

Der elektronische Personalausweis

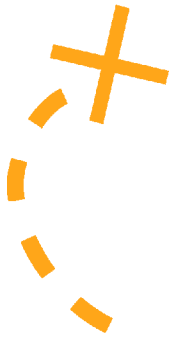
lobby driven security

GDD ERFA Kreis 18.6.2009

AirIT Systems Langenhagen

dn

Systems



Dr. Böttger

IT_Beratung + Projektmanagement

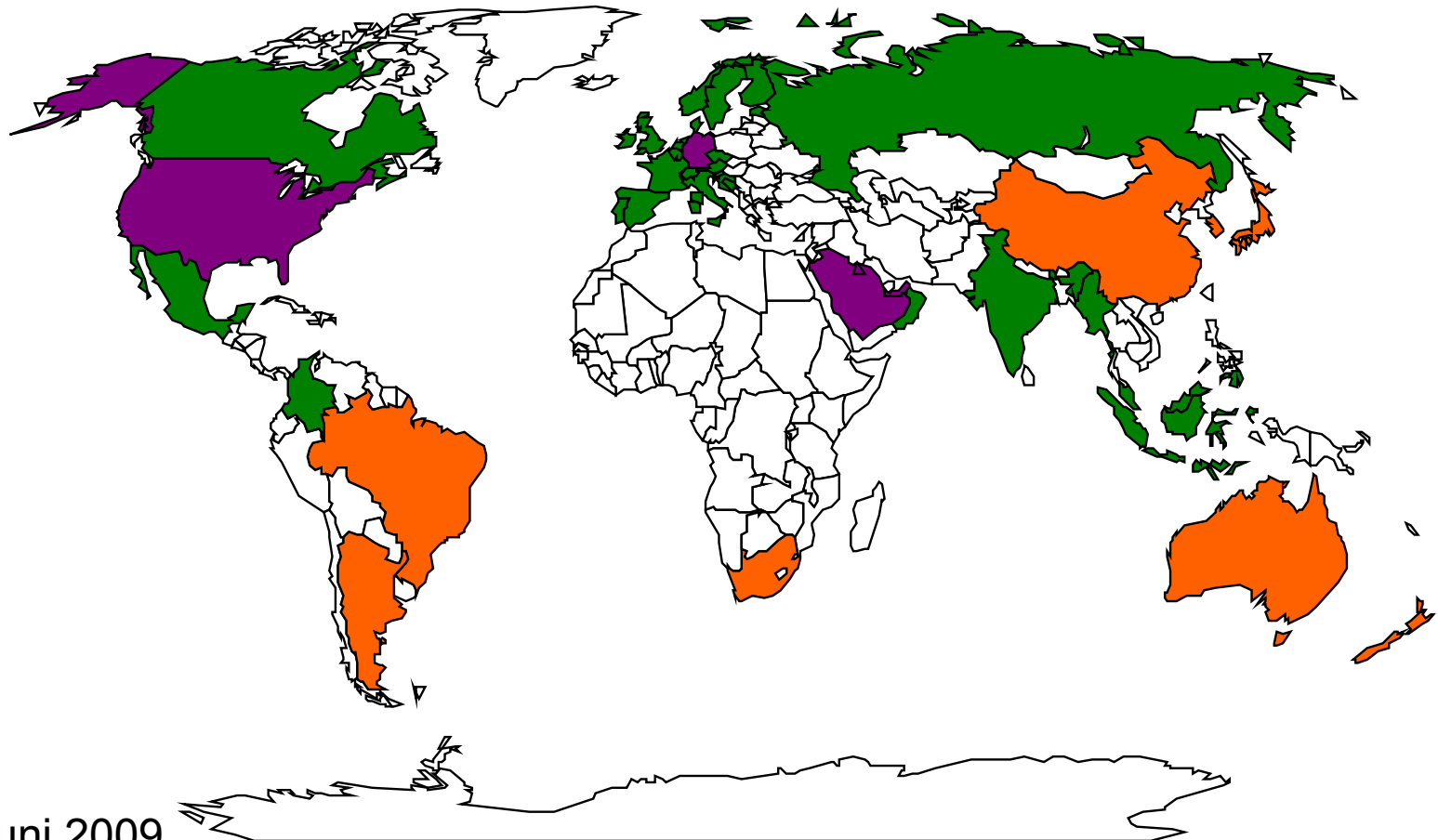
Lukas Grunwald
Dr. Christian Böttger

Über DN-Systems

- Globales Beratungs- und Technologie-Unternehmen
 - Planung
 - Evaluierung
 - Audit
 - Eigenes Rechner- / Netzwerk-Labor
 - Projektmanagement
 - Integrale Sicherheit (nicht nur IT)
 - Investigation / digitale Forensik

Weltweiter Service

- Customers
- Own stuff
- Partner





Kunden DN Systems

- RZ- und Datacenter-Betreiber
- Internet-Service-Provider und Backbone-Betreiber
- Telekommunikations-Konzerne
- Supply-Chain-Betreiber
- Transport und Logistik
- International tätige Konzerne
- Banken und Finanznetz-Betreiber (Kreditkarten-Clearing)
- Produzenten von Sicherheits-Hard- und Software
- Behörden und Staaten



Vorstellung Person

- Freiberuflicher IT-Berater seit Mai 2006
- Vorher Projektmanager und Teamleiter bei einem Systemhaus
- Seit 1996 beruflich in der EDV
- Seit 1994 im WWW
- Seit ca. 1987 im Internet
- Ausbildung: promovierter Physiker
- Seit Ende der '90er freier Autor für *iX* (Heise Verlag)
- Auslandsaufenthalte: Australien, Oman, diverse EU-Länder



Themen

- EDV-Strategie
- Projektmanagement / Interimsmanagement
- Internet und Netze
 - WWW
 - Mail, Anti-SPAM, Sicherheit
- Linux / Open Source
- Groupware
- IT-Security, LI
- EDI / EAI



Einführung: Was ist RFID?

- Radio Frequency Identification (RFID)
 - Drahtlose Übertragung von Informationen zwischen Transponder („Tag“) und „Reader“ (Lese- und Schreibgerät)
 - Bidirektionale Übertragung (Lesen und Schreiben)
 - Transponder („Tag“) kann an etwas befestigt, in etwas eingebaut oder auch in Lebewesen implantiert werden.
 - automatische Korrelation zwischen Objekt und gespeicherter Information

Datenmanipulation (Beispiel)





Generische Angriffe

- Abhören der Information zwischen Transponder und Reader
 - Fälschen der Kommunikation
 - unbefugtes Erlangen von User ID, Nutzdaten und Meta-Daten
 - grundlegende Angriffe auf Strukturen und Tags
 - „Replay Attacken“, um Zugangssysteme auszutricksen



Generische Angriffe

- Fälschung der Identität des Readers und nicht-authorisiertes Schreiben auf den Tag
 - Änderung der UID durch Manipulation des administrative data block
 - Vortäuschen einer falschen Identität
 - UID muss laut Standard in Klartext lesbar sein
 - Manipulation von Produktgruppen und Preisen

Generische Angriffe

- Manipulation von auf dem Tag gespeicherten Daten
 - Manipulation von Nutzdaten
 - Manipulation von Metadaten
 - Austausch von Objekten
 - Scheinbare Duplikation von Objekten



Generische Angriffe

- Deaktivierung des Transponders
 - Verhinderung der Verfolgung von Objekten
 - Verhinderung der Erkennung von Objekten („unsichtbar“)



Generische Angriffe

- Angriffe auf die Middleware und Backend-/Server-Systeme; Manipulation von Datenstrukturen
 - Einbringen von Schadprogrammen („Malware“) in Backend- und Middleware-Systeme
 - z.B. „Datenbank-Würmer“, SQL-Injektion
 - Manipulation von Backend-Systemen
 - „Denial of Service“ - Angriffe auf die Infrastruktur

Generische Angriffe

- „Jamming“ der RFID Frequenzen
 - Kann mit „out-of-the-box“ Polizeifunk- / Handy-Jammern gemacht werden (Breitband Jamming Sender)
 - Angriffe gegen den Anti-Collision-Mechanismus des RFID-Systems
 - Verhindern, dass ein Tag gelesen werden kann
 - Einfacher „Denial of Service“- Angriff gegen das RFID System
 - „Abschalten“ der Produktion, des Verkaufs oder des Zugangs

ePassports / ePersonalausweis



Dr. Böttger
IT_Beratung + Projektmanagement

dn
Systems



This image is a work of a United States Department of Homeland Security employee, taken or made during the course of an employee's official duties. As a work of the U.S. federal government, the image is in the public domain.

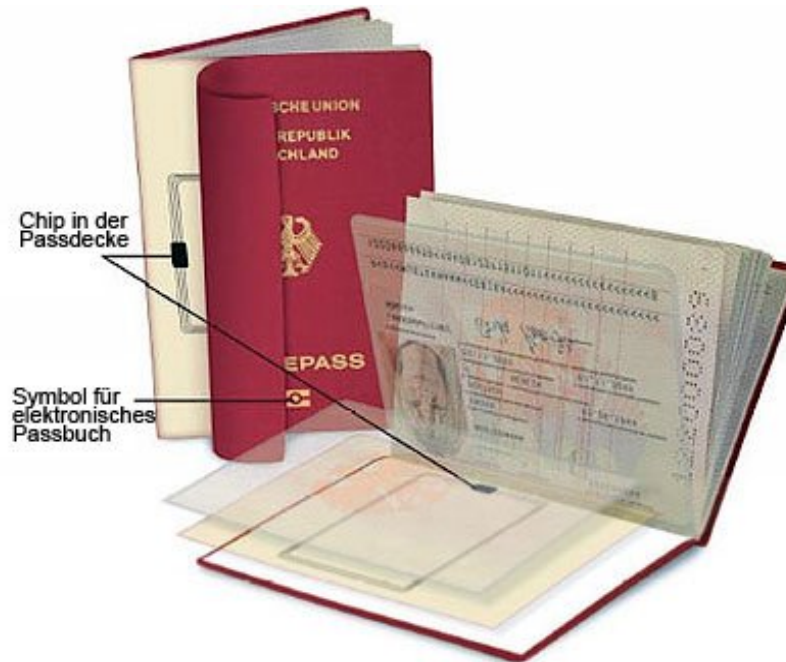
MRTD

- Machine Readable Travel Document
= Electronic Passport (ePassport, ePass)
- Spezifikation durch die ICAO
 - International Civil Aviation Organization, Unterorganisation der UN
- eingeführt auf globaler Basis





Deutscher ePass



- RFID Tag in die Hülle integriert
- Hergestellt von der Bundesdruckerei GmbH
- **Bald auch elektronischer Personalausweis (Chipcard)**

MRTD nach ICAO

- Auf einem RFID Tag werden persönliche Daten und biometrische Daten gespeichert
 - ICAO Standard deckt auch alternative Methoden wie 2D-Barcodes ab
 - Gemeinsamer Standard für Interoperabilität
 - Neben vorgeschriebenen Merkmalen gibt es auch optionale Merkmale

