
- Verfahren zur asymmetrischen Kryptographie beruhen auf schwierigem mathematischen Problem
- Bekanntestes Verfahren RSA nach Rivest, Shamir, Adleman (1977)



Zahlen zu multiplizieren ist einfach:

$$3\ 121\ 163 * 4\ 811\ 953 = \\ 15\ 018\ 889\ 661\ 339$$

Zahlen in Faktoren zu zerlegen ist mühselig:

$$11\ 099\ 399\ 206\ 043 = \\ ???$$

Pilotprojekt „Digitaler Dienstausweis“



Vertrag

Handwritten text representing a contract document.

10110001

G

RSA

00101110

Vertrag

Handwritten text representing a contract document.

00101110

O

RSA

?

Beispiel:
RSA-Signaturen



Warum Chipkarten ?

SigG: Der Zertifizierungsdiensteanbieter hat ... Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten.

SigV: Der Signaturschlüssel darf nicht preisgegeben werden.

Begründung zu SigV: Die Geheimhaltung des Schüssels ... erfordert... eine sichere Signaturerstellungseinheit wie z.B. eine Chipkarte..., die nach Stand der Technik nicht ausgelesen werden kann (auch nicht durch den Signaturschlüssel-Inhaber selbst).

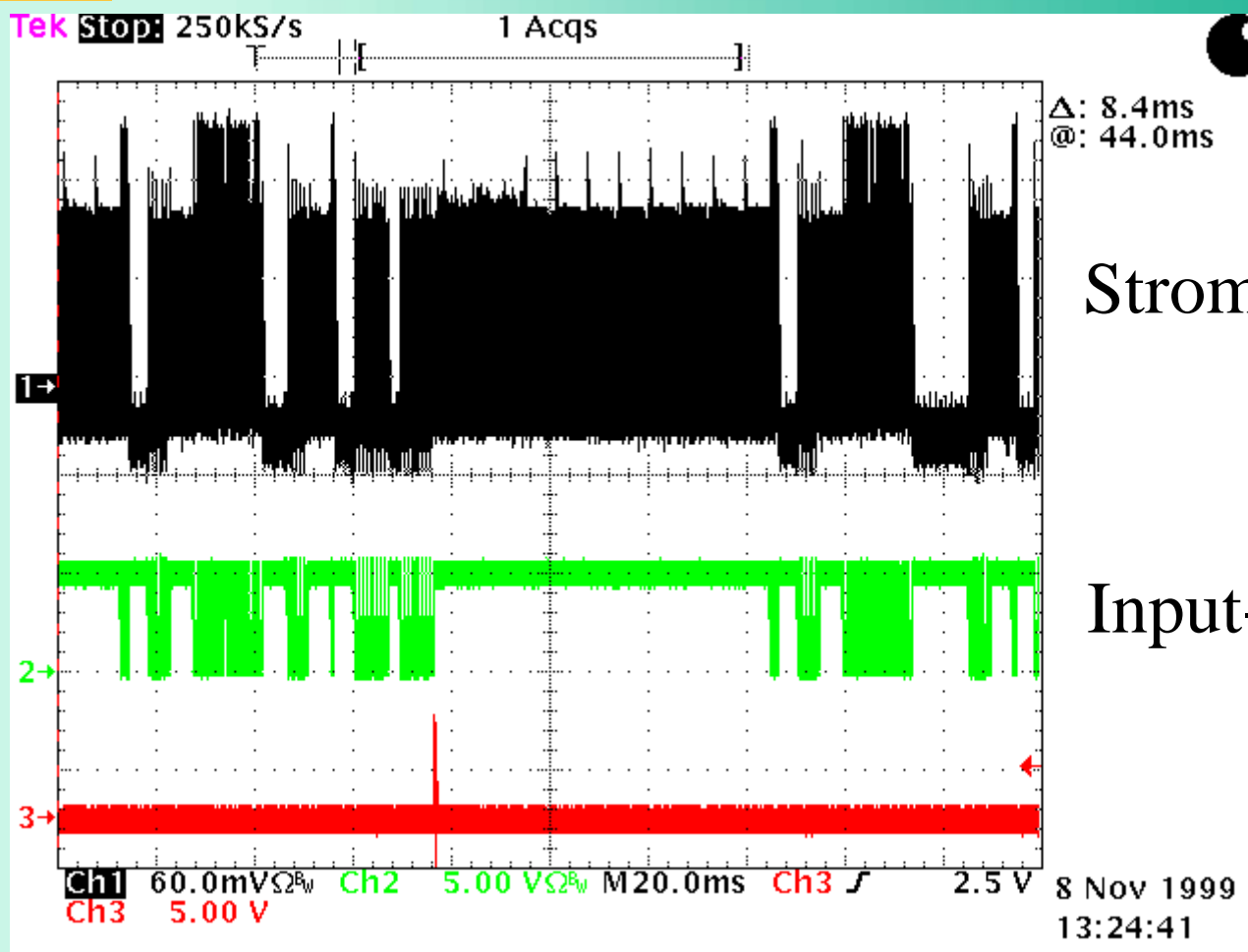
Pilotprojekt „Digitaler Dienstausweis“



Chipkarte = Sicherer Computer

- geprüfte Hardware
- geprüftes Chipkarten-Betriebssystem
- nur genau eine Datenschnittstelle
- Angriffe auf Stromaufnahme der Chipkarte (1999: Differential Power Attacks)

Pilotprojekt „Digitaler Dienstausweis“



Rekonstruktion des geheimen Schlüssels durch Analyse des Stromverbrauchs der Chipkarte

Pilotprojekt „Digitaler Dienstausweis“



Pilotanwendung

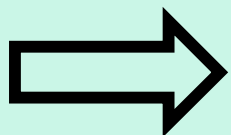
- 70 Mitarbeiter im BMI, 30 Mitarbeiter im BSI, weitere Mitarbeiter im BVA und BKA
- Beginn im November 2001, Ende im Mai 2002

Generalunternehmer für den Piloten

- Bundesdruckerei mit Konsortialpartner: Utimaco, D-Trust, ORGA, UNISYS

Funktionalitäten der Chipkarte

- optische Ausweisfunktion (Fälschungssicherheit)
- Zutrittskontrolle/Zeiterfassung (über kontaktlosen Chip /Magnetstreifen)
- kryptographische Grundfunktionen (über kontaktbehafteten Chip):
 - „qualifizierte elektronische Signatur“ (nach SigG)
 - Verschlüsselung/Digitale Signatur (nach Sphinx/MailTrust V2.0)
 - Authentisierung (wurde nur im Demosystem genutzt)

