Electronic Signatures

Introduction and Applications

Dr. Vesna Hassler

Secure Information Technology Center-Austria (A-SIT)

www.a-sit.at

What is A-SIT?

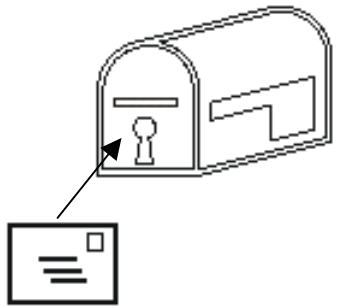
- Secure Information Technology Center
  - Founded in 1999
    - Ministry of Finance, Austrian National Bank, Graz University of Technology
    - non-profit, independent, neutral
  - Confirmation body for electronic signatures
    - Security consulting for public administration and governmental institutions
    - Payment systems assessment and surveillance
    - Security awareness
    - Technology monitoring
    - Membership in international standardization bodies

Overview

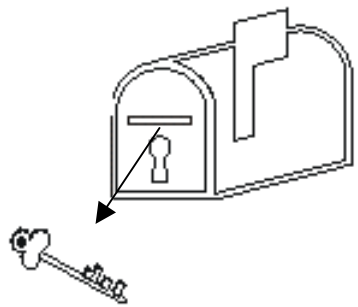
- Public-key cryptography and electronic signatures
- Public-Key Infrastructure (PKI)
- EU directive on electronic signatures
  - Austrian Electronic Signature Law
  - European Electronic Signature Standardization Initiative (EESSI)
- Applications
    - „Bürgerkarte“ (Austrian Citizen Card)

Public-key cryptography

- Public key



- Private key

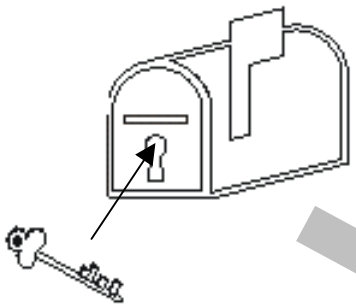


Signature example

In this example the mailbox must be sender specific so that the receiver can be sure that it can come from a specific sender only. In electronic case the public key is sender specific.

Sender: Creation

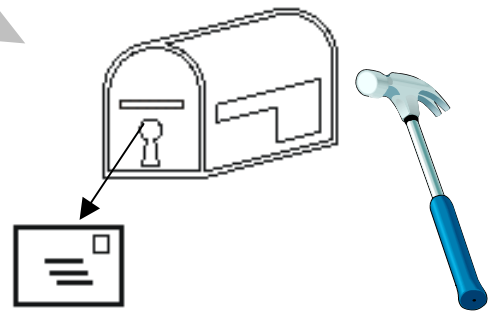
Locks a porcelain mailbox



Private key

Receiver: Verification

Smashes the mailbox



Public key

With electronic signatures signature verification can be repeated as many times as needed.

Electronic signature creation

Document to be signed

„Fingerprint“ or hash value

Hash value encrypted with the private key („signed“)

Document to be signed
Signed hash value
Public key certificate

Time stamp (if available)

Unchangeable document format (no macros!)

Cryptographic hash function, e.g., SHA-1

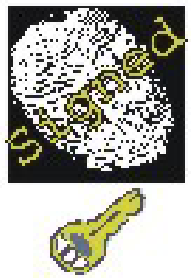
Public-key algorithm, e.g., RSA, elliptic curves

Public key certificate

- Public key must be signatory specific
  - so that the verifier (receiver) can be sure that the signature has not been forged
- Trusted third party = Certification Authority (CA)
  - issues public key certificates that guarantee that a public key belongs to a specific person

Electronic signature verification

Document to be signed
Signed hash value
Public key certificate



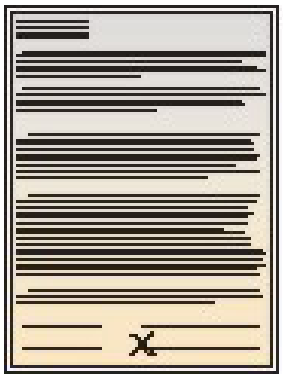
Verify the signature
(i.e., the hash value
encrypted with
the signatory's private key)