MRTD Daten-Layout

- LDS (Logical Data Structure)
 - Daten werden in DG (Data Groups) gespeichert
 - DG1: MRZ Information (mandatory)
 - DG2: Portrait Bild + biometrisches Template (mandatory)
 - DG3 / DG4: Fingerabdrücke, Iris-Bild (optional)
 - EF.SOD: Security Object Data (kryptographische Signaturen)
 - EF.COM: Liste der existierenden Data Groups
- Daten werden in BER-encoded ASN.1 Strukturen gespeichert
- DG2-DG4 benutzen CBEFF – Codierung
 - common biometric file format, ISO 19785



MRTD

Sicherheitsmerkmale

- Zufällige UID für jede Aktivierung
 - normalerweise haben alle ISO 14443 Transponder eine feste eindeutige Seriennummer
 - Die UID wird für den Anti-Kollisionsmechanismus benötigt.
 - Verhinderung der Verfolgung des Trägers ohne vorherige Zugriffskontrolle (Verhinderung einer „Anti-USA-Bürger-Bombe“)
 - Problem: ICAO MRTD Spezifikationen verlangen keine zufällige Seriennummer
 - Nur einige Ländern werden eine zufällige UID verwenden.

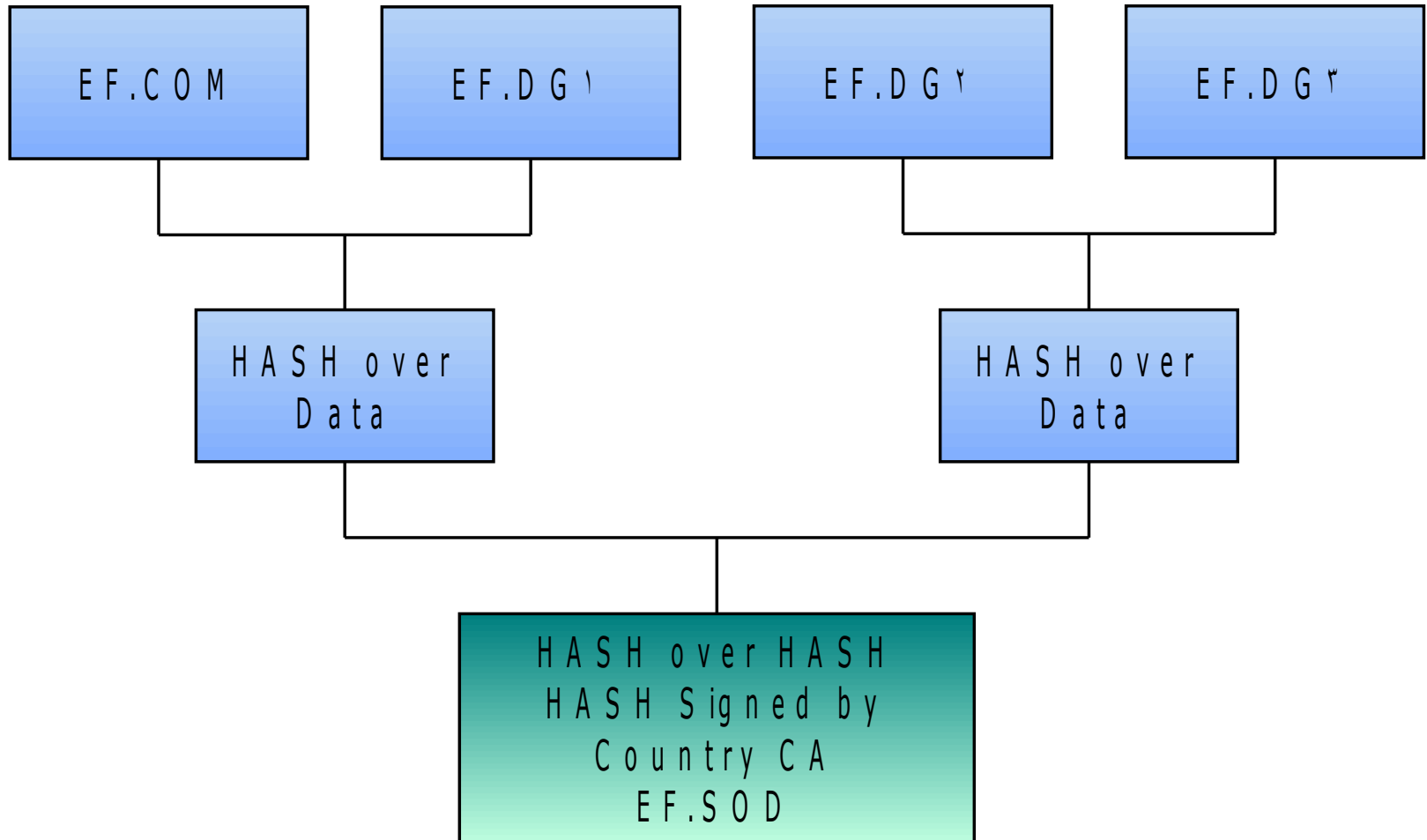


Passive Authentifizierung

- Vorgeschrieben für alle MRTD
- stellt sicher, dass die MRTD/Passport-Daten durch das ausgebende Land elektronisch signiert sind
- Das Lesesystem muss die Hash-Werte der DGs überprüfen:
 - EF.SOD enthält individuelle Signaturen für jede DG
 - EF.SOD ist selber signiert
 - Document Signer Public Key muss durch PKD / bilaterale Kanäle bekannt sein
 - Document Signer Public Key kann auf dem MRTD gespeichert sein
 - Nützt nur etwas, wenn der Country Root CA public key bekannt ist



