

Internationale Aktivitäten und
Standardisierung -
Focus Chipkarten und Europa
Bitkom Forum
Digitale Identitäten – Basis einer
vernetzten Welt 10 2006

Dr. Gisela Meister



Giesecke & Devrient

Agenda

Kurzvorstellung G&D

- Europäische Chipkarten Standardisierungsgremien
- Inhalte
- Beispielanwendungen in der EU
- Umsetzung ECC in Deutschland
- Herausforderungen und Chancen der ECC



European Citizen Card



Giesecke & Devrient

Unsere Vision:



Wir sind weltweit *der* Partner des Vertrauens in der Sicherung von Werten!

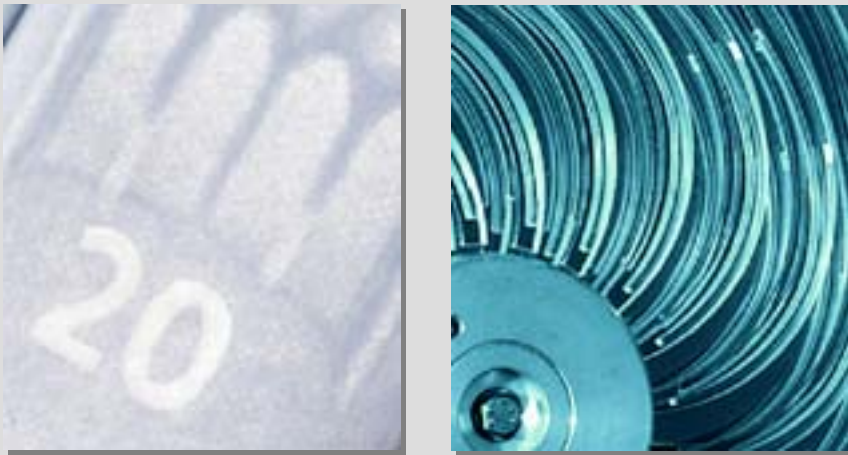
European Citizen Card



Giesecke & Devrient

Produkte und Leistungen

Banknote



Papier und Druck

- für Banknoten
- Sicherheitspapier / -folien
- Anlagenbau
- Service für Druckereien

Banknotenbearbeitung

- Banknotenbearbeitungssysteme und -identifizierungsmodule
- Sicherheitsmerkmale und Sensortechnologie
- Service und technischer Support

Cards and Services



Cards and Services

- für den elektronischen Zahlungsverkehr
- für die mobile Kommunikation

European Citizen Card



Giesecke & Devrient

Produkte und Leistungen

Government Solutions



Systemlösungen für

- ID-Dokumente
- Reisepässe
- Gesundheitskarten
- Personennahverkehr
- Sicherheitsdruck
- Produkt- und Markenschutz
- IT-Sicherheit

