idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

## Press release

### Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
### Oliver Küch

02/07/2014
http://idw-online.de/en/news572589

Contests / awards, Scientific conferences
Information technology
transregional, national

# Preis für Kryptobeweis

**Kryptologen-Team erhält Fraunhofer-SmartCard-Preis für Sicherheitsnachweis von Ausweis-Protokollen**

Der Fraunhofer-SmartCard-Preis 2014 geht an Prof. Dr. Marc Fischlin von der Technischen Universität Darmstadt sowie Dr. Jens Bender und Dr. Dennis Kügler vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Das Forscherteam erhält die Auszeichnung für die Definition, die internationale Verbreitung und Diskussion und nicht zuletzt für den Sicherheitsbeweis zum PACE-Protokoll, heißt es in der Begründung der Jury. Das Protokoll kommt bei der Prüfung von elektronischen Ausweisen zum Einsatz, zum Beispiel bei der Internet-Nutzung des neuen Personalausweises. Übergeben wurde der Preis am Mittwochabend im Rahmen des Fraunhofer-SmartCard Workshops. Der jährlich vergebene Preis würdigt Leistungen um die Chipkarten-Entwicklung und wird von einer unabhängigen Fachjury vergeben.

Das PACE-Protokoll wurde in den frühen 2000er Jahren vom BSI in Deutschland für den Einsatz in internationalen Ausweissystemen entwickelt. PACE steht für Password Authenticated Connection Establishment. Es handelt sich um ein passwortbasiertes Schlüsseleinigungsverfahren, das zur sicheren Prüfung von maschinenlesbaren Ausweisen, insbesondere Reisedokumenten, genutzt wird. In Deutschland erhielt das Protokoll durch die Einführung des neuen Personalausweises und dessen möglicher Internetnutzung erhöhte Bedeutung.

Der mathematische Beweis der Sicherheitseigenschaften gelang Prof. Dr. Marc Fischlin im Jahr 2009. Der Beweis hat die Akzeptanz und die Verbreitung des Protokolls stark gesteigert, und mittlerweile ist PACE von der ICAO (Internationale Zivilluftfahrt-Organisation) für den weltweiten Einsatz in Reisepässen vorgesehen. Seit Januar dieses Jahres ist das Protokoll im deutschen Reisepass implementiert. Die besondere Leistung zeigt sich auch daran, dass der Beweis erstmals in der Geschichte elektronischer Ausweise bereits in der Standardisierung des Protokolls erfolgte. Die mathematische Sicherheit vieler IT-Protokolle wurde bisher nicht standardmäßig gefordert. Der Sicherheitsbeweis von PACE ist ein wesentliches Qualitätsmerkmal dieses Protokolls.

Der SmartCard-Preis ist der europaweit bedeutendste Preis auf dem Gebiet der Chipkarten-Technik. Er wird seit 1994 im Rahmen des Fraunhofer-SmartCard Workshops jährlich verliehen.

URL for press release: http://www.smartcard-workshop.de

Die Preisträger v.l.n.r.: Prof. Dr. Marc Fischlin (TU Darmstadt), Dr. Dennis Kügler (BSI), Dr. Jens Bender (BSI).
Fraunhofer SIT