Signierte Daten





Basic Access Control BAC

- Erlaubt Zugriff auf die Daten, nachdem das Lesegerät autorisiert wurde
- Autorisierung über die Machine Readable Zone (MRZ)
 - 9-stellige Dokumentennummer
 - In einigen Ländern: Ausgebende Behörde + fortlaufende Nummer (kann dann leicht geraten werden)
 - 6-stelliges Geburtsdatum
 - Kann geraten oder als gültig angenommen werden
 - 6-stelliges Verfallsdatum
 - 16 most significant Bytes des SHA1-Hash über MRZ-Info (3DES Schlüssel für S/M (ISO7816 secure messaging) werden benutzt
 - Beim deutschen ePass in 2. Generation und ePA bessere Entropie durch Zufügen einer weiteren Zahl

Password Authenticated Connection Establishment PACE

- Absicherung des Kanals zwischen Reader und Chip
- Patentfrei, starke Verschlüsselung
- **6-stellige PIN**
 - Soll entgegen anderer Pressemeldungen (Heise Ticker) nicht aufgedruckt werden
 - Aber: auch die Feldversuche zur Gesundheitskarte zeigten starke Nutzer-Probleme mit der PIN-Anwendung/Verwendung
- Problem: Fotokopien des Personalausweises werden an vielen Stellen angefertigt und können unkontrolliert kursieren



Extended Access Control EAC

- optionales Verfahren (Deutschland wendet es an für Fingerabdrücke)
- Soll den unerlaubten Zugriff auf biometrische Daten verhindern (außer Passbild)
 - nicht international standardisiert
 - von den ausgebenden Behörden individuell implementiert
 - nur ausgewählten Ländern wird der Zugang gestattet

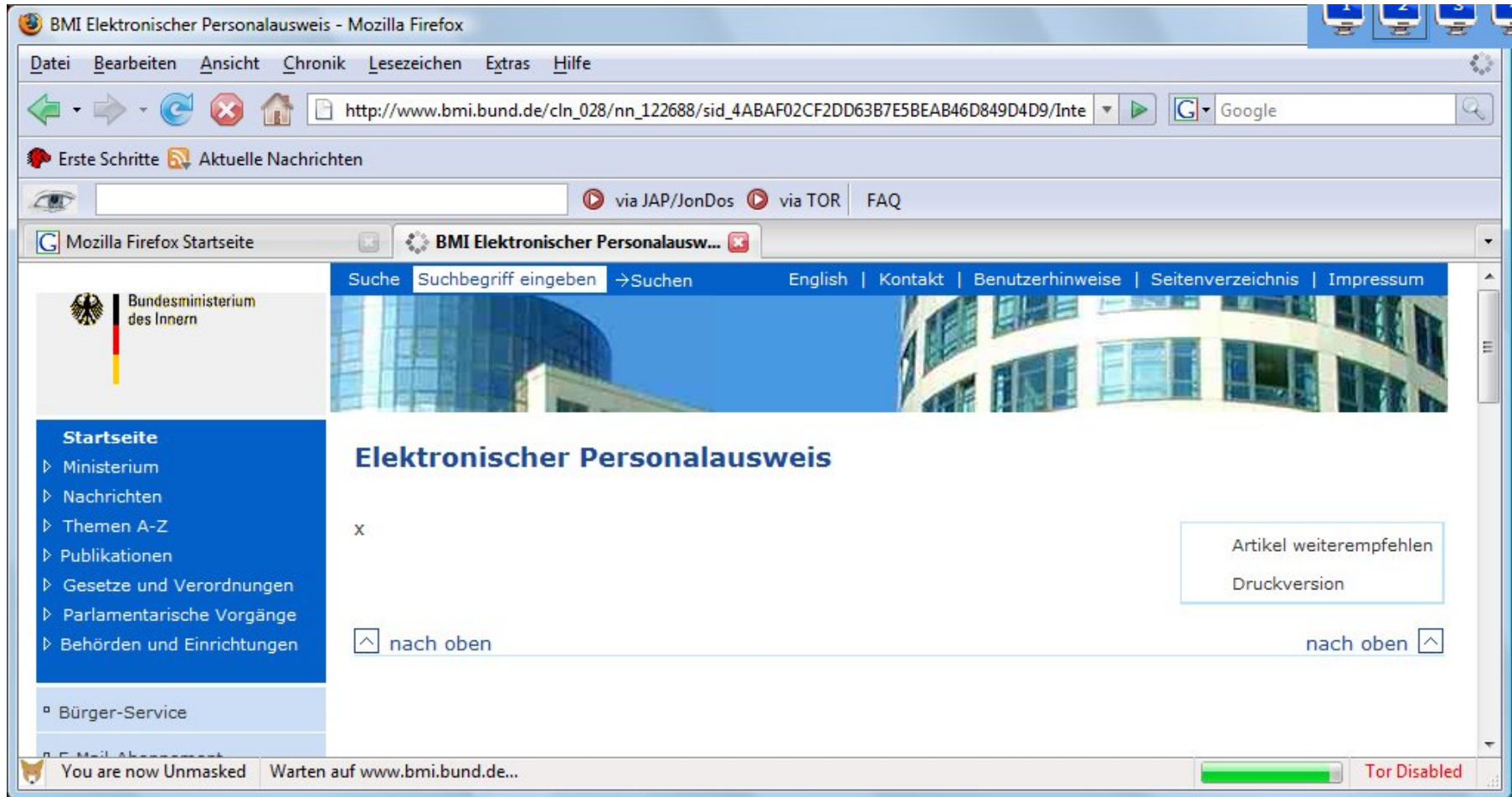
Klonen von ePässen

- „Dual Interface Tags“ können als MRTD Tag fungieren
- Daten können von einem echten ePass ausgelesen werden
- Geklonte ePässe verhalten sich für RFID identisch zu offiziellen ePässen
 - „http://stream.servstream.com/ViewWeb/BBCWorld/File/worl_click_141206_one_hi.aspx?Media=77526“
 - <http://archiv.tagesspiegel.de/archiv/10.02.2007/3053670.asp#>
 - Technology Review, Februar 2007, Seite 91/92
 - SAT1 "Planetopia", 1.10.2006, Gefahren von RFID in elektronischen Reisepässen