New Business



Technologien für neue Märkte

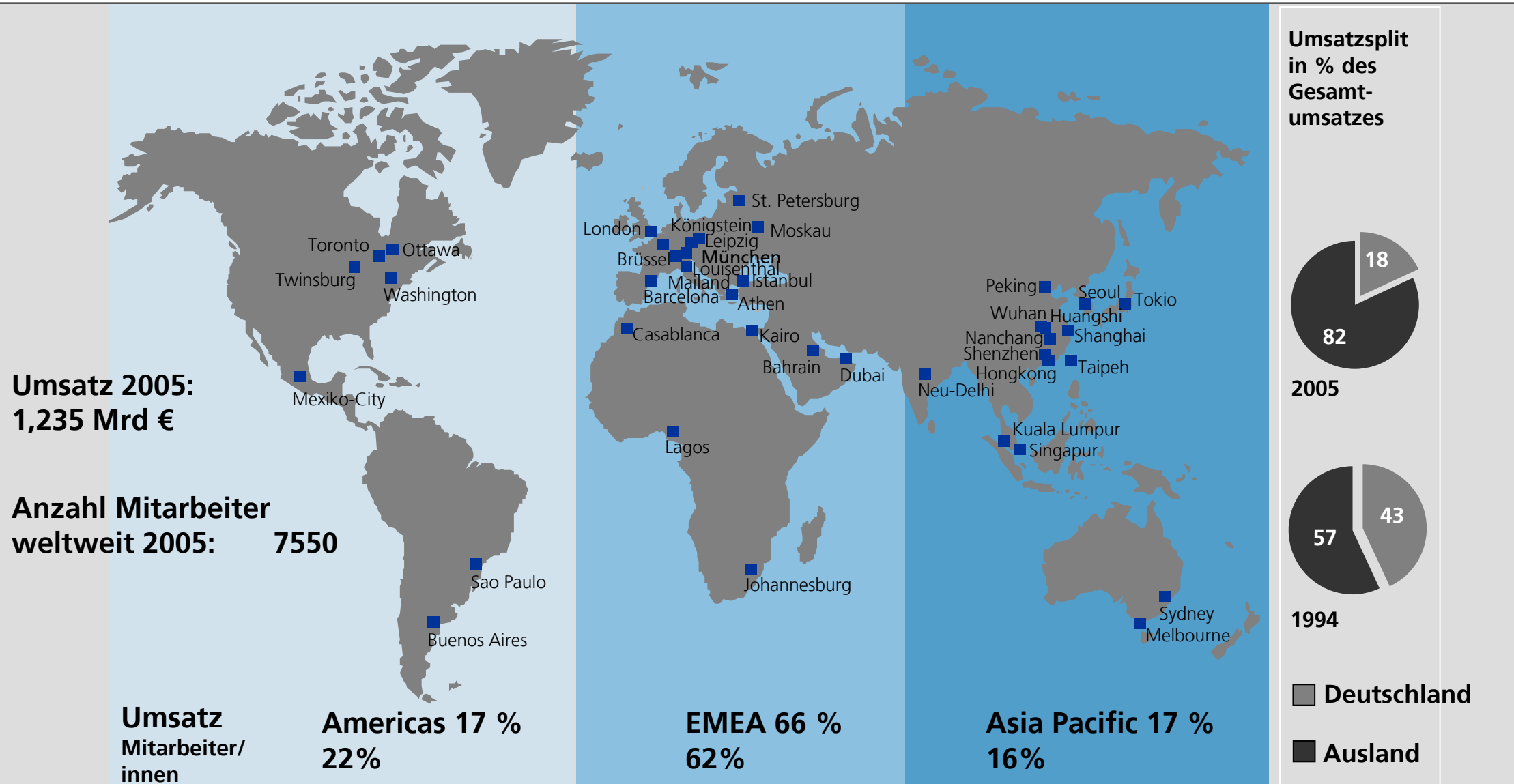
- IT-Sicherheit
- Sicherheitssysteme in industriellen Anwendungen
- Secure Embedded Systems
- Neue Technologien / Applikationen / Partnerschaften

European Citizen Card



Giesecke & Devrient

Weltweite Präsenz des G&D Konzerns



European Citizen Card



Giesecke & Devrient

Agenda

- Kurzvorstellung G&D
- Europäisches Standardisierungsgremien
- Services für Grenzkontrolle und PKI
- Beispielanwendungen in der EU
- Umsetzung ECC in Deutschland
- Herausforderungen und Chancen der ECC