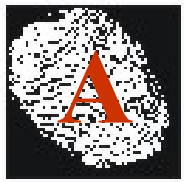
Verify the certificate
(e.g., whether it is valid
and issued by a CA you trust)

Thu Mar 12,
2002 20:00:01
Signed

Verify the time stamp
(it time stamping service
is available)

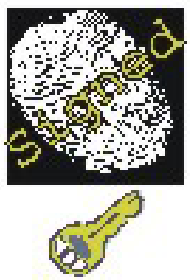
Verifying signed hash

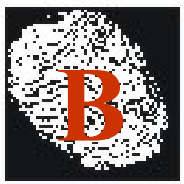




Document to be signed

„Fingerprint" or hash value



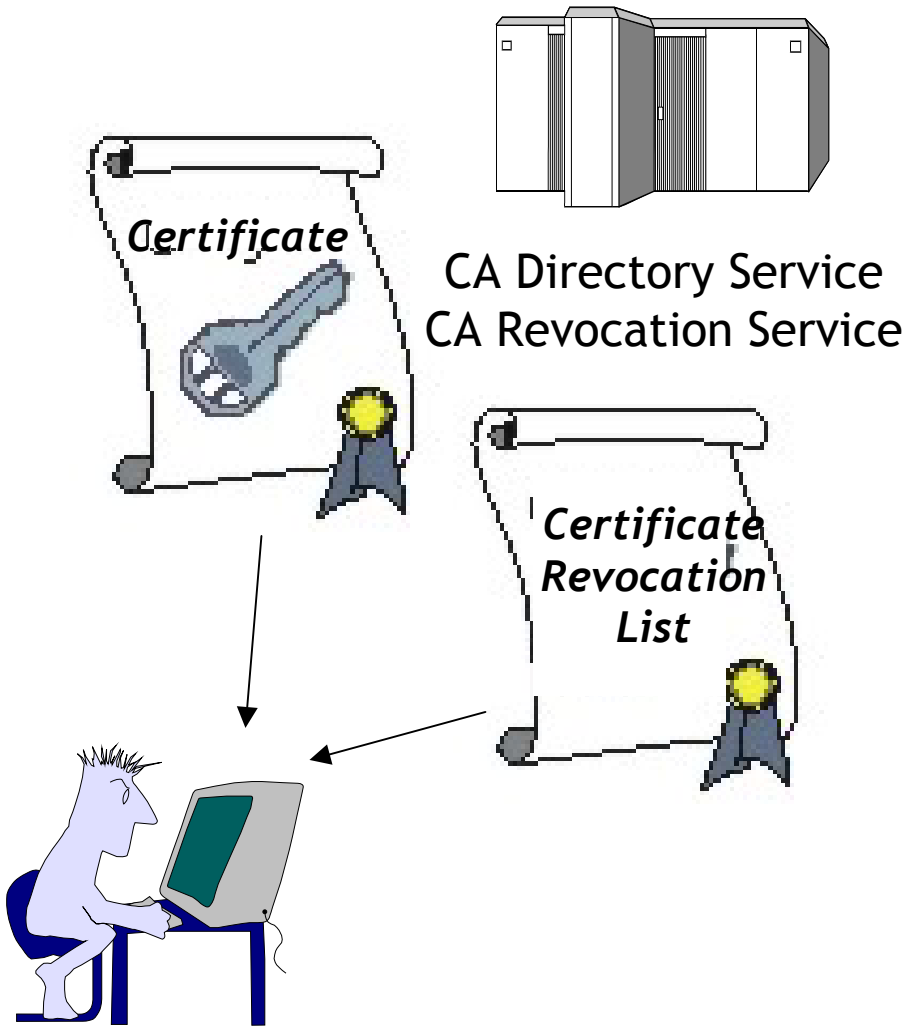


Hash value encrypted wi the private k („signed")

If A=B, the signature is mathematically correct.

This means that the public key from the certificate corresponds to the private key used to compute the signature.

Verifying the certificate



Do I trust this CA?

Do I have the CA's public key? Did I check the fingerprint published in, e.g., an official publication?

Can I verify the signature of the certificate by using the CA's public key?

Is the signatory's certificate valid?

Is the name of the certificate owner the signatory I expect?

Can this public key be used for signing documents?

What is a public key certificate?

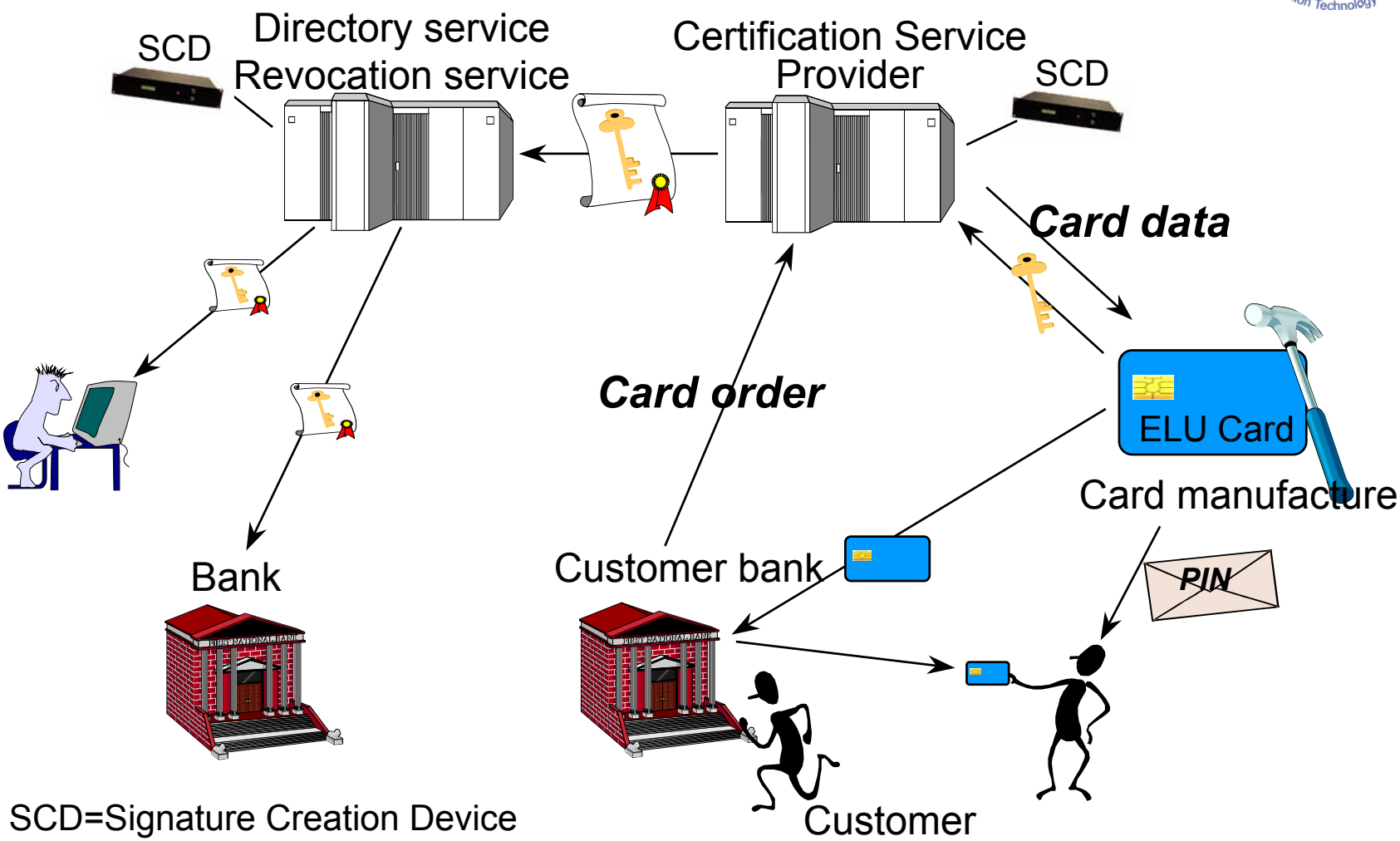
- Certificate is an electronic document in X.509 format signed by the CA

```
Certificate                         ::=     SIGNED { SEQUENCE {
   version                        [0] Version DEFAULT v1,
   serialNumber                       CertificateSerialNumber,
   signature                          AlgorithmIdentifier,
   issuer                             Name,
   validity                           Validity,
   subject                            Name,
   subjectPublicKeyInfo               SubjectPublicKeyInfo,
   issuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier
                                                 OPTIONAL,
   subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier
                                                 OPTIONAL
   extensions                     [3] Extensions OPTIONAL } }
```