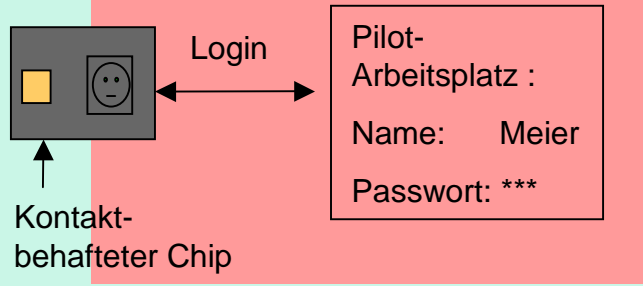
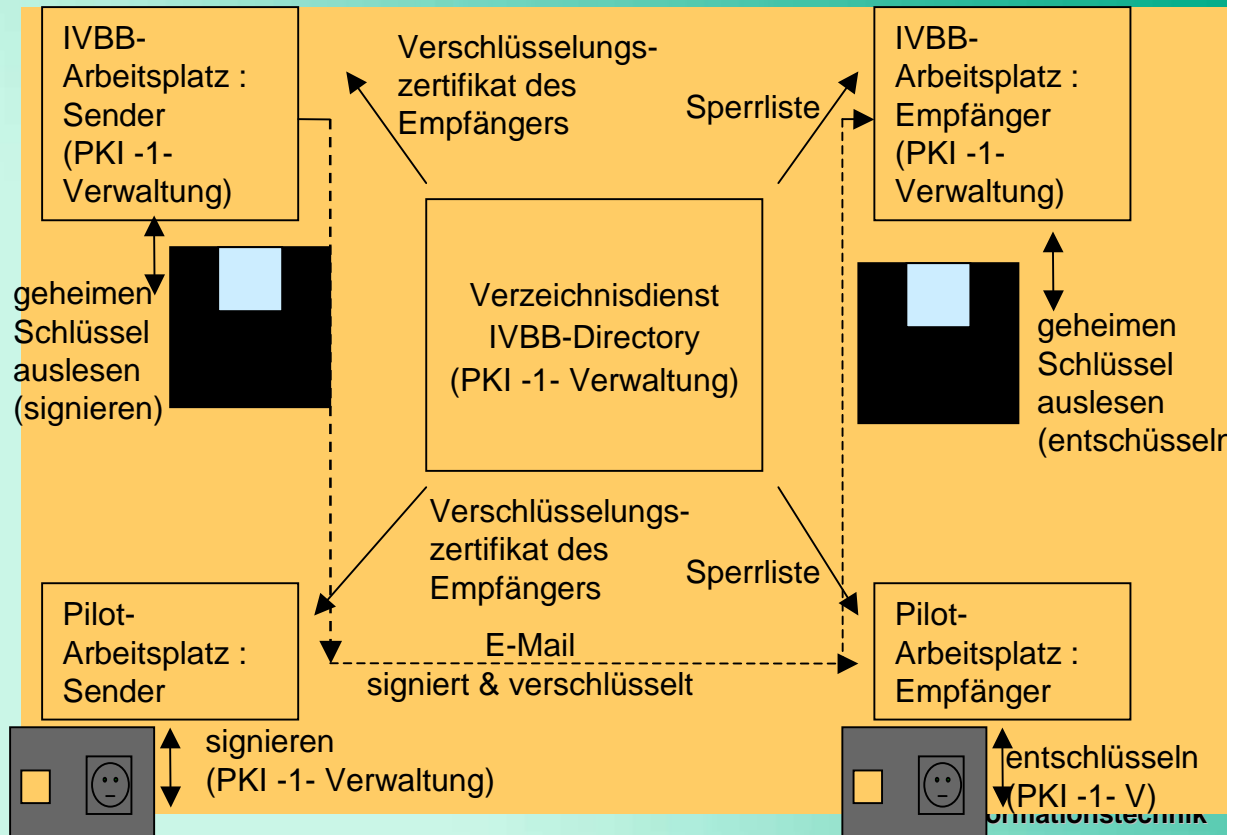
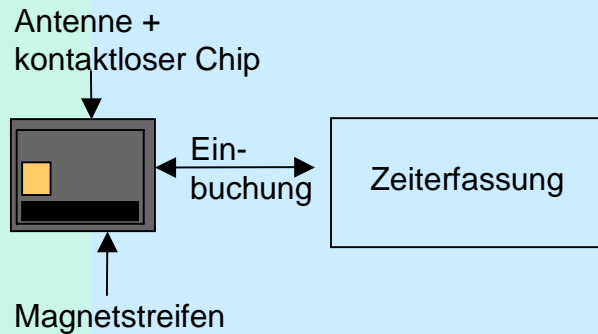
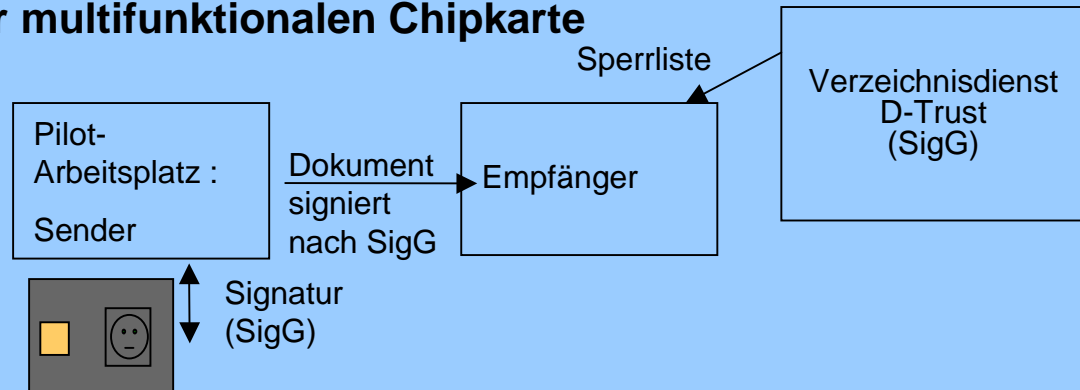
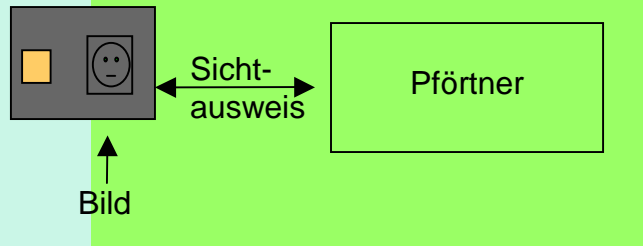


