

# Multifunctional Smart Card and PKI at the University of Mannheim

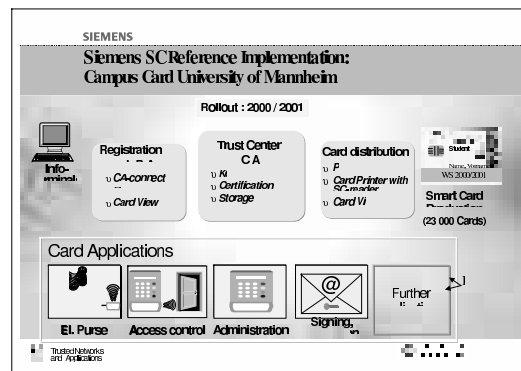
Alexander Hertz

Siemens AG, ICN ISA TNA 1

## 1 The team

The project was implemented by a team of 8 technology partners, led by Siemens AG.

## 2 The two phases of the project



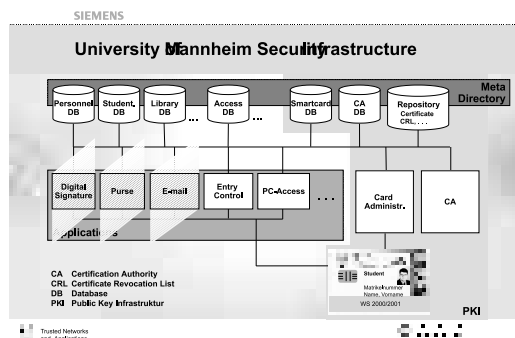
Phase 1, running at the moment, serves to prove suitability and functional efficiency, and basically includes the facilities for the production, storage and distribution of smart card-based ID cards, plus the generation of Public Keys and X.509 Certificates. The first solutions, which have been used since October 2000, are:

- student ID cards
- contactless access control to buildings and rooms
- printing semester tickets.

The cards are designed in such a way as to enable the secure expansion of the chip's file structure to meet Public Key requirements at a later stage. Implementation of all the functions of the new student ID card is set to be completed in the spring of 2001. Phase 2 encompasses the implementation of PKI and the expansion of the infrastructure by incorporating certain selected solutions: **The contactless component of the smart card is**

used as an electronic purse at the POS systems in the cafeteria and the self-service facilities. **The contact-based part of the smart card** will be used for applications such as the library pass, student administration, pre-enrollment, payment of semester fees, obtaining semester tickets, printing of Certificates, registration for examinations, courses and other events, seeking details of grades, changes of address, digital signature and the encryption of e-mails.

### 3 Security Infrastructure with PKI



The use of smart cards calls for a security infrastructure (certification infrastructure). To accommodate the new desired applications, such as payment transactions, digital signature and encryption of transmitted data, an entire system for asymmetric key generation, administration and distribution has been created).

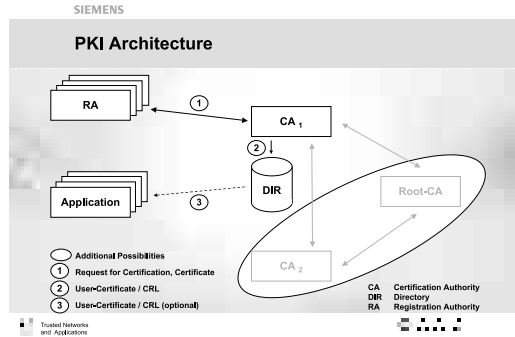
#### University of Mannheim security infrastructure

As illustrated, the security infrastructure can be divided into blocks:

- **The Public Key Infrastructure (PKI)** comprising
  - Card administration
  - Certification Authority (CA)
  - The associated databases
  - Repository/directory for Certificates and revocation lists
  - The smart card as the carrier medium for the Private Keys
- The smart card-based **applications**

### 4 PKI Architecture

Any participant is registered at the RA



The request for certification is transmitted to the CA where, on the smart card, the necessary keys are generated, the certificates are stored in the directory and the smart cards are delivered via the RA. On the other hand whenever keys are generated within the CA, the private key is transmitted encrypted to the smart card and decrypted in the card (secure messaging).

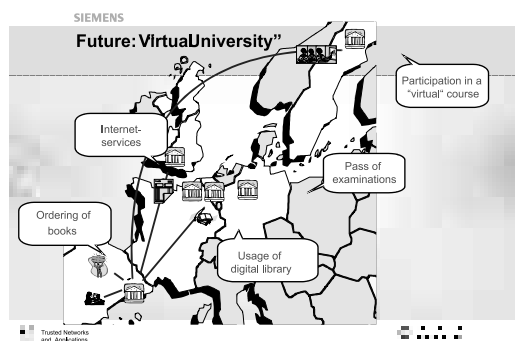
At any access to a secured application, the validity of the card is checked versus the relating certificate.

Optionally the certificates can be stored within an application.

The PKI Architecture is designed to co-operate with other Certification Authorities.

This might be a governmental 'Root CA', a CA of another University or any further CA supporting an X.509 cross-certification.

## 5 Virtual University



The University of Mannheim is a good example for what we call a 'Virtual University'.



More and more services become network based using multifunctional smart cards together with Public Key Infrastructure for secure access.

