

Institut für
Informationsmanagement
Bremen GmbH

Introducing eID as a Multi-Facet Innovation

The German Case

Torsten Noack

DEXA – EGOV, 31.08.2009, Linz

Content

- eID-Card Characteristics
- Overview: eID-Card Timeline
- Actor Constellation
- Technological Paths
- Decision-Making Process Biometry
- General Conclusions

eID-Card characteristics - eID function

1. Use for eGovernment and eBusiness
2. Certificated identity - not only of the citizen: access only by certified service providers
3. Mutual authentication between ePA-chip and eID-terminal (service provider)
4. eID-Access only with citizen-PIN
5. Separate access rights for each data field
6. Data transfer only via encrypted channel
7. Function for using pseudonym access
8. Age verification without providing date of birth (boolean operation)

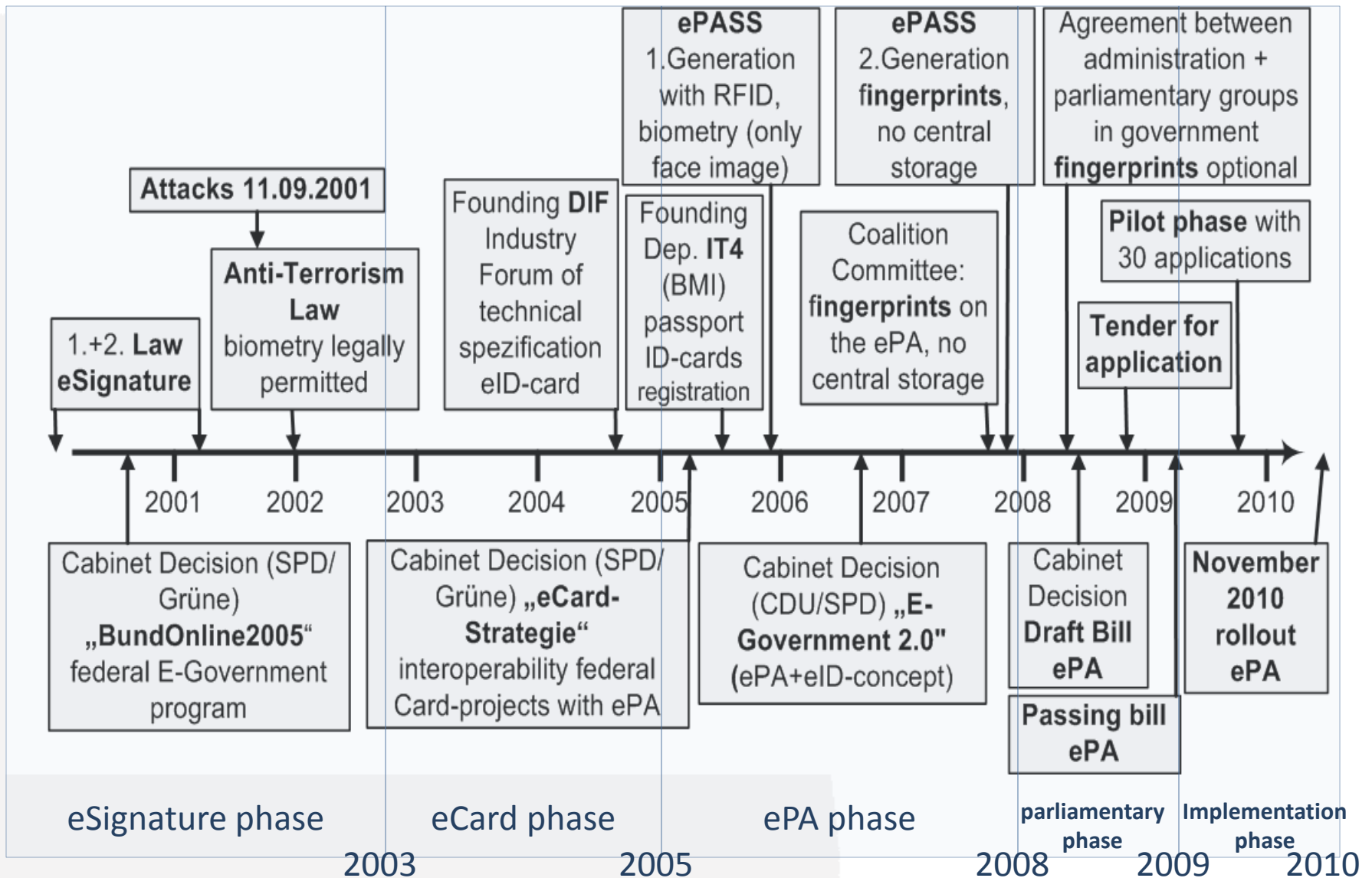
Service provider certification

1. Certification request of service provider (eGovernment + eBusiness) at Federal Office of Administration
2. Check of the purpose of the service and the safety specifications
3. Generation of the certificate from service provider PKI and https-certificate
4. Certificate with authorization contents is signed and transferred to the service provider
5. Service provider has now the access to the ePA-data

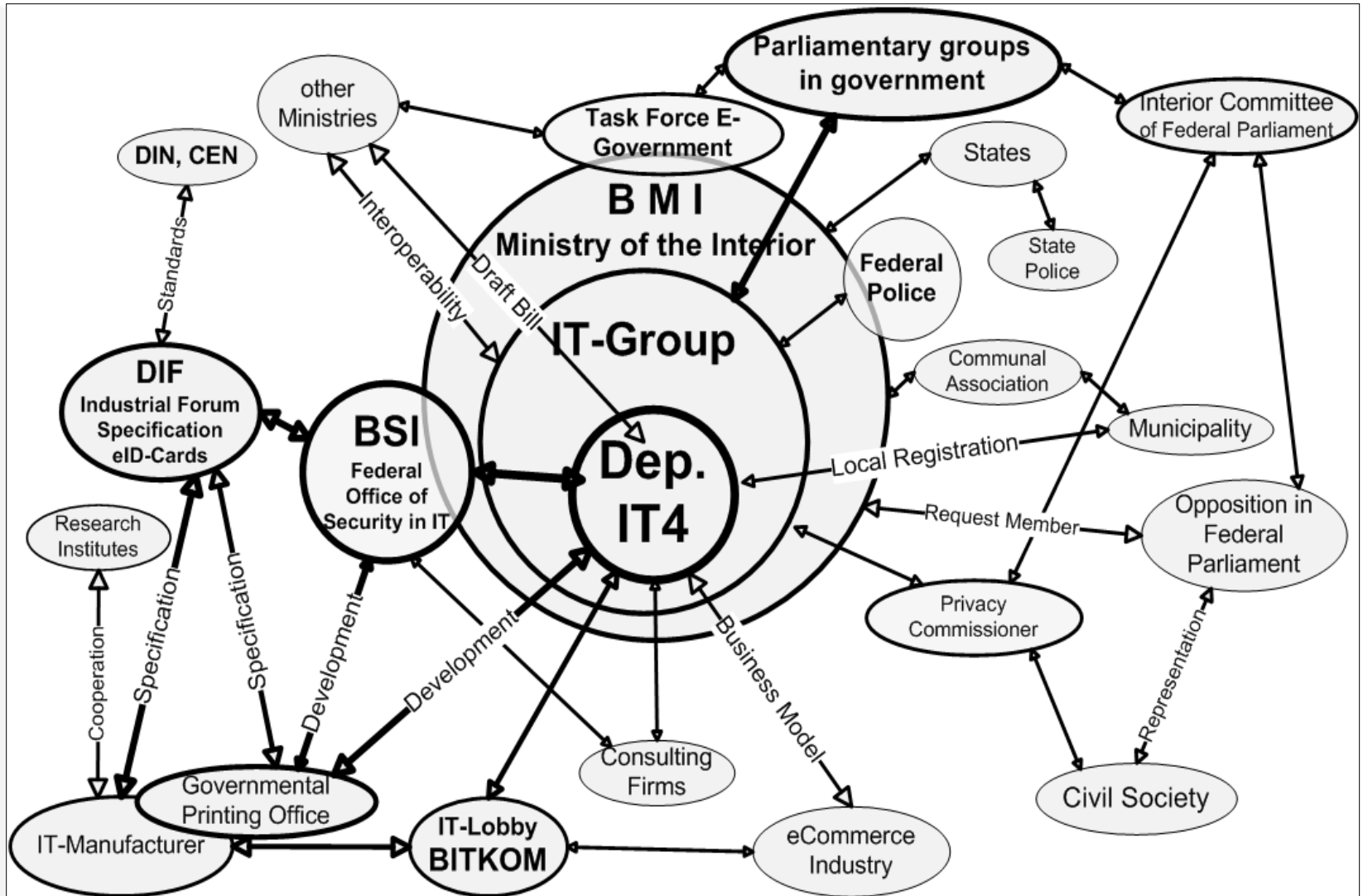
Description online authentication process – citizen view

1. Citizen connects to service provider via browser/internet
2. Citizen connects the ePA to the contactless reader (connected to user terminal)
3. Service provider sends access certificate with access rights for data fields
4. Citizen selects and confirms the access to each data fields
5. Citizen enters the ePA-PIN (six digit number)
6. Service provider gets the access to data fields