Verfügbare Informationen

- Suche nach „elektronischer Personalausweis“ auf www.bmi.bund.de (Suchfeld) ergibt folgenden Link:
- http://www.bmi.bund.de/cln_028/nn_122688/SiteGlobals/Forms/Suche/serviceSucheFormular,templateId=processForm.html?resourceId=122734&input_=&pageLocale=de&searchEngineQueryString=elektronischer+personalausweis&submit=Suchen&sortString=-score&searchArchive=2&searchIssued=0&path=%2FSites%2FBMI%2FInternet%2F&maxResults=5000
- **1. Elektronischer Personalausweis**
Wesentliches Kennzeichen des neuen Dokumententyps ist ein Chip zur Speicherung der Ausweisdaten, mit dessen Hilfe sich der Dokumenteninhaber auch im Internet sicher ausweisen kann. Der elektronische Personalausweis macht die Personenidentifikation sicherer und komfortabler. 90% 18.08.2006
- **Grobkonzept zum ePA – August 2008**
http://www.bmi.bund.de/cae/servlet/contentblob/122648/publicationFile/9169/Grobkonzept_Personalausweis.pdf
(116 Seiten)

Verfügbare Informationen



Lobby-driven Security

- Sicherheit lässt sich nicht durch Mehrheitsbeschluss herbeizaubern
- Kompromisse sind typisch für Lobby-Arbeit
- → Sicherheit passt nicht zu Lobby-Arbeit
- ICAO-Standard
 - Zu kompliziert, jeder Teilnehmer wollte sein Lieblingsspielzeug dabei haben (RFID statt 2D Barcode etc)
 - Eigene Algorithmen und „Standards“ statt bewährter und getesteter Off-the-shelf Technologien
 - Nicht hauptsächlich von Security Spezialisten gemacht
- Elektronischer Personalausweis:
 - Zugang auch für nicht-hoheitliche Stellen mit ganz anderen Interessen

Chaos der Standards

- TLV and ASN.1 sind nicht korrekt implementiert
- Redundante Meta Formate für biometrische Daten
- Wenn der unterschreibende Schlüssel eines Landes unzuverlässig/geklaut ist, ist das Land verloren
 - es gibt *keinen* Weg, ein MRTD-Zertifikat zurückzurufen!
- Die Daten müssen erst vom Lesegerät komplett gelesen und ausgewertet/interpretiert werden, *bevor* sie verifiziert werden können
- Design wurde durch politische Kompromisse erreicht, nicht von IT-Security Experten
- Daten können manipuliert werden



ePA: Ziel der Einführung

- „Die Bundesregierung bereitet **für eine sichere gegenseitige Identifizierung im Internet** die Einführung des elektronischen Personalausweises (ePA) vor.“
- ePA enthält eine optionale **qualifizierte** digitale **Signatur**. (entspricht *notariell beglaubigter* Unterschrift)
- Mit dem ePA „stellt der Staat .. ein Ausweisdokument zur Verfügung, das **eBusiness** sicherer macht“.
- BITKOM schwärmt von der **Bürgerkartenfunktion** des ePA.
- Mit dem ePA „könne ... eine Art **Standard-Authentisierung** geschaffen werden“.
- **Online-Geschäfte, Finanztransaktionen, eGovernment**
 - Was hat das mit einem **Ausweis** zu tun?

ePA: Funktionen laut BSI

- **ePersonalausweis-Funktion**
 - Analog zum ePass, mit Biometrie
 - Nur für **hoheitliche Aufgaben**
- **eID-Funktion**
 - **Opt-Out**, kann auf Wunsch bei der Auslieferung ausgeschaltet werden
 - Persönliche und dokumentenbezogene Daten
 - z.B. **Name, Adresse, Ablaufdaten, keine Biometrie**
 - Verwendung für eGovernment und eBusiness
- **Qualifizierte elektronische Signatur**
 - **Opt-In**, nur auf Antrag des Inhabers, zusätzliche Kosten

ePA: eID + Signatur

	Traditionell	Elektronisch	
		Wissen	Wissen + Besitz
Identifizierung	Vorlage des Personalausweises	Username + Passwort	Neu: eID
Transaktion	Unterschrift	TAN	elektronische Signatur

- ePass Funktion zur Identifizierung
- Signatur für die Transaktion

Ausweise in Europa (BSI)

- **Belgien**
 - Keine Biometrie
 - Personaldaten und eID-Zertifikat **ohne Zugriffsschutz**
- **Niederlande**
 - Gesichtsbild und Personendaten mit **BAC**
- **Italien**
 - Gesichtsbild/Fingerabdrücke **ohne Zugriffsschutz**
 - **eID mit PIN**
- **Spanien**
 - Gesichtsbild/Fingerabdrücke **ohne Zugriffsschutz**
 - Zertifikat für Signatur, **keine separate eID**