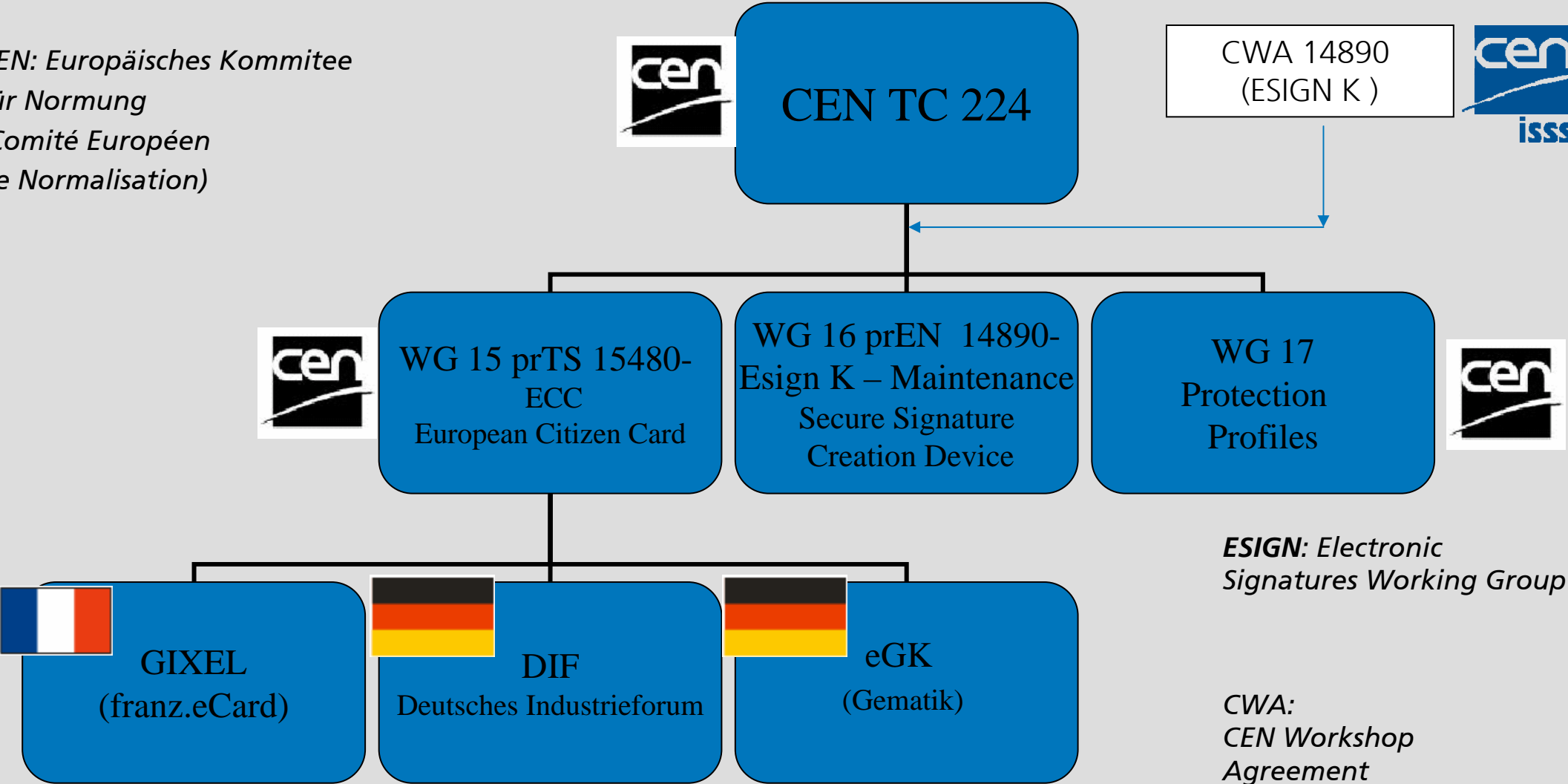
European Citizen Card



Giesecke & Devrient

Europäische Standardisierungsgruppen – und Anwender

CEN: Europäisches Komitee für Normung
(Comité Européen de Normalisation)



ESIGN: Electronic Signatures Working Group

CWA:
CEN Workshop Agreement

European Citizen Card



Standardisierung Europäische Bürgerkarte

■ Zuständiges Normungsgremium: CEN TC224 WG15 (Chair, L. Gaston, Gemalto)

■ prTS 15480 European Citizen Card

- ECC-1 : Physical Interfaces (in finale Abstimmung)
- *ECC-2 : Logical Data Structure (TF Chair, Dr. G. Meister G&D) (in finaler Abstimmung)*
- ECC-3 : Personalisierung & Middleware (Profil zu ISO /IEC 24727, gestartet)
- ECC-4: Benutzer – Profile zu ECC-1 und ECC-2 (neu)

■ Sektorübergreifendes Normungsgremium für IAS Services auf der Karte (Chair, Dr. G. Meister G&D)

- CEN TC224 WG16 (Maintenance E-SIGN K)
- prEN 14890 : Application Interface for Smart Cards used as Secure Signature Creation Devices (preliminary European Norm)
 - Part 1: Basic Services,
 - Part 2: Additional Services
- basiert auf CWA 14890 (“E-SIGN K”) allgemein durch alle Kartenhersteller in Europa für IAS (Digitale Signaturen) umgesetzter “Standard”)

European Citizen Card



Giesecke & Devrient

Agenda

- Kurzvorstellung G&D
- Europäisches Standardisierungsgremien
- Services für Grenzkontrolle und PKI
- Beispielanwendungen in der EU
- Umsetzungsmöglichkeiten der ECC in Deutschland
- Herausforderungen und Chancen der ECC



European Citizen Card



Giesecke & Devrient

Dienstleistungen der ECC-2 - Service orientiert nach kontaktbehaftetem und /oder kontaktlosem Interface

■ Datenschutz durch Etablierung

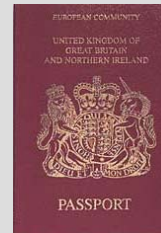
■ Kontaktbehaftetes Interface - *End to End Security*

- Geräteauthentisierung
mit Session Key
Vereinbarung zur
Absicherung von IAS
Diensten (z.B. digitale
Signatur) ref. nach
prEN 14890

eines *Trusted Channels*

■ Kontaktloses Interface - zusätzlich *Benutzer-initiiert*

- BAC / EAC Protokoll bei
Ausweisfunktion ref.
nach ICAO 9303 / EU
Passport Direktive auf
der Basis des BSI TR
- *Erweiterter
Handlungsbedarf zur
Absicherung von IAS
nach BSI/ DIF)*



European Citizen Card



Giesecke & Devrient

Dienstleistungen der ECC-2 - Services orientiert nach Anwendungskontext

■ Ausweisfunktion

- Referenzierung der ICAO 9303 Standards (LDS und PKI) mit
 - Passiver Authentisierung mit Zertifikaten
 - Basic Access Protokoll zum Schutz der Gesichts-Biometrie und zum Auslesen der Zertifikate
- Referenzierung des Technischen Reports (BSI) zum
 - Extended Access Control (EAC) Protokoll

■ Bürgerkarte

- Bereitstellung der IAS Services Identifikation, Authentisierung, Signatur nach prEN 14890

Bereitstellung der IAS Services Identifikation, Authentisierung, Signatur

■ Karten-basierte Services

- Geräteauthentisierung - Basis RSA oder Elliptische Kurven GF(p)
 1. Echtheitsprüfung der Karte und des Terminals
 2. Autorisierung (CV Zertifikate)
 3. Trusted Channel Etablierung (Datenschutz)
- Benutzer – Identifikation/ Authentisierung per Biometrie (Fingerprint) und / oder Passwort (PIN / PUK) nach prEN 14890

■ Benutzer orientierte Services nach prEN 14890 - Basis RSA oder Elliptische Kurven GF(p))

- Verschlüsselung (Key – Decipherment)
- Client Server Authentisierung
- Rollenbezogenes ID – Management
- Elektronische Signatur (advanced / qualified)



European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

European Citizen Card



Giesecke & Devrient

Agenda

- Kurzvorstellung G&D
 - Europäisches Standardisierungsgremien
 - IAS Services
- ## Beispielanwendungen in der EU
- Umsetzung ECC in Deutschland
 - Herausforderungen und Chancen der ECC