Certificate Revocation List (CRL)

- CRL is an electronic document in X.509 format signed by the CA
- CRLs are published at regular intervals or on demand
- A certificate can be revoked or suspended for many reasons
  - keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, etc.

Example PKI


SCD
Directory service
Revocation service
Certification Service
Provider
SCD
Card data
Card order
ELU Card
Card manufacture
Bank
Customer bank
PIN
Customer
SCD=Signature Creation Device

EU Directive 1999/93/EC on Electronic Signatures

- Community framework for electronic signatures
- Article 9 Committee to assist the EC
  - Notified body in each country (e.g., A-SIT, BSI)
- Advanced electronic signature
  - uniquely linked to the signatory
  - capable of identifying the signatory
  - created using means that the signatory can maintain under his sole control
  - linked to the data to which it relates in such a manner that any subsequent change is detectable

EU Directive introduces...

- Qualified certificate
  - must fulfill the requirements from Annex I
  - Certification Service Providers (CSP, i.e., CA) issuing qualified certificates
    - must fulfill the requirements from Annex II
  - other electronic signature types should not be automatically denied legal recognition!

EESSI

- European Electronic Signature Standardisation Initiative
  - An industry initiative in support of the European Directive on Electronic Signatures
- Standardization: CEN and ETSI
  - CEN/ISSS WS/E-Sign: Signature creation and verification, Certification Service Providers (CSP)

    http://www.cenorm.be/isss/Workshop/e-sign/Default.htm
  - ETSI SEC ESI: X.509 and qualified certificates, CSP security policies, signature formats (e.g., XML), time stamp protocols

    http://portal.etsi.org/sec/el-sign.asp
- More information:

  http://www.ict.etsi.fr/eessi/EESSI-homepage.htm

Secure signature-creation devices (SSCD)

- Signature creation device (SCD) could be
  - a PC with SW
  - a Personal Digital Assistant with SW
  - a smart card with a signature application
  - a dedicated HW device with a signature application
- Secure SCD must fulfill Annex III
  - Article 9 Committee's decision (July 2002):
    - SSCD must be evaluated according to the Common Criteria and against the SSCD Protection Profile

Common Criteria (CC)

- Common Criteria for IT Security Evaluation
  - 1999: CC Version 2.1 = ISO/IEC 15408 Part 1-3
  - Info: www.commoncriteria.org
- CC evaluations and certifications are internationally recognized
  - based on the CC Mutual Recognition Arrangement
- A product independent security assurance and security functional requirements can be defined by a protection profile (PP)

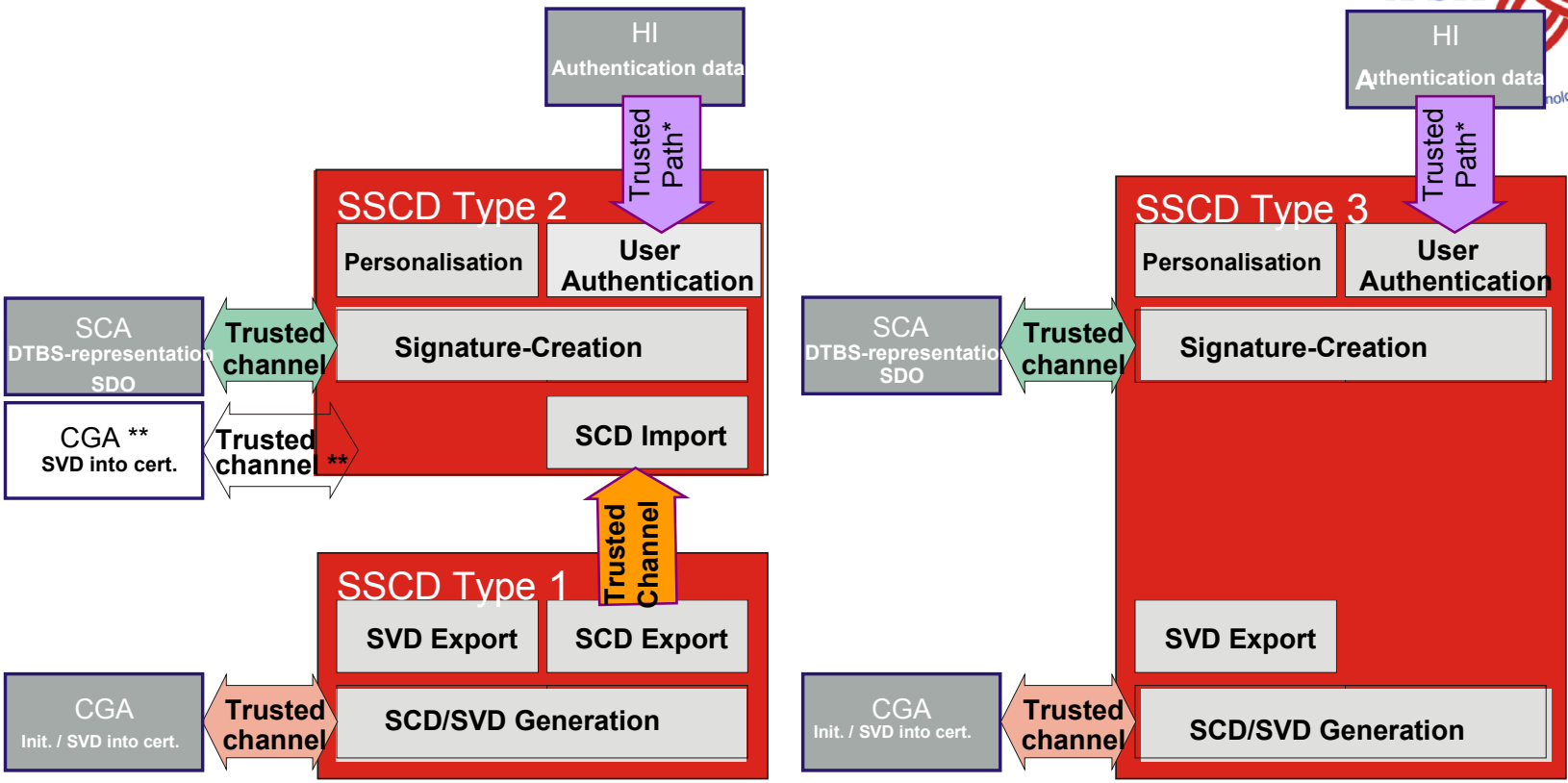
CC: Evaluation

- CC evaluates products, systems, and protection profiles
- Certificates
  - recognized certification bodies
  - licensed evaluation facilities
  - national certification schemes
- Evaluation levels:
  - Assurance: EAL1 bis EAL7 (max)
  - Strength of functions: basic, medium, high
  - Security target: product specific
  - Protection profile: technology neutral