4 verschiedene Schlüssel/Zertifikate auf dem kontaktbehafteten Chip

Pilotprojekt „Digitaler Dienstausweis“



Einsatz der multifunktionalen Chipkarte



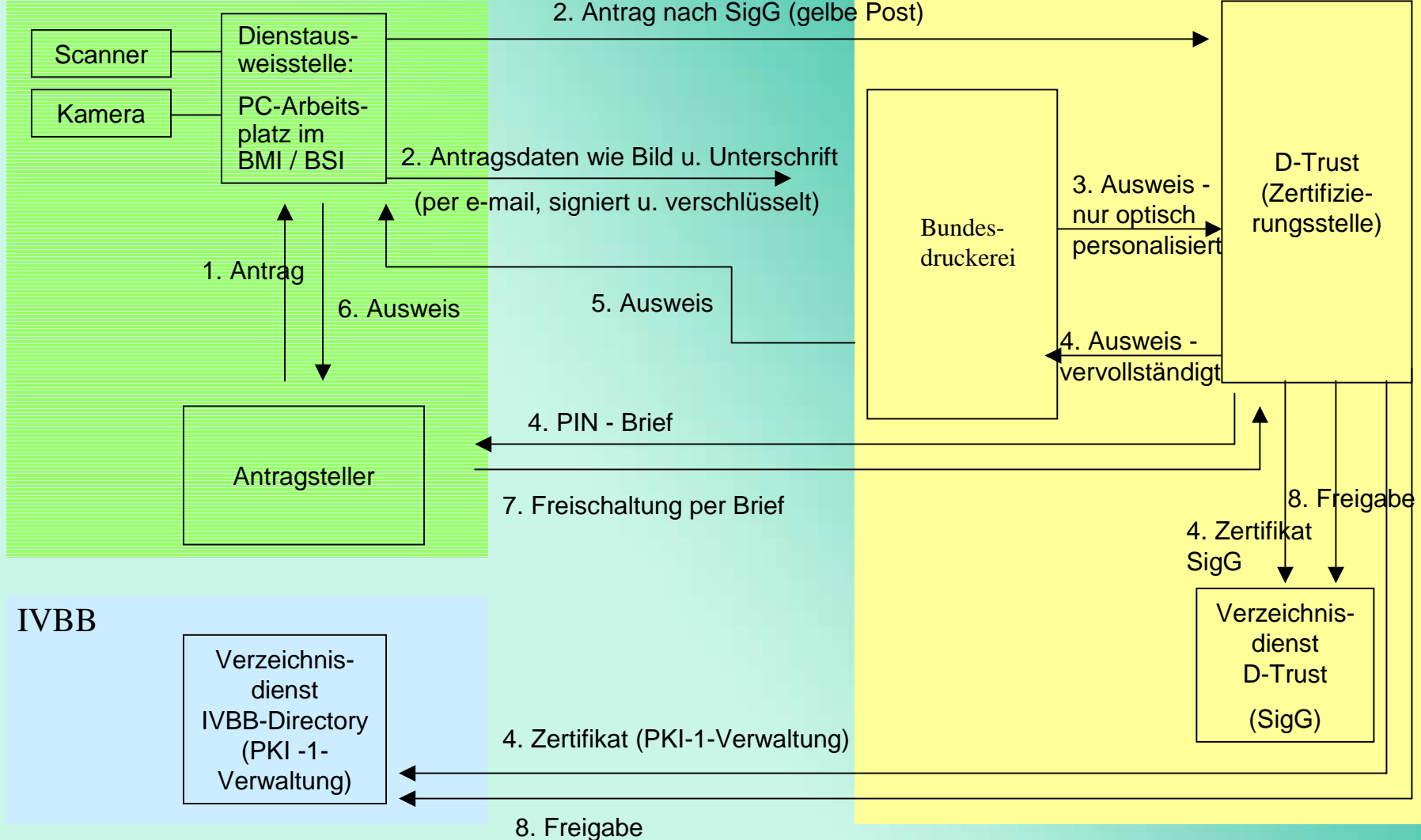
Pilotprojekt „Digitaler Dienstausweis“



Ablauf der Ausweiserstellung

BMI/BSI

Bundesdruckerei/D-Trust

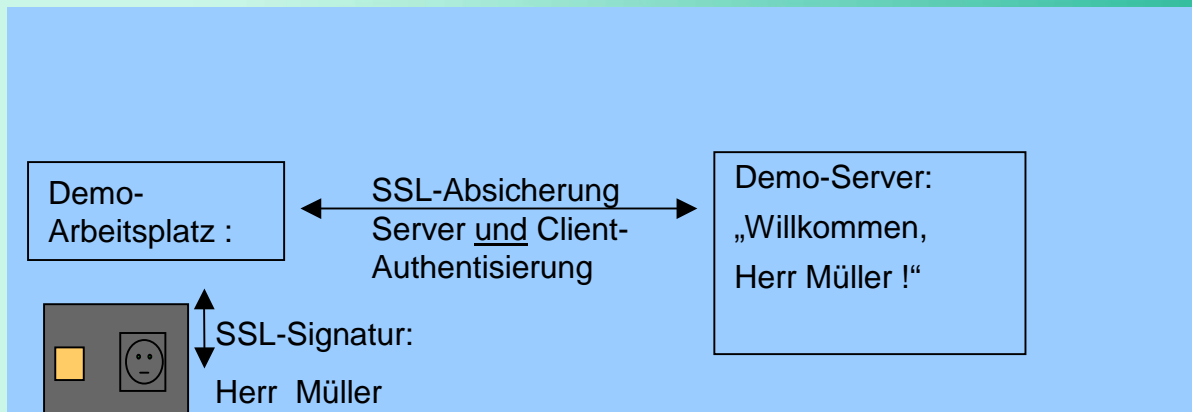


Pilotprojekt „Digitaler Dienstausweis“



Funktionalität des Demosystems

- Client-Authentisierung mit SSL



- Signieren von PDF-Dokumenten (Vorteil: Lesbarkeit ohne weiteres Tool)

Open Source Client

- Nutzung des digitalen Dienstausweises zum Signieren und Verschlüsseln von E-Mails im Linux-Umfeld (Projekt „Ägypten“ des BSI)

Pilotprojekt „Digitaler Dienstaussweis“



Technische Probleme im Piloten

- Abläufe in der Dienstaussweisstelle OK
- Chipkarte OK; Sperrlisten und Verzeichnisdienste OK
- Laufzeitverhalten der Software mangelhaft => Update im April 02
- Bedienerführung mangelhaft (2 verschiedene PINs)
- SPHINX-Interoperabilität problematisch
- Verteilung und Neuinstallation der Software sehr aufwändig
- Single-Sign-On-Funktionalität nicht auf andere Programme ausweitbar

Grenzen des Piloten

- Keine Einbindung in Arbeitsabläufe
- Keine Vorgaben für Signaturen und Verschlüsselungen
- Keine flächendeckende Ausstattung mit SPHINX-Produkten
- Keine einfache Lesbarkeit von signierten Dokumenten
- Kaum Akzeptanz von E-Mail-Absicherung

Pilotprojekt „Digitaler Dienstausweis“



Was haben wir gelernt

- Nutzung von „qualifizierten elektronischen Signaturen“ schwierig; für alle zumutbar ?
- Falsche PIN-Eingabe sollte korrigierbar sein ==> PUK
- Schlüsselbackup für Entschlüsselungsschlüssel auf der Karte

Ausblick

- BMI bereitet Roll-Out des digitalen Dienstausweises vor
- Bedarfsabfrage bei den verschiedenen Behörden
- Ziel: Komponentenmodularität je nach Anforderung der Behörde

Information über den Piloten

<http://www.bsi.bund.de/projekte/digdiaw/index.htm>