

24. SIT-SmartCard Workshop

Termin	5. und 6. Februar 2014, Mittwoch / Donnerstag
Organisator	Ulrich Waldmann Fraunhofer-Institut für Sichere Informationstechnologie SIT Rheinstr. 75, 64295 Darmstadt
Programm-Komitee	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 5. Februar 2014, Ort: IHK Darmstadt, Rheinstr. 89 (neben SIT)

ab 8:30	Anmeldung
10:00-10:05	Begrüßung Ulrich Waldmann, Fraunhofer SIT
10:05-10:30	Keynote Prof. Dr. Kai Rannenber, Universität Frankfurt
Session I	Hardware & Kryptographie Session Chair: Ulrich Waldmann, Fraunhofer SIT
10:30-11:00	Angriffe auf Sicherheitschips Dr. Peter Laackmann und Marcus Janke, Infineon Technologies, München
11:00-11:30	Kommunikations- und Kaffeepause
11:30-12:00	Fortschritte bei Template-Analysen von Crypto-Prozessoren Dr. Joachim Schüth, T-Systems GEI, Bonn
12:00-12:30	Vergleich von eID-Privacy-Konzepten aus kryptographischer Sicht Prof. Dr. Marc Fischlin, CASED und TU Darmstadt
12:30-13:00	Grenzen der algorithmischen Kryptographie Prof. Dr. Werner Schindler, BSI, Bonn und CASED, Darmstadt
13:00-14:00	Imbiss & Kommunikationspause

Mit freundlicher Unterstützung von:



Giesecke & Devrient



Session II

Physical Uncloneable Functions

Session Chair: Michael Hegenbarth, Bundesdruckerei

14:00-14:25

Einsatz und Prüfung von Physical Uncloneable Functions
Dr. Rainer Plaga, BSI, Bonn

14:25-14:50

Sicherheitsanalyse von kommerziell verfügbaren PUFs
Prof. Dr. Jean-Pierre Seifert, TU Berlin

14:50-15:15

Sicherheitsarchitekturen mit Physical Uncloneable Functions
Dr. Olga Kulikovska und Dr. Walter Fumy, Bundesdruckerei, Berlin

Session III

Testen, Evaluieren, Zertifizieren

Session Chair: Detlef Kraus, SRC

15:15-15:40

Automatische Codegenerierung aus visuellen Testfallspezifikationen
Dr. Bastian Cramer und Dr. Dennis Klassen, achelos, Paderborn

15:40-16:10

Kommunikations- und Kaffeepause

16:10-16:35

Entwicklung von Standards für die Evaluierung von Chipkarten
Wolfgang Killmann, T-Systems, Bonn

16:35-17:00

Zertifizierungsprozess für das COS der eGK in der Praxis
Bertolt Krüger, SRC, Bonn

Vortrag zum Fraunhofer SmartCard-Preis 2014

17:00-17:30

Password Authenticated Connection Establishment
Dr. Jens Bender und Dr. Dennis Kügler, BSI, Bonn

17:30-17:45

Verleihung des Fraunhofer SmartCard-Preises an Dr. Jens Bender, Dr. Dennis Kügler und Prof. Dr. Marc Fischlin
Laudatio: Dr. Gisela Meister, Giesecke & Devrient

17:45-18:30

Pause (Ortswechsel zum SIT)

Abendveranstaltung im SIT (Rheinstr. 75)

ab 18:30

SmartBuffet
Buffet mit Fassbier & Wein

ab 19:00

Trio Azul
Anibal Civilotti, Argentinien - Gesang, Gitarre
Omar Plasencia, Venezuela - Percussion, Vibraphon
Kurt Holzkämper, Deutschland - Kontrabass

Mit freundlicher Unterstützung von:



Giesecke & Devrient



Session IV

Standardisierung

Session Chair: Gerd Pfeiffer, CardInsight

09:00-09:30

Datenobjekt-basierendes Kartenbetriebssystem

Achim Pietig, tmCn, Paderborn

09:30-10:00

Neue Parameter in ISO 14443

Hans Pirch, HID Global

10:00-10:30

Smart Cards - aktuelle Themen in der Telekommunikation

Heiko Kruse, Morpho Cards, Paderborn

10:30-11:00

Kommunikations- und Kaffeepause

Session V

Zukunft der Signaturkarten

Session Chair: Dr. Gisela Meister, Giesecke & Devrient

11:00-11:30

EU-Verordnung zur elektronischen Identifizierung, Authentisierung und Signatur (eIDAS)

Klaus-Dieter Wolfenstetter, Deutsche Telekom, Darmstadt

11:30-12:00

Technische Rahmenbedingungen der EU-einheitlichen Regulierung von elektronischer Identifikation, Authentisierung und Signatur, Arno Fiedler, Nimbus Technologieberatung, Berlin

12:00-12:30

Trustworthy Systems supporting Server Signing

Franck Leroy, Docapost EBS, Frankreich

12:30-13:30

Imbiss & Kommunikationspause

Session VI

Telekommunikation und mobile Sicherheit

Session Chair: Dr. Friedrich Tönsing, T-Systems

13:30-14:00

BSI-Sicherheitskarten auf mobilen Geräten

Dr. Gerhard Schabhüser, BSI, Bonn

14:00-14:30

Mobile ID der Global Platform

Alexander Summerer, Giesecke & Devrient, München

14:30-15:00

Embedded SIM - Status und Verantwortlichkeiten

Frank Sudholt, Deutsche Telekom, Bonn

15:00-15:30

Kommunikations- und Kaffeepause

Session VII

Neue Konzepte und Anwendungen

Session Chair: Uwe Schnabel, HID Global

15:30-16:00

Key2Share for Authentication Services

Alexandra Dmitrienko, Fraunhofer SIT, Darmstadt

16:00-16:30

Anwendungen identitätsbasierter Kryptographie

Juliane Krämer, TU Berlin

16:30-17:00

Lokale Integritätsverifikation von Systemen durch Java Smart Cards

Dr. Holger Kinkelin, TU München

Mit freundlicher Unterstützung von:



Giesecke & Devrient

