Stand: 09.02.2016

Fraunhofer SIT

26. SmartCard Workshop

Termin	**17. und 18. Februar 2016, Mittwoch / Donnerstag**
Organisator	Ulrich Waldmann Fraunhofer-Institut für Sichere Informationstechnologie SIT Rheinstr. 75, 64295 Darmstadt
Programmbeirat	Michael Hegenbarth, Bundesdruckerei Detlef Kraus, SRC Dr. Gisela Meister, Giesecke & Devrient Dr. Gerd Pfeiffer, CardInsight Uwe Schnabel, HID Global Dr. Friedrich Tönsing, T-Systems Ulrich Waldmann, Fraunhofer SIT

Mittwoch, den 17. Februar 2016

ab 7:30	***Anmeldung***
09:00-09:05	***Begrüßung*** Ulrich Waldmann, Fraunhofer SIT
09:05-09:40	***Keynote*** MinR Achim Hildebrandt, BMI, Berlin
Session I	***Sichere Chipkarten*** Session Chair: Ulrich Waldmann, Fraunhofer SIT
09:40-10:05	**Konzepte für Chip-Sicherheit** Dr. Dennis Kügler, BSI, Bonn
10:05-10:30	**Sichere Updates von COS-Funktionen** Dr. Dominik Klein, BSI, Bonn
10:30-11:00	***Kaffeepause***

Mit freundlicher Unterstützung von:

T-Systems · SAFRAN Morpho · Bundesdruckerei · Giesecke & Devrient · SRC security consulting · NXP · TÜVIT TÜV NORD GROUP · HID

Stand: 09.02.2016

Mittwoch, den 17. Februar 2016

Session II — *Kryptographische Sicherheit*

Session Chair: Uwe Schnabel, HID Global

11:00-11:30	**Wirksamkeit von Blindingtechniken gegen Seitenkanalangriffe** Prof. Dr. Werner Schindler, BSI, Bonn
11:30-12:00	**Neuer Leitfaden für Elliptische Kurven Kryptographie** Dr. Dirk Feldhusen, SRC, Bonn Dr. Manfred Lochter, BSI, Bonn
12:00-12:30	**Sicherheitsmodelle auf Basis von SmartCard-Funktionalität** Hauke Meyn, NXP, Hamburg
12:30-13:30	***Mittagspause***
13:30-14:00	**Mehrkanal-Kryptokomponente für das BOS-Funknetz** Dr. Werner Schelb, T-Systems, Bonn

Session III — *Sichere Ausweise*

Session Chair: Michael Hegenbarth, Bundesdruckerei

14:00-14:25	**Mobiler Führerschein** Thomas Aichberger, Veridos, München
14:25-14:50	**Multi-applikative Ausweise auf Java Cards** Benjamin Drisch, cv cryptovision, Gelsenkirchen
14:50-15:15	**Virtuelle ID auf dem Smartphone** Philip Hoyer, HID Global, Walluf
15:15-15:40	**Ausweise und Gesichtsbilder der 3. Generation** Dr. Andreas Wolf, Bundesdruckerei, Berlin
15:40-16:10	***Kaffeepause***

Session IV — *Telekommunikation*

Session Chair: Walter Mohrs, Telekom Deutschland

16:10-16:35	**Subscription Management mit der Embedded SIM** Daniel Daksiewicz, Giesecke & Devrient, München
16:35-17:00	**eSIM - Die SIM-Karte aus der Cloud** Stefan Kaliner, Telekom Deutschland, Bonn
17:00-17:30	**Vortrag der Preisträger** Hanno Dietrich, Morpho Cards, Paderborn Walter Mohrs, Telekom Deutschland, Bonn
17:30-18:30	***Pause***

Abendveranstaltung

ab 18:30	**SmartBuffet**
ab 19:00	**La Java Blue Trio** Nathalie Schäfer - Gesang, Steffen Stütz - Piano, Wolfgang Ritter - Kontrabass

Mit freundlicher Unterstützung von:

Stand: 09.02.2016

Donnerstag, den 18. Februar 2016

09:00-09:30	***Keynote*** Salvatore Francomacaro, NIST, Washington, USA
Session V	***Standardisierung*** Session Chair: Dr. Gisela Meister, Giesecke & Devrient
09:30-10:00	**Standards for Identity Management and Privacy - Work in ISO/IEC JTC 1/SC 27/WG 5** Prof. Dr. Kai Rannenberg, Universität Frankfurt
10:00-10:30	**Signaturen nach der eIDAS-Verordnung** Dr. Christoph Sutter, TÜViT, Essen
10:30-11:00	***Kaffeepause***
11:00-11:30	**Status Online Rollout der eGK** Dr. Alfred Fiedler, gematik, Berlin
Session VI	***Sichere Zahlung*** Session Chair: Detlef Kraus, SRC
11:30-12:00	**Host Card Emulation (HCE) – Überblick und Lösungen** Dietmar Maierhöfer, Giesecke & Devrient, München
12:00-12:30	**Sicherheitsüberlegungen zu HCE** Sandro Amendola, SRC, Bonn
12:30-13:30	***Mittagspause***
Session VII	***Paarungsbasierte Kryptographie*** Session Chair: Dr. Friedrich Tönsing, T-Systems
13:30-14:00	**Effizienz und Sicherheit von paarungsbasierter Kryptographie** Prof. Dr. Johannes Blömer, Uni Paderborn
14:00-14:30	**Practical Second Order Fault Attacks against Pairing** Dr. Juliane Krämer, TU Darmstadt
14:30-15:00	**Sicherheitsprozesse für den Einsatz attributsbasierter Kryptographie in der "Financial Cloud"** Agnes Diller, achelos, Paderborn
15:00-15:30	***Kaffeepause***
Session VIII	***Sichere Automobilkommunikation*** Session Chair: Ulrich Waldmann, Fraunhofer SIT
15:30-16:00	**Hardware-Basierte Sicherheitskonzepte in Automobilen** Andreas Fuchs, Fraunhofer SIT, Darmstadt

Mit freundlicher Unterstützung von: