USECA

USECA Demonstrator

USECA

USECA Demonstrator

Monika Horak
Giesecke & Devrient GmbH
Prinzregentenstraße 159
D-81607 München
Monika.Horak@gdm.de

- USECA (**U**MTS **Sec**urity **A**rchitecture)
- Demonstrator - Introduction
- USECA USIM
- Demonstrator Features
- Demonstrator Modules
- 3GPP - Demonstrator V1

USECA

AC336 USECA (1)

- Partners
  - Vodafone Ltd (project coordinator)
  - Siemens Atea
  - Giesecke & Devrient
  - Panasonic Mobile Communications Development Centre
  - Siemens AG
- Key activities
  - to review security requirements and define a comprehensive set of security features
  - to define a comprehensive set of security mechanisms, protocols and procedures
  - to define a functional and physical security architecture
  - to participate in the UMTS standardization activities and to contribute USECA results to the process

USECA

USECA (2)

- Supporting activities
  - to define the security features and procedures involving the USIM
  - to investigate terminal security
  - to validate critical concepts in demonstrators
  - to investigate legal issues
  - research oriented theme: to define a public key infrastructure
- Results
  - substantial support for standards bodies
  - USECA Demonstrator

USECA

USECA Demonstrator

- Validate the soundness and feasibility of the results of USECA
- Demonstrator
  - USIM
  - Chipcard Terminal
  - PC-SW simulates terminal, network, USIM, intruder
- Authentication and key establishment procedure
  - 3GPP
  - ASPeCT protocol
    - **A**dvanced **S**ecurity for **Pe**rsonal **C**ommunications **T**echnologies
    - research oriented
    - uses public key techniques
    - allows integration of micropayment system (‘tick payments’)
    - public key protocol implemented on the USECA USIM

USECA

USECA USIM

- Multi-application smart card: GSM + UMTS
- File system and card commands in accordance with 3GPP and ISO/IEC
- Authentication and key agreement:
  - 3GPP protocol
  - ASPeCT protocol
- Cryptographic functions:
  - Functions f1-f5, f1*
  - Symmetric encryption
  - Elliptic curve routines (ASPeCT protocol)

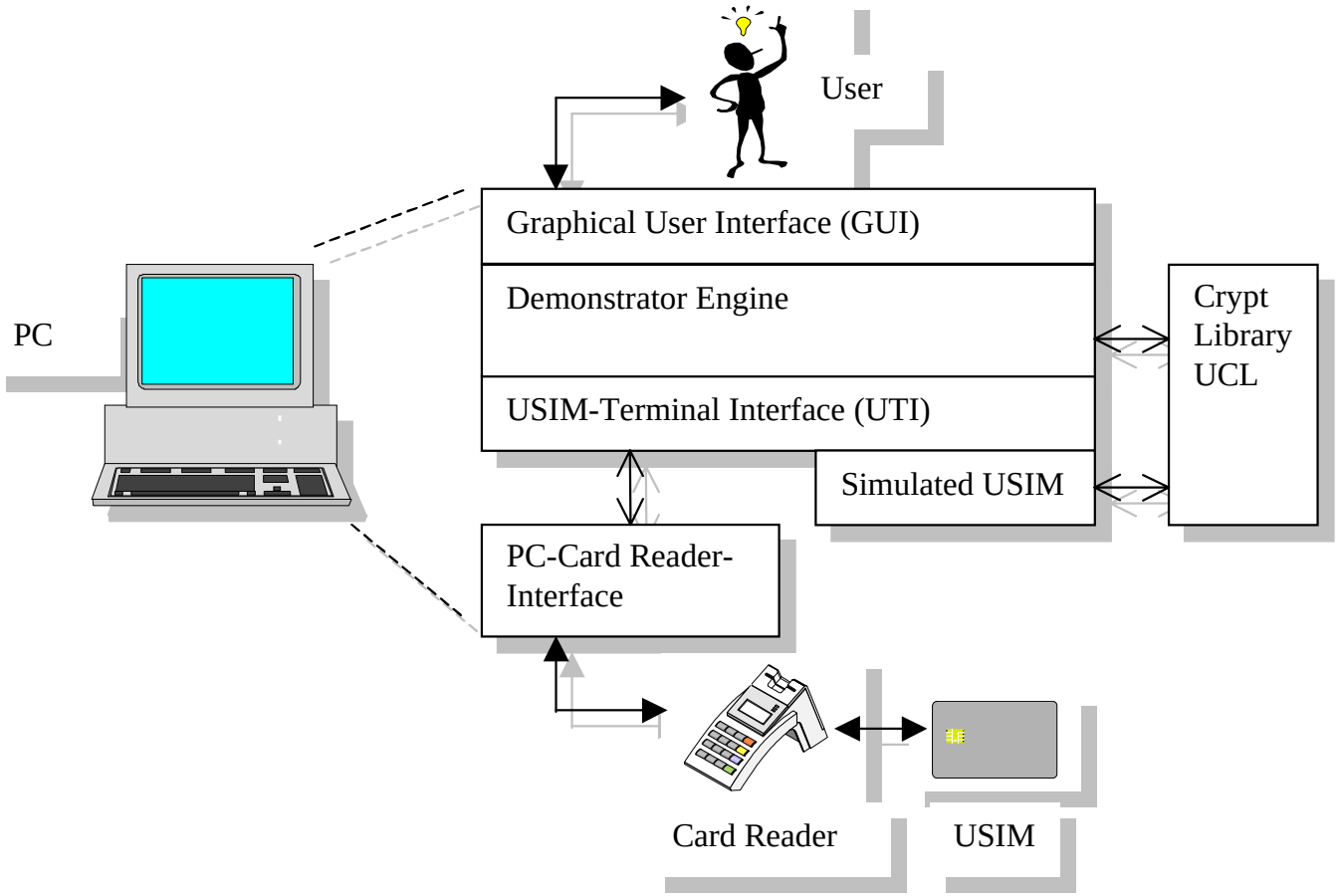
USECA

Demonstrator Features

- Visualisation of
  - the UMTS authentication and key establishment protocol
  - protocol flows, protocol messages and state variables of the system
  - the system behaviour in case of failures or fraud attempts
- Analysing
  - exact tracing of the implemented authentication protocols
  - simulation of fraud attempts
  - user intervention: manipulation of system state variables or protocol messages
- Evaluation
  - time measure functions
  - log functions

USECA

Demonstrator Modules



USECA

3GPP - USECA Demonstrator V1

- USIM File System
  - file name
  - additional files for analysing and visualisation purposes
- Commands
  - INTERNAL AUTHENTICATE
  - response: RES or RAND_US || AUTS
- Management of Sequence Numbers
  - USIM stores SQN_US, RAND_US, Δ

USECA

Demonstrations