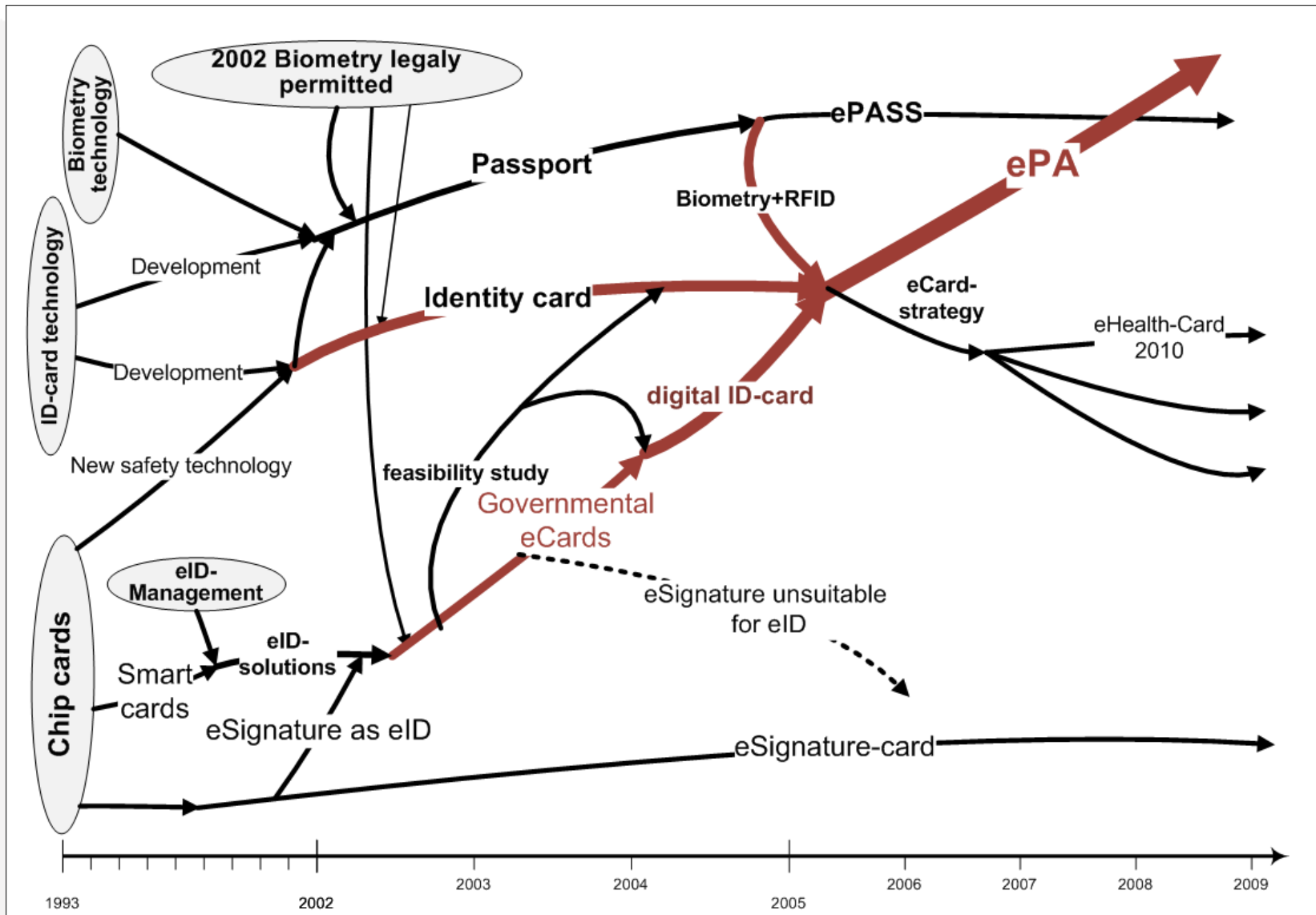
eID-Card/ePA timeline with main factors



Actor constellation



Technological paths of eID-card



Decision-making process biometry

- Anti-terrorism law 2002 legally permitted biometry in passport and identity card
- First realization biometry with ePASS (2005) by EU-regulations and ICAO-standards
- Transfer by eID-Card because of travel document
- Stepped restriction by political actors because of privacy concerns
 - Fingerprint only in the ePA-chip (2007: no central storage)
 - Fingerprint only optional (2008)

Some Conclusions

The following factors are responsible for a fast and mostly conflict-free implementation of the new functions of ePA:

- Core team of experts on administrative/governmental level
- Central competence in governmental institutions (BMI → IT-Group + Dep. IT4, BSI) completed with industrial competence
- Previous technology of ePASS (same Dep. IT4 + BSI) prepared solutions on ePA (RFID, biometry, eID)

Privacy enhancement by eID-technology:

Mutual authentication between citizen (ePA-chip) and service provider (eID-terminal) reduces safety risks like phishing