

Die [Fakultät für Informatik und Mathematik](#)
lädt ein im Rahmen der Vortragsreihe
„Datenschutz und IT-Sicherheit“:

Fakultät für
Informatik und
Mathematik



Globale E-Mailverschlüsselung an Jedermann

**Mechanismen und Verfahren zum
benutzertransparenten Zugriff auf digitale Zertifikate**

Dr. Gunnar Jacobson
Secardeo GmbH

Mittwoch, 26.10.11 um 17:00 Uhr in R 3.017

Abstract:

Wer kennt das nicht: "...beim Verschlüsseln für die (externen) Empfänger sind Probleme aufgetreten..." - auf diese typische Fehlermeldung der E-Mailanwendung reagiert der Benutzer genervt mit einem Klick auf "Unverschlüsselt senden!".

Viele E-Mails könnten Ende-zu-Ende zwischen Benutzern verschlüsselt werden, die ein Public Key Zertifikat besitzen. Millionen von Zertifikaten warten weltweit verteilt auf verschiedenen Zertifikatsverzeichnissen von Unternehmens- und Behörden-PKIs sowie öffentlichen Trustcentern auf ihre Nutzung. Der Vortrag erläutert, welche Probleme zu solchen Fehlermeldungen führen und mit welchen Maßnahmen und Mechanismen sie beseitigt werden können, um PKI-Interworking herzustellen. Dabei wird gezeigt, wie eine Client-Anwendung die benötigten X.509-Zertifikate für externe Empfänger bekommt, ihnen vertraut und damit beispielsweise eine S/MIME-Nachricht verschlüsseln kann. Neben der effizienten Suche durch einen Certificate Broker wird auch erläutert, wie der öffentliche Zugriff auf die eigenen Zertifikate abgesichert erfolgen kann. Mechanismen und Dienste wie Cross-Certification, Root-Signing, Certificate Trust Lists und PKI-Bridges zur Etablierung von organisationsübergreifendem Vertrauen werden gegenübergestellt.

Diese bereits in großen PKIs im praktischen Einsatz befindlichen Technologien werden ergänzt durch ein neuartiges Verfahren: Identity Certified Encryption - ICE. Hiermit können E-Mails mit herkömmlichen Anwendungen wie Outlook auch an beliebige Empfänger, die kein Zertifikat besitzen, Ende-zu-Ende verschlüsselt werden. Der Vortrag skizziert hiermit einen Blick in die Zukunft: Die benutzertransparente Ende-zu-Ende Verschlüsselung an Jedermann im Internet.

Klaus Köhler