Advanced Security for Systems Engineering WS12

Security in der Praxis -
Machine Readable Travel Documents

Stefan Brandl

Agenda

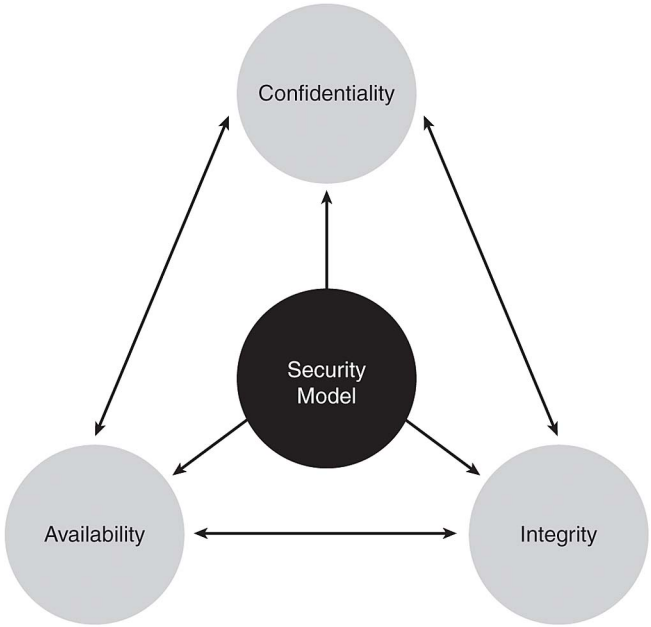
- Security
- Machine Readable Travel Documents - Ecosystem
- ePass - Technology
- Security features
- Interchange & Future
- Challenges & Myths

Security

- security - what is it?
  - consists of multiple definitions
  - information security, it-security, data security/privacy, physical security, etc...
- security architecture
  - structure and planning of the concept and design
  - incorporate different security domains
  - key facts
    - requirements
    - framework
    - changes & continuous improvement

Security

- core principles
  - confidentiality
  - integrity
  - availability
- enhancements
  - authenticity
  - non-repudiation
- all in one vs. discrete and individual
  - trade-offs **will** occur
  - business requirements



Security

- plenty of possibilities
  - need to know
  - least privilege
  - least functionality
  - separation of duties
  - rights and permissions
    - dac - mac - ndac (rbac, orcon, drm, et al)
  - k.i.s.s.
  - psychology

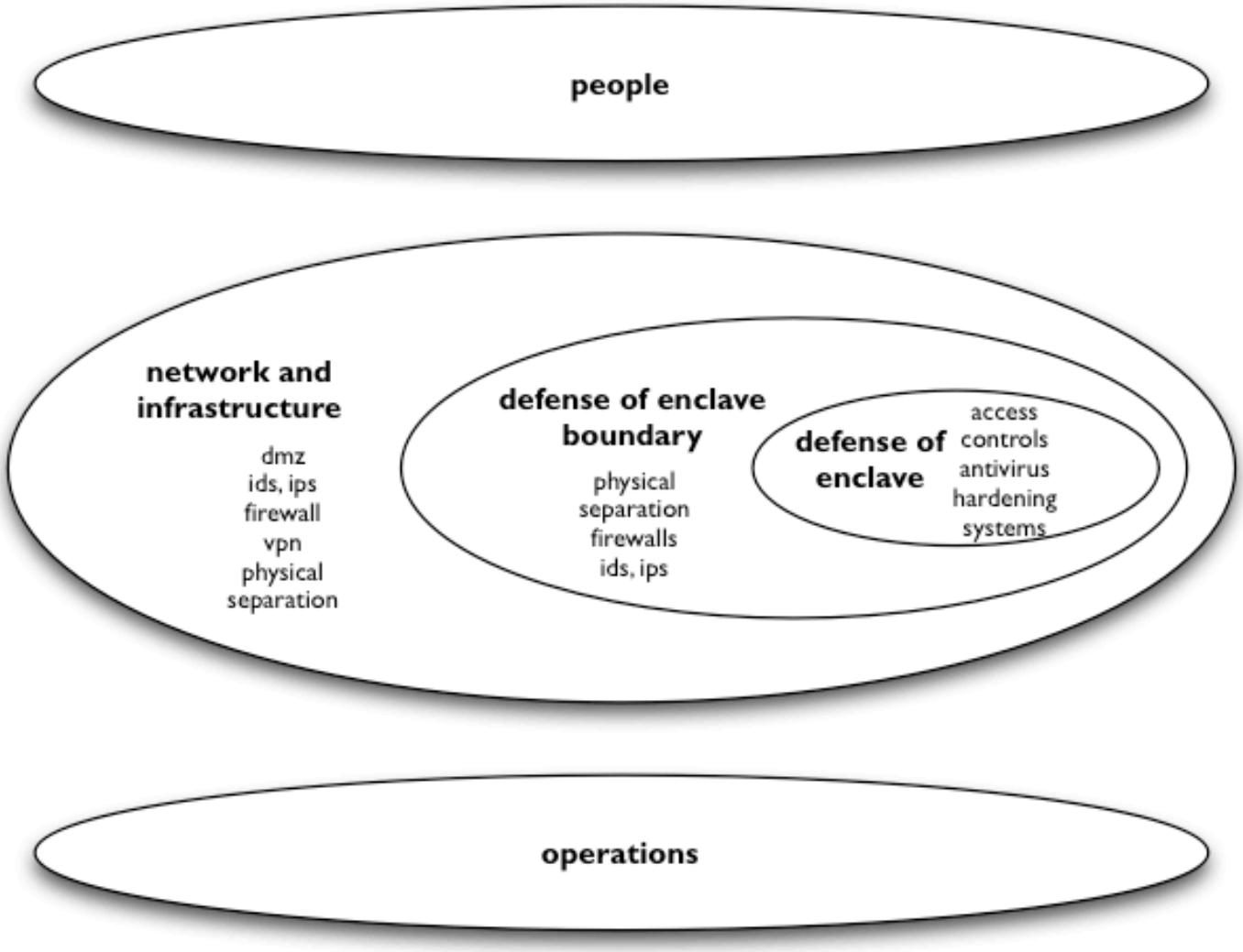
Security

- considerations
  - holistic security analysis
  - search for weakest link
  - end to end perspective
  - maintenance
  - software vs. hardware
  - usability & transparency
  - different views
    - operations
    - systems
    - technical

Security

- considerations
  - attacks
    - vectors
    - surface
    - motivation
- layered security
  - combination of different and independent elements, modules, domains
  - meshing and covering of controls
  - mixture of software, hardware, people
  - risk acceptance

Security


people
network and infrastructure
dmz
ids, ips
firewall
vpn
physical separation
defense of enclave boundary
physical separation
firewalls
ids, ips
defense of enclave
access controls
antivirus
hardening systems
operations

Machine Readable Travel Documents

- ecosystem
  - subject - document holder
  - object - id
  - token - document
  - front-end
    - inspection systems
    - border controls
  - backend
    - public key infrastructure(s)
    - databases
    - international interoperability

Machine Readable Travel Documents

- id
  - name
  - biometric data
    - face
    - fingerprint(s)
- goal
  - verifying identity of document holder
  - providing authenticity of document

ePass - Technology

- austrian passport since june 2006 with Chip
  - since march 2009 issuance of 2nd generation

- profile:
  - smart card chip (ICC) / NXP 80KB
  - smart card operating system (STARCOS)
  - passport application ICAO specification (Doc 9303)
  - contact less communication via RFID

ePass - Technology

- radio frequency identification (RFID)
  - original purpose: automatic identification and location by tags/ transponder
  - active / passive tags
  - development since WWII
  - transmission of information cleartext
  - machine readable travel documents (MRTDs)
    - ISO 14443
    - range of active communication
      - nominal / within lab environment: 0 – 1m
      - passport chip: ~10cm

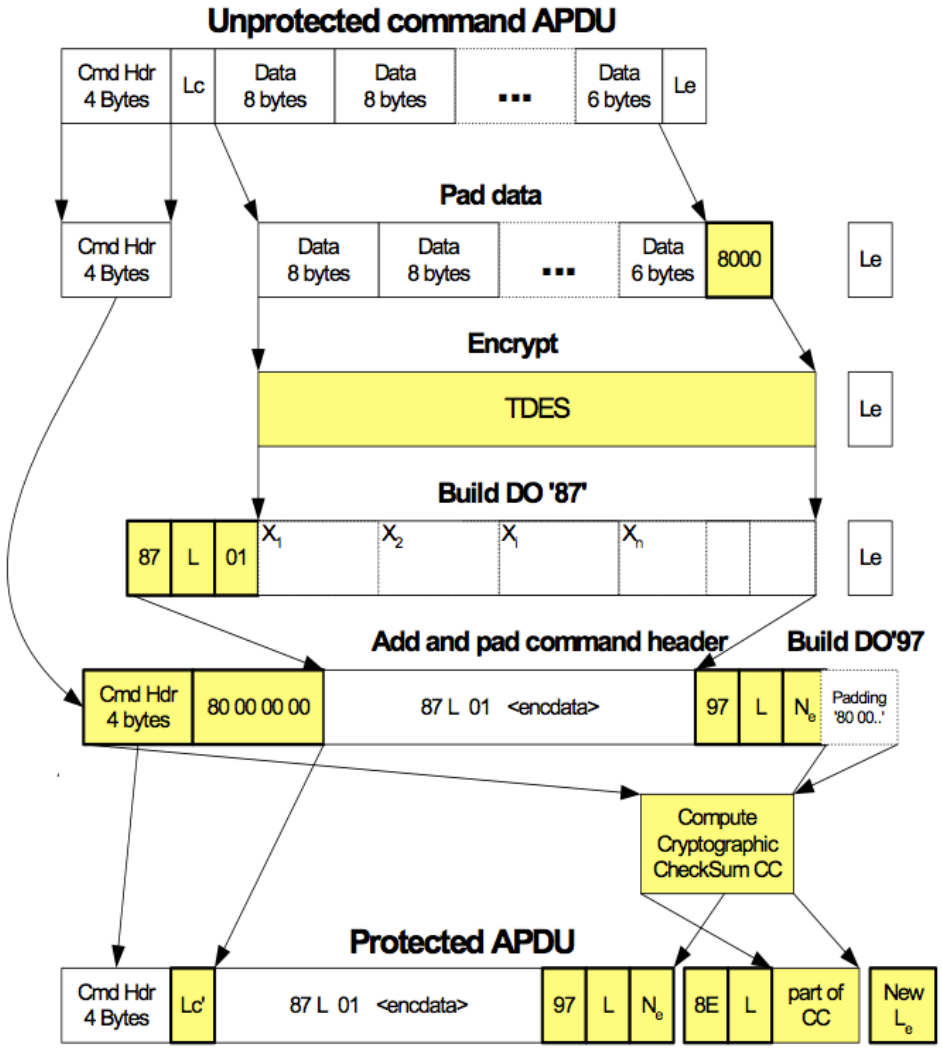
Security features - Chip | ICC

- hardware
  - chip-design per se
  - internal bus system
    - no contact/listening/modification from external
    - scrambling of bus informationen
  - shielding against electrical, optical and thermal interference
    - active sensors
  - self destruction on breach
  - internal checksum and signature calculations
  - common criteria eal 5+

Security features - Chip | OS

- smart card chip operating system
  - closely incorporated with hardware
  - functionality comparable to personal computer
    - kernel, memory management, security manager
    - master file, dedicated files, elementary files
  - common criteria eal 4+ (including special enhancements)
  - communication with OS by using ISO command set
    - „application protocol data unit“ (APDU) the only channel
    - ISO 7816-x
    - protected transmission by encryption (“encAPDU”)

