INHALTSVERZEICHNIS

24. SIT-SMARTCARD WORKSHOP

KEYNOTE

INTEGRATING AND TRIALLING ATTRIBUTE-BASED CREDENTIALS ON SMARTCARDS FOR BUILDING TRUST THE ABC4TRUST PROJECT
Ahmad Sabouri, Jonas Lindstrøm Jensen, Kasper Lyneborg Damgård, Janus Dam Nielsen, Kai Rannenberg 8

SESSION I: HARDWARE & KRYPTOGRAPHIE

ANGRIFFE AUF SICHERHEITSCHIPS
Marcus Janke, Peter Laackmann 24

FORTSCHRITTE BEI TEMPLATE-ANALYSEN VON CRYPTO-PROZESSOREN
Joachim Schüth 34

VERGLEICH VON eID-PRIVACY-KONZEPTEN AUS KRYPTOGRAPHISCHER SICHT
Marc Fischlin 44

GRENZEN DER ALGORITHMISCHEN KRYPTOGRAPHIE
Werner Schindler 52

SESSION II: PHYSICAL UNCLONEABLE FUNCTIONS

EINSATZ UND PRÜFUNG VON »PHYSICAL UNCLONABLE FUNCTIONS«
Rainer Plaga, Dominik Merli 64

SICHERHEITSANALYSE VON KOMMERZIELL VERFÜGBAREN PUFs
Jean-Pierre Seifert 70

SESSION III: TESTEN, EVALUIEREN, ZERTIFIZIEREN

AUTOMATISCHE CODEGENERIERUNG AUS VISUELLEN TESTFALLSPEZIFIKATIONEN
Bastian Cramer, Dennis Klassen 74

ENTWICKLUNG VON STANDARDS FÜR DIE EVALUIERUNG VON CHIPKARTEN
Wolfgang Killmann 84

ZERTIFIZIERUNGSPROZESS FÜR DAS COS DER eGK IN DER PRAXIS
Bertolt Krüger 92

VORTRAG ZUM FRAUNHOFER SMARTCARD-PREIS 2014

PASSWORD AUTHENTICATED CONNECTION ESTABLISHMENT
Jens Bender, Dennis Kügler 102

SESSION IV: STANDARDISIERUNG

DATENOBJEKT-BASIERENDES KARTENBETRIEBSSYSTEM, TEIL 2
Achim Pietig 112

NEW PARAMETER IN ISO/IEC14443
Hans-Juergen Pirch 118

SMART CARDS – AKTUELLE THEMEN IN DER TELEKOMMUNIKATION
Heiko Kruse 128

SESSION V: ZUKUNFT DER SIGNATURKARTEN

TECHNISCHE RAHMENBEDINGUNGEN DER EU-EINHEITLICHEN REGULIERUNG VON ELEKTRONISCHER IDENTIFIKATION, AUTHENTISIERUNG UND SIGNATUR
Arno Fiedler 138

TRUSTWORTHY SYSTEMS SUPPORTING SERVER SIGNING
Franck Leroy 146

SESSION VI: TELEKOMMUNIKATION UND MOBILE SICHERHEIT

MOBILE ID
Alexander Summerer 160

EMBEDDED SIM – STATUS UND VERANTWORTLICHKEITEN
Frank Sudholt 168

SESSION VII: NEUE KONZEPTE UND ANWENDUNGEN

KEY2SHARE FOR AUTHENTICATION SERVICES
Christoph Busold, Alexandra Dmitrienko
Christian Wachsmann 172

ANWENDUNGEN IDENTITÄTSBASIERTER KRYPTOGRAPHIE
Juliane Krämer 182

LOKALE INTEGRITÄTSVERIFIKATION VON SYSTEMEN DURCH JAVA SMART CARDS
Holger Kinkelin, Michael Dorner,
Georg Carle 190