



Fraunhofer Institut  
Sichere Informations-  
Technologie

# 18. SIT-SmartCard Workshop

|                   |  |
|-------------------|--|
| Datum:            | <b>5. und 6. Februar 2008</b>  |
| Organisator:      | <b>Dr. Markus Schumacher</b><br>Leiter „Smart Devices und Embedded Security“<br>Fraunhofer-Institut für Sichere Informationstechnologie SIT<br>Rheinstr. 75, D-64295 Darmstadt<br>Tel. +49-6151-869-204, Fax -127<br>e-mail: markus.schumacher@sit.fraunhofer.de |
| Programm-Komitee: | Michael Hegenbarth, Bundesdruckerei<br>Detlef Kraus, SRC<br>Dr. Gisela Meister, G+D<br>Dr. Gerd Pfeiffer, CardInsight<br>Dr. Markus Schumacher, Fraunhofer SIT<br>Bruno Struif, Fraunhofer SIT<br>Ulrich Waldmann, Fraunhofer SIT                                |

## Dienstag, 05.02.2008, Ort: Dolivostraße 15, Darmstadt

|                  |   |
|------------------|---|
| ab 08:30         | <b>Anmeldung</b>  |
| 10:00-10:05      | <b>Begrüßung</b><br>Prof. Dr. Claudia Eckert, Fraunhofer SIT  |
| 10:05-10:35      | <b>Keynote</b><br>Dr. Ulrich Sandl, Bundesministerium für Wirtschaft und Technologie  |
| <b>Session I</b> | <b>Kryptographie</b><br>Session Chair: Detlef Kraus, SRC  |
| 10:35-11:05      | <b>Schlüsselableitungen für symmetrische Algorithmen</b><br>Burkhard Fuchs, T-Systems,<br>Prof. Dr. Ernst-Günter Giessmann, Humboldt Universität Berlin |
| 11:05-11:30      | <b>Kommunikations- und Kaffeepause</b>  |
| 11:30-12:00      | <b>Algorithmenkataloge in Deutschland – ein Überblick</b><br>Dr. Georg Illies, BSI  |
| 12:00-12:30      | <b>Wechsel des Root-Schlüssels in der Praxis</b><br>Marcus Lippert, FlexSecure  |
| 12:30-13:30      | <b>Imbiss &amp; Kommunikationspause</b>   |

## **Session II**

### **Chiptechnologie und Betriebssysteme**

Session Chair: Dr. Gerd Pfeiffer, CardInsight

13:30-14:00

#### **Status und Trends der SmartCard-Chips**

Werner Sahle, Sagem Orga

14:00-14:30

#### **Sicherheit der Chipkarten-Plattform**

Dr. Peter Laackmann und Marcus Janke, Infineon

14:30-15:00

#### **Java Card 3.0- Putting the Web in a Smart Card**

Eric Vetillard, Trusted Labs und Java Card Forum

15:00-15:30

#### **Kommunikations- und Kaffeepause**

## **Vortrag der SIT-SmartCard-Preisträger 2008**

15:30-16:15

#### **Schlüssel zum Erfolg - was wir aus der Vergangenheit für die Zukunft der Kartentechnologie lernen können**

Wolfgang Effing, Klaus Finkenzeller, Wolfgang Rankl

16:15-17:00

#### **Pause (Ortswechsel zum SIT)**

## **Abendprogramm im SIT-TK-Labor (Rheinstr. 75)**

17:00 Uhr

#### **Verleihung des SIT-SmartCard-Preises an**

**Wolfgang Rankl / Wolfgang Effing sowie Klaus Finkenzeller**

Laudatio:

Bruno Struif, Fraunhofer SIT

Michael Hegenbarth, Bundesdruckerei

17:30 Uhr

#### **SmartBuffet mit Fassbier & Wein**

#### **Ausstellung "Ausweise gestern und heute - vom**

**handgeschriebenen Papiausweis zur SmartCard"**

19:00-19:20

#### **"Kalendarische Jahrhundertereignisse"**

Dr. Dirk Scheuermann, Fraunhofer SIT

ab 19:30

#### **Live Band „Western-Wood-Stompers“ & Gelegenheit für Geschäftskontakte**

**Mittwoch, 06.02.2008, Ort: Dolivostraße 15, Darmstadt**

## **Session III**

### **Nationale & internationale Standards und ihre Anwendung**

Session Chair: Dr. Gisela Meister, G+D

10:00-10:30

#### **Aktuelle Standardisierungsthemen bei ISO/IEC und CEN**

Maximilian Reinders, SRC

10:30-11:00

#### **Übersicht über die neuesten Aktivitäten bei ETSI**

Walter Mohrs, T-Mobile

11:30-12:00

#### **Aktuelle Standardisierungsthemen aus Anwendersicht**

Uwe Schnabel, ITG

12:00-13:00

#### **Imbiss & Kommunikationspause**

## **Session IV**

### ***Kontaktlose Chipkarten***

Session Chair: Michael Hegenbarth, Bundesdruckerei

13:00-13:30

#### **Anwendungsstrategien für das passwortbasierte Authentisierungsverfahren PACE**

Dr. Dennis Kügler, BSI

13:30-14:00

#### **Lösungsansätze bei 14443-Kommunikationsproblemen**

Florian Peters, Bundesdruckerei

14:00-14:30

#### **Kommunikationspause**

## **Session V**

### ***Quo vadis Gesundheitskarte***

Session Chair: Dr. Markus Schumacher, Fraunhofer SIT

14:30-15:00

#### **Migrationsstrategie für kryptographische Dienste von eGK und HPC**

Dr. Alfred Fiedler, gematik

15:00-15:30

#### **New Generation of the Slovene Health Insurance Card**

Marjan Sušelj, Tomaz Marčun, Health Insurance Institute of Slovenia

15:30-16:00

#### **Konzepte der Stapel- und Komfortsignatur**

Ulrich Waldmann, Fraunhofer SIT