Security features - Chip | encAPDU



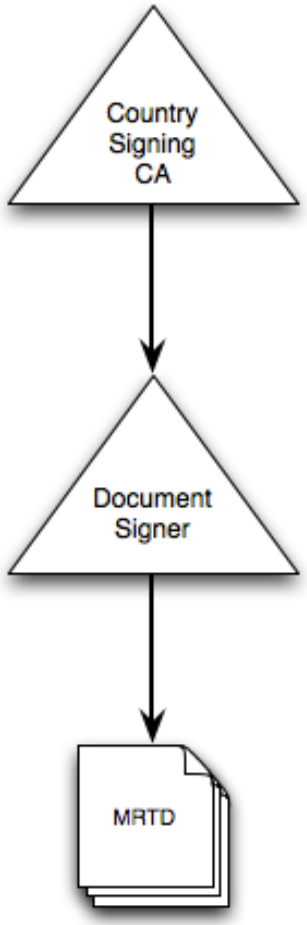
„Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements“ cwa14890-01-2004-Mar.pdf

Security features - Software | BAC

- basic access control (BAC)
  - authentication between MRTD and reader (inspection system)
  - challenge response
  - initiating and establishing secure messaging
  - key derivation based on machine readable zone (MRZ)
    - document number
    - birth date
    - validity date
  - secure messaging algorithmus: 3DES | 112bit (!)

Security features - Software | PA

- passive authentication (PA)
  - protection of integrity
  - digital signature of complete content
  - prerequisite: national public key infrastructure
    - Country Signing Certificate Authority (3072/4096Bit)
    - Document Signer (2048/3072Bit)
  - mandatory
  - saved in Document Security Object (EF.SOD)
- problem: chip substitution



„Specifications for Electronically Enabled Passports with Biometric Identification Capability“ ICAO DOC 9303 Part 1 Volume 2