CC and SSCD

- Secure Signature Creation Devices Protection Profile (SSCD-PP)
  - prepared by the CEN/ISSS Area F for the EESSI
  - requires EAL4+
  - evaluated by an evaluation lab
- Three SSCD types:
  - Type 1: Key generation
  - Type 2: SSCD without key generation
  - Type 3: SSCD with key generation

SSCD-PP



HI: Human Interface
SCA: Signature Creation Application
CGA: Certificate Generation Application
SCD: Signature Creation Data
SVD: Signature Verification Data

Austrian Electronic Signature Law

- Law in 1999, Ordinance in 2000
  - the first implementation of the EU Directive on Electronic Signatures
  - Germany had the first Signature Law (but not EU Directive compliant)
- New: Secure Electronic Signatures
  - Advanced Electronic Signatures with SSCD
  - in Germany: Qualified Electronic Signatures

Secure electronic signatures

- Confirmation body license required for
  - SSCD
  - devices and mechanisms for secure entering of authorization information (PIN)
  - devices and mechanisms for secure viewing of documents to be signed („What you see is what you sign" – WYSIWYS)
  - devices and mechanisms for cryptographic hash computation (if not implemented on SSCD)

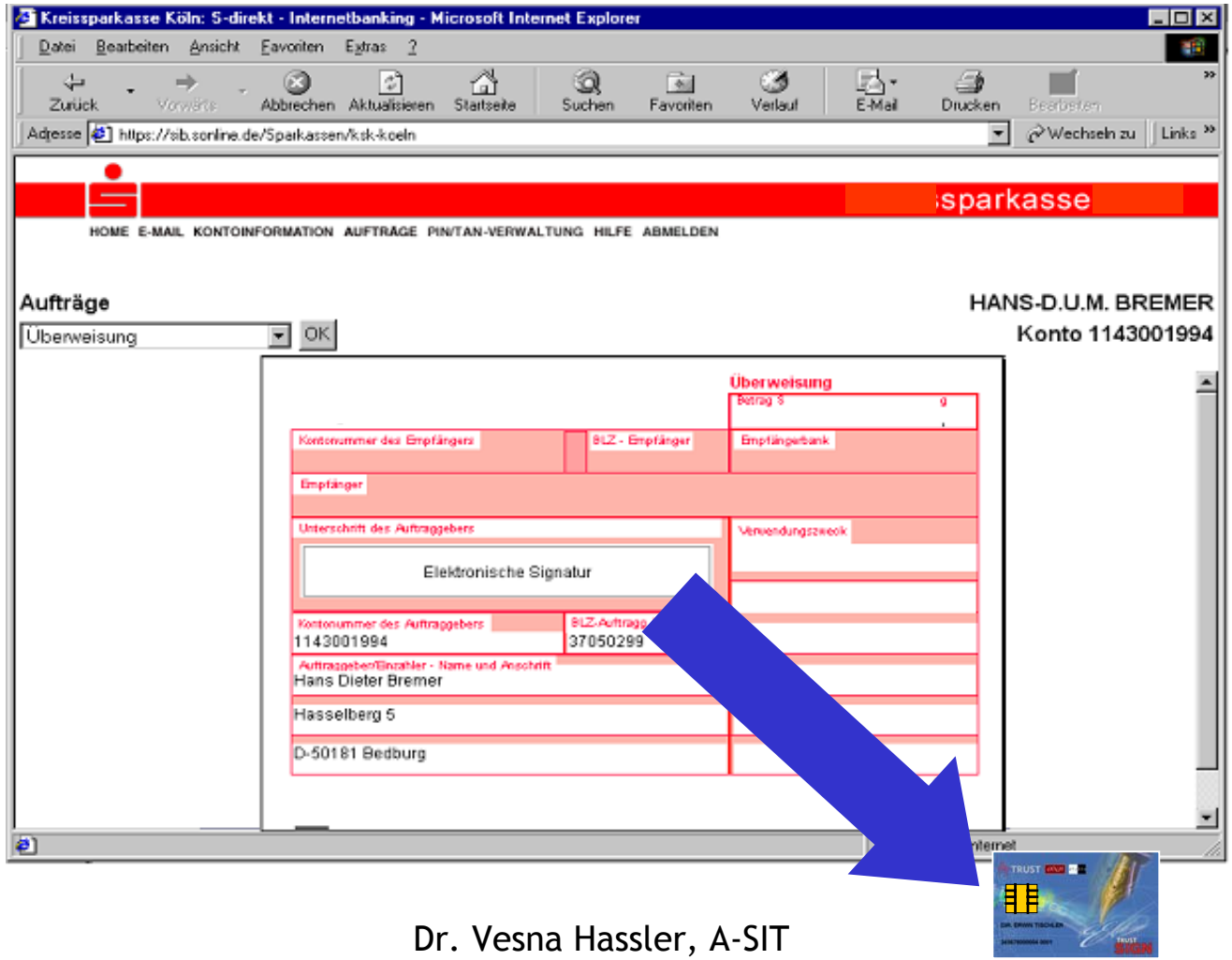
Current situation in Austria

- Supervisory authority:
  - *Telekom-Kontrol Kommission* supported by the *Rundfunk- und Telekom Regulierungsbehörde*
- Accredited CSPs for qualified certificates:
  - A-Trust and A-Sign
- Licensed SSCDs:
  - Philips SCC P8WE5032V0G with STARCOS SPK2.3 , Infineon IC SLE663X320P with CardOS M/4.01, T-Systems E4 KeyCard v3.0
- Licensed smart card readers:
  - Sign@tor Terminal v1.0, Kobil KAAN Professional
- Licensed secure viewers:
  - BDC hot:Sign, BDC MBS-Sign

Applications of electronic signatures

- e-mail, e-banking, e-commerce, e-business, e-government
- No killer application yet
- Problems:
  - no internationally recognized PKI
  - different legal approaches (EU, USA, Japan...)
  - no trust in the PC environment
  - complex technology, difficult to learn
  - no serious investments by banks and industry

Example: Payment receipt



Dr. Vesna Hassler, A-SIT

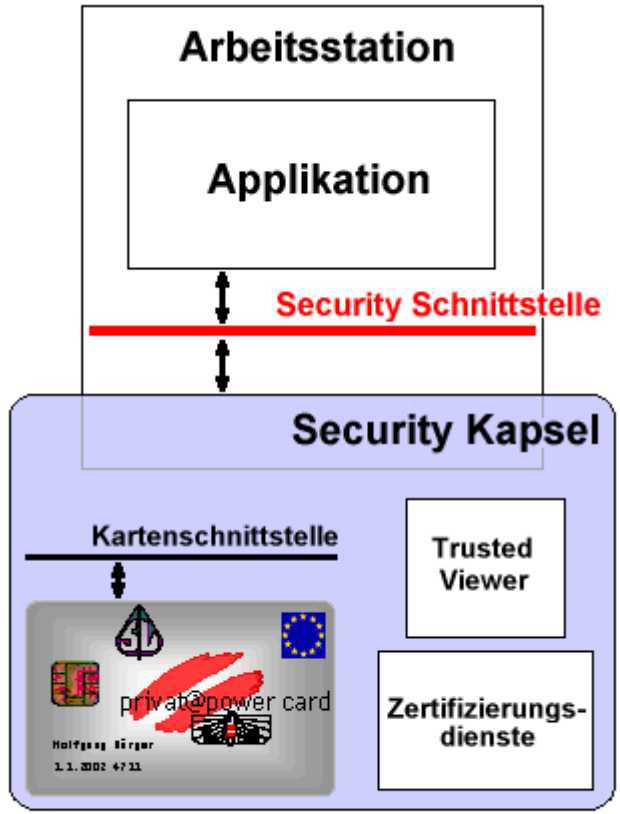
Austrian Citizen Card („*Bürgerkarte*")

- Idea:
  - equip the new social insurance card with electronic signature functionality
  - no sensitive data on the card is unprotected
  - for signature function, a PIN is required
  - signatures with elliptic curves and XML
    - XMLDSIG is a W3C recommendation
  - for e-goverment, but e-commerce should follow
  - should be available in 2004

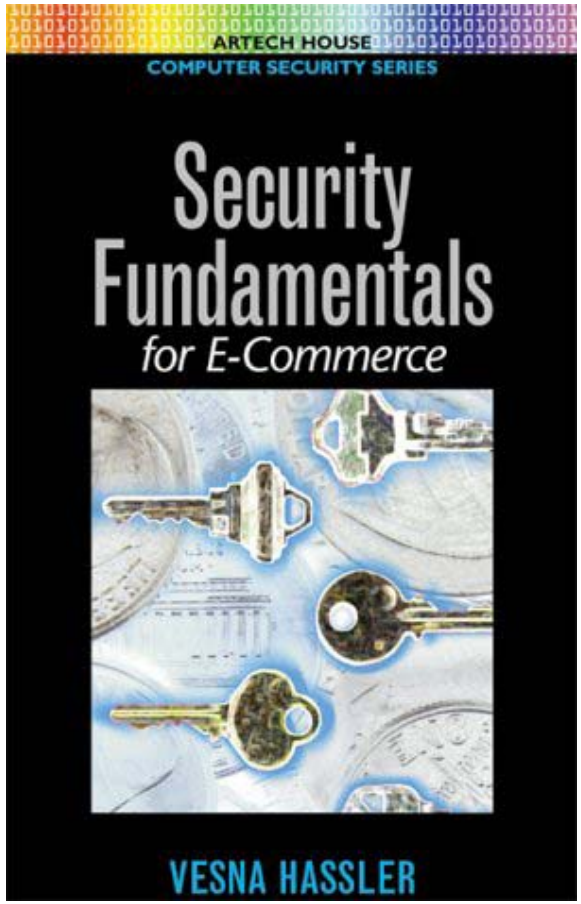
Security Layer

- Compatibility of the Citizen Card with other technologies should be achieved through a *Security Layer*
  - More info:

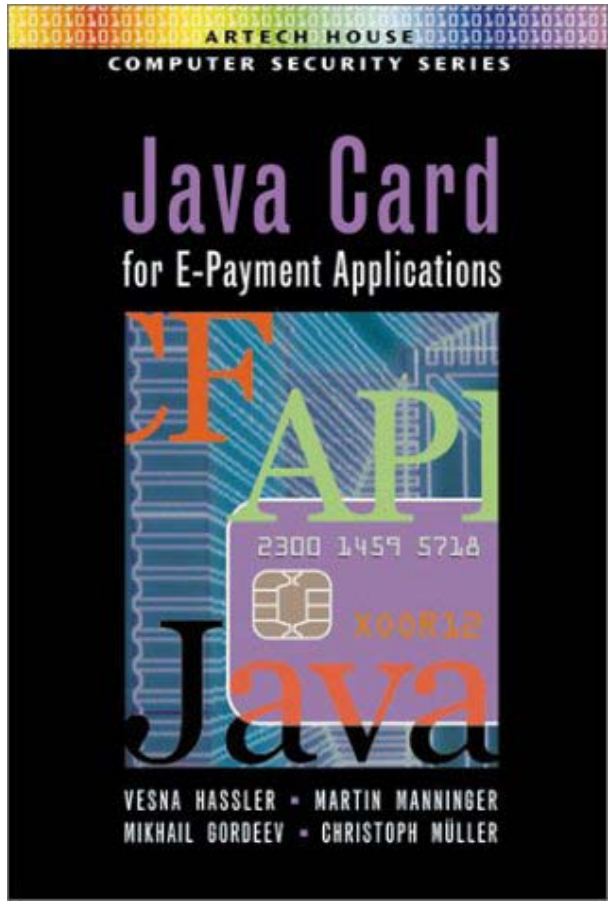
www.buergerkarte.at/SLAYER/SecurityLayer.html



My books
(www.artech-house.com)



Hardcover/Digital (pdf)



Hardcover