And
(Grc

stems

Merkmal	Land						
	Belgien	Estland	Italien	Schweden	Hongkong	Spanien	Niederlande
Kosten f. Bürger (EUR)	10	10	25	42	keine (40 für Ersatzdokument)	7	31
Gültigkeit	5 Jahre	10 Jahre	5 Jahre	5 Jahre	unbefristet	10 Jahre	5 Jahre
Chip/ Interface	Kontaktchip	Kontaktchip	Kontaktchip und Laserstreifen	Kontaktchip und kontaktloser Chip	Kontaktchip	Kontaktchip	Kontaktloser Chip
Biometrie	nein	nein	ja (Gesichtsbild und Fingerabdrücke)	ja (Gesichtsbild)	ja (Gesichtsbild und Daumen)	ja (Gesichtsbild und Fingerabdruck-Template)	ja (Gesichtsbild)
Zertifikate	Authentisierung/elektron. Signatur	Authentisierung/elektron. Signatur	Authentisierung/elektron. Signatur	nein	Authentisierung/elektron. Signatur	Authentisierung/elektron. Signatur	nein
Zugriffsschutz für Biometrie- und Personendaten	kein	kein	kein	BAC	kein	kein	BAC
Speicherung Wohnanschrift	nur im Chip gespeichert	nein	nein	nein	nein	nein	nein

13. Jur

Tabelle 11: Merkmale der elektronischen Personalausweise anderer Länder



Datenschutz (BSI)

- Zugriff nach Eingabe einer geheimen PIN
 - Erfahrungen mit Gesundheitskarte-Feldversuch (6-stellig?)
- Zugriff nur durch zertifizierte Dienstanbieter
 - Überprüfung der Zertifikate durch den Chip
 - Aber: der hat keine Uhr ...
 - Zertifikat-Rückruf nicht möglich
 - Was passiert, wenn Dienstanbieter Zertifizierung verliert?
 - Was passiert, wenn Zertifizierungunternehmen verschwindet?
- Auslesen nur über verschlüsselten Kanal

Zugriffsrechte (BSI)

- **Feldgenaue Zugriffsrechte**
 - Zertifikat des Dienstanbieters enthält Zugriffsrechte für einzelne Felder
 - Durch PIN-Eingabe weiter einschränkbar
- Weitere Funktionen
 - **Altersverifikation** („älter als ...“ ohne Geburtsstagsangabe)
 - Nur eine Abfrage pro PIN-Eingabe
 - **Dokumentengültigkeit** (abgelaufen ja/nein)
 - **„restricted Identity“**
 - **Anbieter kann Ausweise wiedererkennen ohne neue Übertragung der Personendaten**
 - Anbieterspezifisch, nicht universell für alle Anbieter



Anwendungen kommerziell (B2C)

- Online-Banking
- Versandhandel und Auktionen im Internet
- Internetservice allgemein
- Sichere E-Mail und Datensafe (Bürgerportale)
- Alterskontrolle
- Elektronischer Autoschlüssel
- Qualifizierte elektronische Signatur

Anwendungen eGovernment



Dr. Böttger
IT_Beratung + Projektmanagement

dn
Systems

- Online-Ummeldung
- ELSTER
- Internet-Auskunft aus Registern, Datenbanken und Verfahren
- Kfz-An- und Ummeldung
- Überprüfung gewerblich Beschäftigter

Anwendungen Wirtschaft

- Elektronische Prozeßabwicklung in der Wirtschaft
- Elektronische Prozeßabwicklung in der Verwaltung
- Zugangskontrollen
- Einloggen in IT-Systeme und Mitarbeiterportale

Vorschläge für die QES mit dem elektronischen Personalausweis

Dr. Böttger
IT_Beratung + Projektmanagement

dn
Systems

- ELENA (JobCard)
- Elektronisches Handels- und Unternehmensregister
- Elektronische Buchungen und Rechnungen

Anforderungen (BMI)

9.2.1.4 Anforderungen an das Ausweisdokument – Zusammenfassung

Lfd. Nr.	Anforderung
Elektronische Schnittstelle (Chip)	
TE.1	Der elektronische Personalausweis wird mit einem Chip ausgestattet, der eine kontaktlose Schnittstelle aufweist.
TE.2	Der Speicherchip ist so auszulegen, dass er die biometrischen Merkmale in elektronischer Form (Gesichtsbild und Fingerabdrücke des Inhabers) und eID-Daten sowie ein qualifiziertes Signaturzertifikat und die entsprechenden kryptographischen Schlüssel aufnehmen kann.
Physisches Kartenformat	
TE.3	Als Format für den Kartenkörper des elektronischen Personalausweises wird das Scheckkartenformat (ID1) vorgesehen.
TE.4	Der Ausweis muss einen Schichtenverbund aufweisen, der eine Separierung der echtheitssichernden Elemente von den datentragenden Schichten wirksam verhindert.
TE.5	Soweit möglich ist das Material selbst mit Sicherheitsmerkmalen auszustatten. Falls der Kartenaufbau kein Sicherheitspapier entsprechend dem bisherigen Personalausweis aufweist, ist eine Kompensation der Sicherheitsmerkmale des Papiers über die Mindestanforderungen in den übrigen Bereichen der sicherungstechnischen Ausstattung hinaus vorzusehen.
TE.6	Die Kartenoberfläche ist mit einer Sicherheitsprägung mit Mikroschrift- und Kippeffektmerkmalen auszustatten, nach Möglichkeit spezielle Formgebung des Kartenkörpers zur Unterscheidung von handelsüblichen Rohlingen.



Anforderungen

Lfd. Nr.	Anforderung
Gültigkeitsdauer	
TE.7	Gültigkeitsdauer des Dokuments ab Ausstellungsdatum: 10 Jahre, bei Personen unter 24 Jahren 6 Jahre Gültigkeit.
Haltbarkeit	
TE.8	Der elektronische Personalausweis muss hohen Anforderungen an Haltbarkeit und Gebrauchstauglichkeit genügen. Er muss die in einschlägigen Normen festgelegten Anforderungen zur Beständigkeit unter extremen klimatischen Bedingungen, Haltbarkeit unter mechanischer Belastung und Resistenz gegen Strahlung und chemische Einwirkungen erfüllen. Als Leitlinie sind die von ICAO im Technical Report on Durability of Machine Readable Passports ⁷ publizierten Anforderungen zu berücksichtigen.
Kopierschutz	
TE.9	Der elektronische Personalausweis ist mit hochgradig gegen digitale Reproduktions- und Kopiertechniken schützenden, optisch variablen Elementen als Sicherheitsmerkmalen auszustatten (z. B. durch vollflächige Integration eines individualisierten, optisch variablen Sicherheitselements auf der Kartenvorderseite, das mindestens die im bisherigen PA realisierten Sicherheitsfunktionen umfasst). Darüber sind kryptographische Vorkehrungen gegen das Kopieren bzw. Verifizieren des Chips zu etablieren (Chip Authentication).
Schutz gegen Manipulation/ Erkennung von Fälschungen	
TE.10	Zum Schutz der inhaltlichen Angaben sind Personenmerkmale, wie Lichtbild und Inhaberunterschrift durch sichere Verfahren in das Dokumentenmaterial zu integrieren.
TE.11	Die spezielle Ausstellungstechnik muss eine hochgradige Absicherung gegen Verfälschungsmanipulationen bewirken und von allgemein zugänglichen digitalen Drucktechniken eindeutig unterscheidbar sein.
TE.12	Es sind geeignete physikalische Sicherheitsmerkmale für eine maschinelle Echtheitsprüfung zu integrieren, die mindestens das technologische Niveau der in den bisherigen deutschen Ausweisdokumenten enthaltenen Maschinenprüfmerkmale aufweisen.
TE.13	Die auf dem Chip des ePA gespeicherten Daten sind mittels elektronischer Signaturen gegen Manipulationen zu schützen (Passive Authentication).

Tabelle 13: Anforderungen an das Ausweisdokument



Mögliches Aussehen (BMI)



Planung

Laut Grobkonzept BMI 2.Juli 2008:

Die technischen und organisatorischen Voraussetzungen sollen nach gegenwärtiger Planung bis Ende 2009 geschaffen werden. Die Durchführung der erforderlichen Pilotierungs- und Feldtestmaßnahmen ist von Mitte 2008 bis voraussichtlich Mitte 2009 geplant.

ePA: dual-use != security

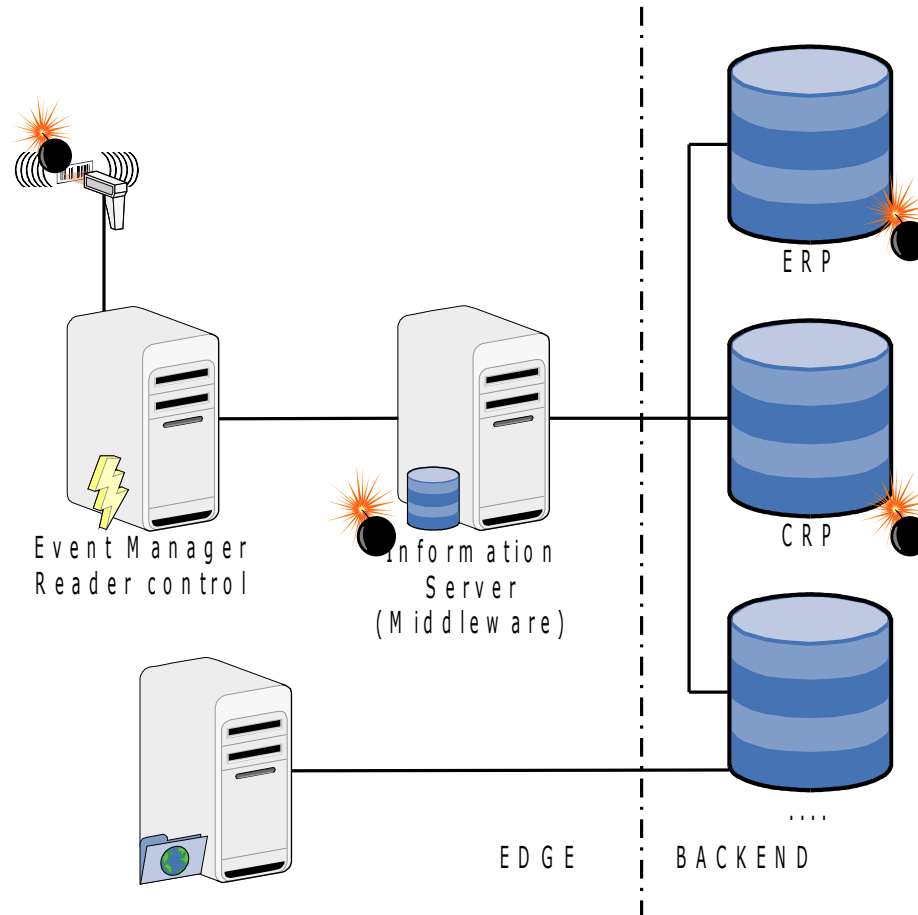
Advocatus diaboli sagt:

- Der ePA soll also auch für kommerzielles Identity-Management eingesetzt werden, z.B. im Internet
 - Das bringt Geld in die Staatskasse?
- Einsatz für qualifizierte digitale Signatur wird diskutiert
 - Ohne Zwang nutzt die ja fast niemand...
- Es besteht die Gefahr, dass wirtschaftliche Interessen das Design und das praktische Enrollment aus Sicherheits-Sicht ungünstig beeinflussen.
- <http://de.internet.com/index.php?id=2040983>
- <http://www.internet-sicherheit.de/fileadmin/docs/publikationen/Dietrich-ePA-CeBIT-2008-datakontext-forum.pdf>

IT Sicherheitsrisiken

- UID könnte verändert werden
- ePass-Tag könnte als Zugangs-Tag in anderen Zusammenhängen benutzt werden
- Manipulierte DGs (z.B. JPEG2000) könnten die Lesegeräte zum Absturz bringen
 - erfolgreich demonstriert mit den Geräten mehrerer Länder
 - <http://www.heise.de/newsticker/meldung/93723>
 - Wenn man einen Absturz provozieren kann, kann man vermutlich auch Schadprogramme einbringen

Einbruch in das System





Organisation

- Das Problem mit der Identität lässt sich
 - nicht nur durch Technologie lösen
 - nicht vollkommen automatisieren
 - Es muss in einen Organisationsprozess eingebunden werden.
 - Es muss immer kostenorientiert aufbereitet werden.

ePass / ePA - 1

- ICAO Spezifikation steht konträr zu den „Best Practices“ für die Absicherung von Informationssystemen:
 - bisher geschlossenes Kontrollsystem (optische Leser für MRZ) werden geöffnet (RFID). Gefahr von Angriffen auf die Lesestationen.
 - BAC-Schlüssel ist auf dem MRTD aufgedruckt.
 - Handling PACE in der Praxis durch Nutzer unklar
 - Schloss und Schlüssel liegen zusammen vor. In vielen Ländern ist es **vorgeschrieben**, Fotokopien des Passes z.B. in Hotels zu machen...

ePass / ePA - 2

- ICAO Spezifikation steht konträr zu den „Best Practices“ für die Absicherung von Informationssystemen:
 - Gültigkeit des EAC Schlüssels kann vom MRTD nicht geprüft werden, da kein Zeitnormal vorliegt (MRTD hat keine eingebaute Uhr). Ein Rückrufmechanismus für Schlüssel existiert nicht. Verwendet wird der Zeitstempel des letzten Zugriffs. Möglichkeit der Entwertung durch bewusst falsche (zukünftige) Zeitstempel durch Angreifer. Schreibschutz auf dem MRTD muss wegen der Zeitstempel aufgehoben werden.

ePass / ePA - 3

- Sicherheit der Datenübermittlung
 - für EAC muss online bei einer zentralen Stelle angefragt werden
 - kein EAC und damit auch keine neuen Pässe für Auslandsdeutsche in „nicht vertrauenswürdigen“ Ländern
 - Technologie stellt nur einen kleinen Teil dar, organisatorische Maßnahmen fehlen im Gesetz
 - Es ist anscheinend noch nicht einmal der gleiche Standard wie bei der Übermittlung von Kontodaten von Banken an das BAFin festgeschrieben



ePass / ePA - 4

- BAC: Schlüssel kann aus MRZ generiert werden
 - MRZ durch Fotokopie des MRTD erhältlich (Flugreisen, Hotels, Mietwagen, ...)
- PACE: Schlüssel-Handhabung (Gesundheitskarte...) unklar
- Auch ohne Auslesen der Daten kann durch reinen Verbindungsaufbau mit BAC ein Bewegungsprofil aufgezeichnet werden
- Auslesen des Passbildes mit BAC beschert dem Angreifer ein Biometrie-geeignetes Bild des Opfers
- Auslesen der BAC-geschützten Daten kann nicht bemerkt bzw. nachgewiesen werden
- Pass sollte nicht nur in Deutschland „sicher“ sein: ein Pass ist schließlich gerade zum Einsatz im Ausland gedacht



ePersonalausweis

- grundsätzlich gleiche Technik wie beim ePass
- Zusätzlich PACE – technische Bewertung noch nicht möglich; Erfahrungen mit PIN bei Gesundheitskarte negativ
- Fingerabdrücke durch EAC geschützt
- **► Kryptographie ist nicht das Problem, sondern der Rest des Standards**
- **Organisation kritisch:** langer Weg vom Fingerabdruck-Scanner im Bürgerbüro bzw. Lesegerät „auf Streife“ bis zur zentralen Datei. Ist wirklich jeder Schritt und jedes Kabel „sicher“?
- **erkennungsdienstliche Erfassung aller Bürger ab 16 Jahren**
 - Polizei / Ermittler - Wunschtraum
 - Bürger-Albtraum
 - Generalverdacht für alle?

Fragen ?



Thank You



Dr. Böttger

IT_Beratung + Projektmanagement

Dr. Christian Böttger

Bentestraße 10

31311 Uetze

Phone: +49.5173.9249744

Mail: c.boettger@boettger-consulting.de

<http://www.boettger-consulting.de/>



13. Juni 2009



DN-Systems GmbH

Hornemannstr. 11-13

31137 Hildesheim, Germany

Phone: +49-5121-28989-0

Mail: info@dn-systems.de

<http://www.dn-systems.de/>

DN-Systems International Limited

P.O. Box 285 282

Dubai · U.A.E.

Phone: +971-50-2861299

Mail: info@dn-systems.com



- Über DN-Systems
- Weltweiter Service
- Kunden DN Systems
- Vorstellung Person
- Themen
- Einführung: Was ist RFID?
- Datenmanipulation (Beispiel)
- Generische Angriffe
- Generische Angriffe
- Generische Angriffe
- Generische Angriffe