European Citizen Card



Giesecke & Devrient

Überblick europäische eID Karten



Bereits eingeführte eID Karten

- Finnland
 - Signaturkarte,
 - keine Ausweispflicht
 - derzeit keine Biometrie
- Estland
 - Signaturkarte
 - Ausweispflicht
 - derzeit keine Biometrie,
 - vom Staat vergebene offizielle email Adresse im Zertifikat gespeichert
- Belgien
 - Signaturkarte
 - Ausweispflicht,
 - derzeit keine Biometrie

eID Karten in Planung

- Frankreich
 - Basiert auf IAS Spezifikationen der GIXEL Gruppe
 - Mehrere Ministerien beteiligt; durch MOI Team geleitet
 - Anwendungsfälle: eGovernment und Digitale Signatur
 - Anwendungskontext für den zivilen Bereich
 - ICAO 9303 kompatible LDS (Logical Data Structure) wie ePass
 - ECC und ICAO 9303 kompatibel
- Portugal
 - März 2006 : Proof of Concept & Kick Off durch Premierminister
 - 2007: Testpiloten in Açores
 - 2008 - 2011: Ausgabe von 10 Mio Karten
 - 5 Ministerien beteiligt (Justice, Finance & eAdmin, Social Affairs, Health)

European Citizen Card

 Giesecke & Devrient

Agenda

- Kurzvorstellung G&D
- Europäisches Standardisierungsgremien
- Inhalte der EU Spezifikation
- Beispielanwendungen in der EU
- Umsetzung ECC in Deutschland
- Herausforderungen und Chancen der ECC



European Citizen Card



Giesecke & Devrient

- Gründungsmitglieder / Organisations -
Kommittee
 - Giesecke & Devrient
 - Bundesdruckerei
 - Infineon
- Arbeitsgruppen
 - AG 1 Karten (Chair G. Meister / G&D)
 - AG 2 Terminal (Chair S.Vater, SCM /
H. Boos , BSI)
 - AG 3 Middleware (A. Fiedler, Orga)



- Kommentierungskreis / AG – Teilnehmer
 - Industrieunternehmen (Siemens BS,
T- Systems, Philips, Gemplus
Deutschland, Microsoft Deutschland,..)
 - Bundesministerien, Ämter wie BSI
und bmi un Datenschutzbeauftragte
 - Liaison: Normierungsgruppen (DIN,
CEN, ...)

Beitrag des Deutschen Industrieforums (DIF) 2006 zum ePA

- Unterstützung des BSI bei der Erstellung von Schnittstellen-Dokumenten Karte, Terminal und Middleware, Management im Kontext eID und ePA

- Berücksichtigung der von BMI / BSI vorgegebenen Anforderungen

- Positionsermittlung für nationale und europäische Gremien

- Unterstützung des DIN bei der Erstellung von europäischen und international relevanten Standards zum Thema eID

- Diskussion/ Ermittlung der deutschen Position

- Aktive Mitarbeit bei Europäischen Gremien CEN TC 224 WG 15 / WG 16 / Eurosmart (?)

Auszug aus Vortrag Andreas Reisen(BMI, Referat IT4) in Wien, 06./07.07.2006



Project Report: Plannings of a German eID Card

Schedule:

Introduction of a German eID Card in 2008

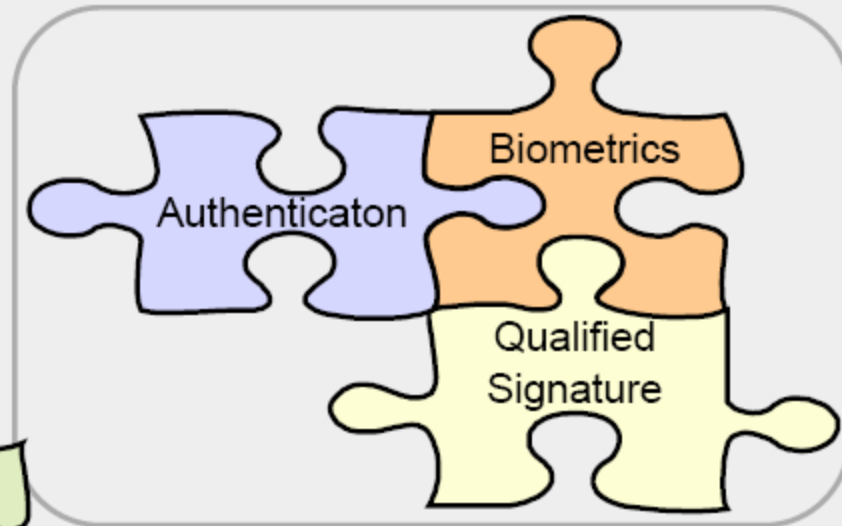
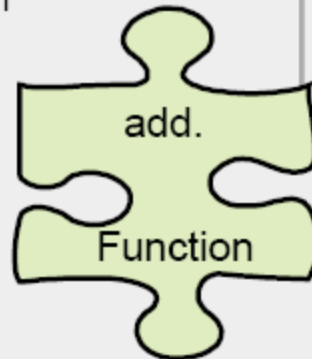
Legal basis:

Revised national ID card law in planning

Planned Functions:

- Biometrics (according to ePass)
- Electronic authentication
- Qualified signature

→ Modular concept
to increase
acceptance for an
eID Cards standard



Aufbau einer Europäischen Bürgerkarte *mit DIF Beteiligung*

- Sichere visuelle Identifikation (Bild, Sicherheitsmerkmale)
- Nutzung des ID-1 Karten- Formats
- Mikroprozessorkarte mit grossem Speicher
- *kontaktbehaftetes oder kontaktloses Interface*
- *Sicherheitsprotokolle zum Schutz der Privacy*
- *Unabhängigkeit der Schnittstelle von der Implementierung - Native und Java Cards*
- CC Evaluierung basierend auf standardisierten Protection Profiles
- *Nationale / Sektorspezifische Profile*
 - *kontaktlos / eID / Elliptische Kurven*
- *ePass Applikation (Biometrie) zum vereinfachten Reisen innerhalb Europas (optionales on-card Fingerprint Matching)*
- *Authentisierungsapplikation für eGovernment und eBusiness (optional qualifizierte Signatur)*

Agenda

- Kurzvorstellung G&D
- Europäisches Standardisierungsgremien
- Inhalte der EU Spezifikation
- Beispielanwendungen in der EU
- Rolle des DIF zur eCard Strategie

Herausforderungen und Chancen der ECC



European Citizen Card



Giesecke & Devrient

Herausforderungen und Chancen der ECC in Europa

- Europa - weite Lesbarkeit durch eine standardisierte Middleware (ECC-3)
- Sicherstellung von Privacy Aspekten (insbesondere bei biometrischen Daten)
- Technische Realisierbarkeit und Kosteneffizienz durch Beteiligung der führenden Industriefirmen an der Spezifikation
- Technologieführerschaft europäischer Firmen
- Integration proprietärer Lösungen
 - Einige Europäische Länder haben schon unabhängig von der ECC eine proprietäre elektronische ID herausgegeben
- Nutzung für
 - eGovernment – Services auch auf lokaler Basis (Gemeinde) sowie
 - eBusiness (z.B. ebay)
- Sichere Identifikation sowie bequemes Reisen innerhalb Europa (ID-1 Dokument)

European Citizen Card



Thank you for your Attention

Contact:

Gisela Meister
Leiterin Security & Evaluation
Tel. +49 89 4119-1931
e-Mail: Gisela.Meister@de.gi-de.com

Giesecke & Devrient GmbH
Prinzregentenstr.159
81607 München