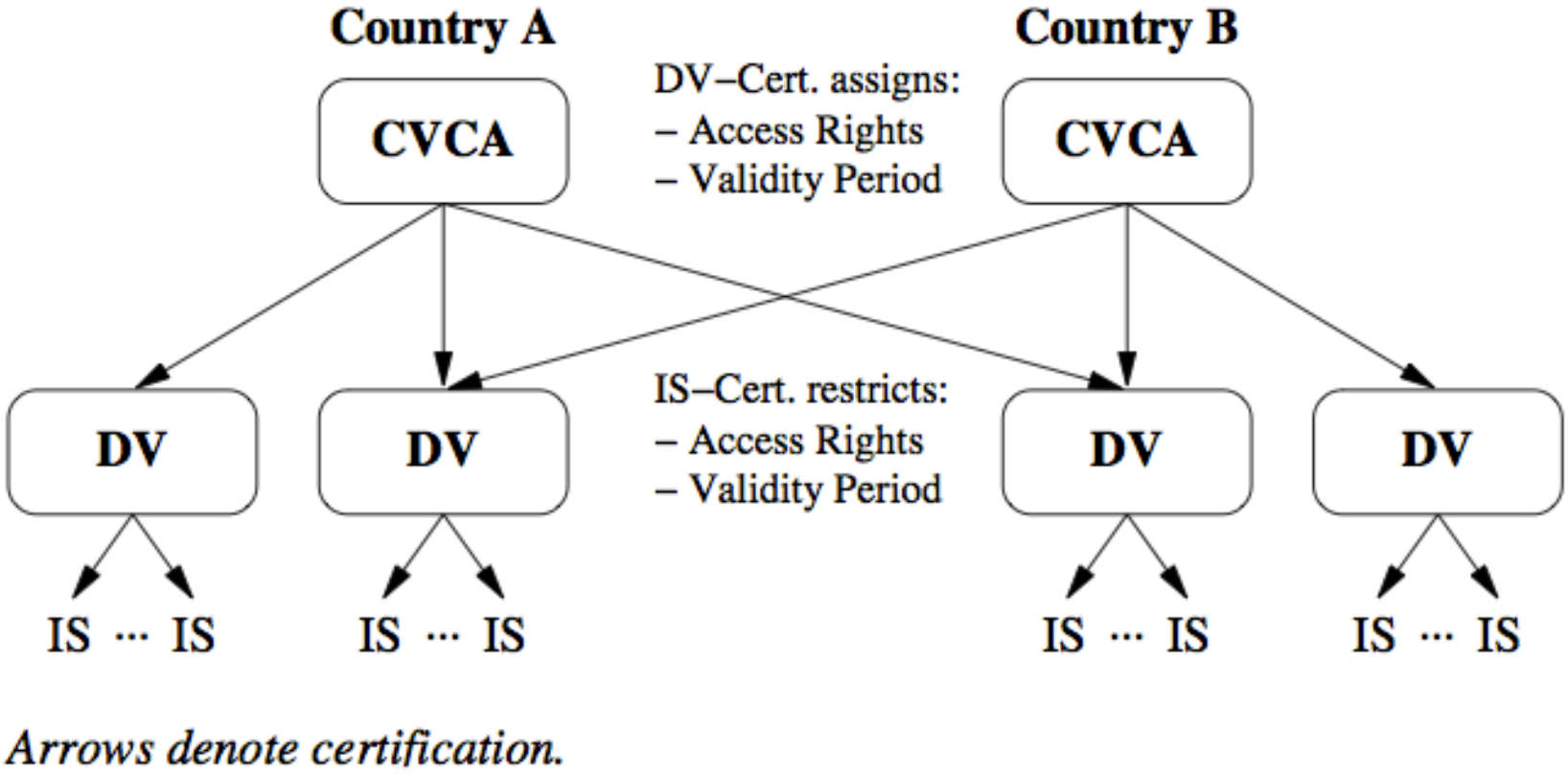
Security features - Software | AA

- active authentication (AA)
  - protection against chip-substitution
  - challenge response
  - additional asymmetrical keypair on chip
    - private key only known to chip
    - public key accesible (DG15)
  - rsa 1024 bit
  - only "1st Generation" of austrian passports (pre-fingerprint/eac)

Security features - Software | EAC

- extended access control (EAC)
  - protection of sensitive biometric data (fingerprint, iris, et al)
  - fine grained control of access
  - two protocols
    - chip authentication
    - terminal authentication
  - prerequisite: public key infrastructure
    - independent of CSCA
    - multiple tiers
      - country verifying certificate authority (CVCA)
      - document verifier (DV)
      - inspection system (IS)

Security features - Software | EAC



„Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)“
Technical Guideline TR-03110

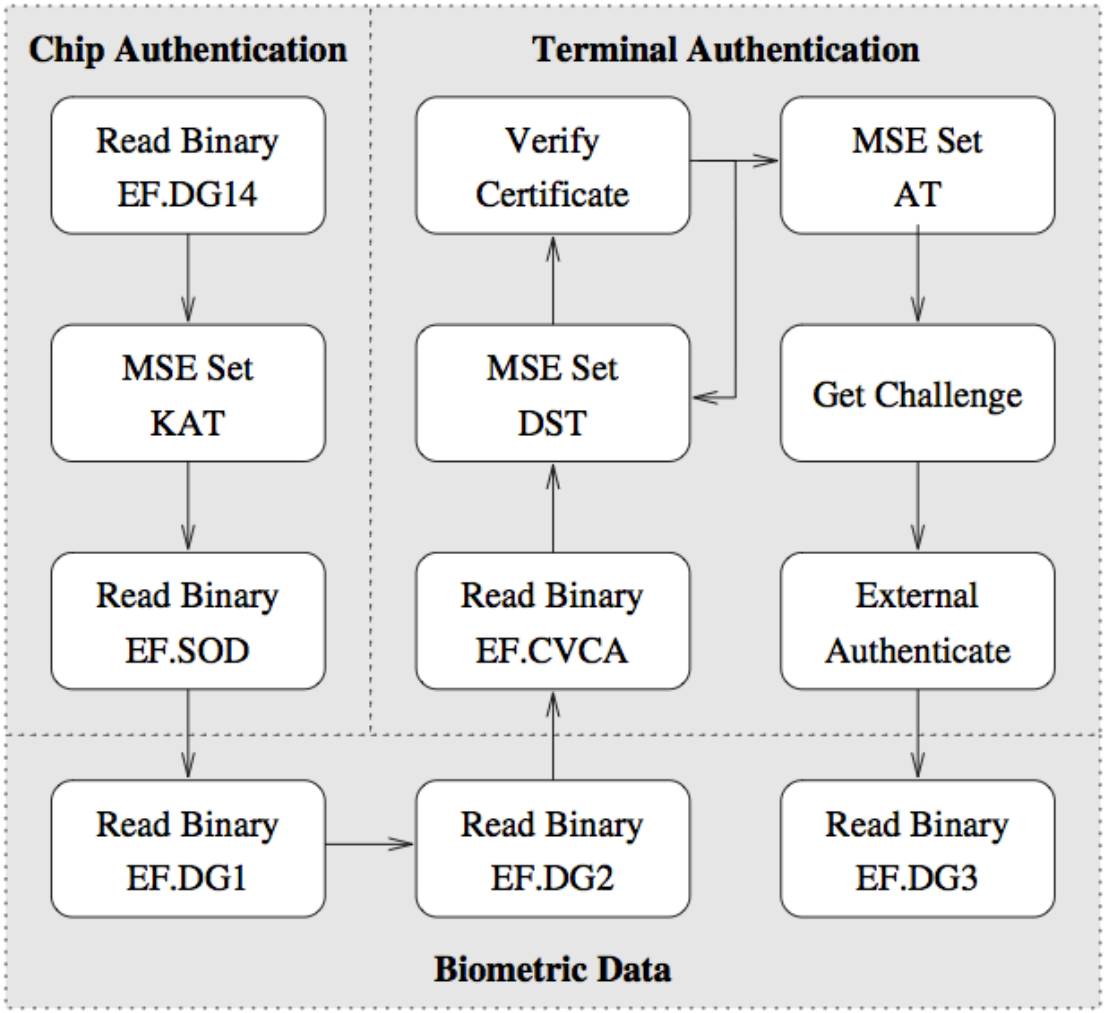
Security features - Software | CA

- EAC – chip authentication (CA)
  - establishing a strong cryptographic channel between chip and reader
  - detection of chip substitution
  - elliptic curve diffie-hellman
  - 224/256bit keysize for dh-handshake
  - 3DES | 168 bit session key

Security features - Software | TA

- EAC – terminal authentication (TA)
  - authentication providing access for sensitive data
  - inspection system must provide its authenticity
    - reading device using a terminal certificate
    - reading device must provide whole certificate chain twoards passport chip
    - MRTD-chip validates certificate chain
  - challenge-response identification of reading device
  - control matrix of which data can be accessed (rbac)

Security features - Software | Workflow



„Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)“
Technical Guideline TR-03110

Interchange & Future

- certificate interchange
  - international
    - ICAO public key directory (PKD)
  - between european states
    - establishment of single point of contact (SPOC)
    - web service for communication between SPOCs
- future security features
  - password based authentication encryption (PACE)
  - supplemental access control (SAC)
    - terminal authentication as first step
    - only authorized readers can communicate with chip

Challenges & Myths

- challenges
  - precise implementation necessary
    - *"The future of digital systems is complexity, and complexity is the worst enemy of security."*
  - „stick to the standards" – no room for individuality or errors (see examples)

- examples
  - JPEG2000 buffer overflow
    - http://www.wired.com/politics/security/news/2007/08/epassport
  - „elvis passport"
    - http://www.youtube.com/watch?v=0u4pg_XwNk8

Challenges & Myths

Challenges & Myths

- random serial number tracking
  - „A Traceability Attack Against e-Passports“
    - http://www.cs.bham.ac.uk/~tpc/Papers/PassportTrace.pdf

- measurement of radiation of RFID systems (MARS)
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/Mars_Teilbericht_ITherorie_pdf.pdf?__blob=publicationFile

Kontakt

DI (FH) Stefan Brandl, CISSP-ISSAP
Head of e-government IT & security
Austrian State Printing House

brandl@staatsdruckerei.at
https://www.xing.com/profile/Stefan_Brandl4

esse

Thank you!

http://security.inso.tuwien.ac.at/advsecsyseng-ws2012/