RUHR-UNIVERSITÄT BOCHUM

RUB

Sec2

Ein mobiles Nutzer-kontrolliertes Sicherheitskonzept für Cloud-Storage

20.09. – 21.09.2011

Horst Görtz Institut für IT-Sicherheit
Lehrstuhl für Netz- und Datensicherheit

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Quelle: [http://www.miriadna.com]

Motivation

Risiken von Cloud Computing

Quellen:
[isc.sans.edu, www.cloudtweaks.com, nakedsecurity.sophos.com, www.infoworld.com, www.hgi.rub.de, www.zdnet.com, www.futuregov.asia, www.pcworld.com]

Sec² Konzept
Zielsetzung 1/2

- Nutzer-kontrollierte Sicherheit

  Benutzer behalten Kontrolle über ihre Daten
- Skalierbarkeit

  Konzeptionell auf Erweiterbarkeit und Interoperatibilität ausgelegt
- Effizienz

  Optimierte kryptografische Operationen (High-/Low-Level Optimierungen)
- Mobilität

  Auf mobilen Geräten nutzbar

Sec² Konzept
Zielsetzung 2/2

- Transparenz

  Für Benutzer weitestgehend transparent zu verwenden

- Nahtlose Integration

  Einfach zu integrieren, Co-existente Lösung zu bestehenden Strukturen

- Hybride Dokumente

  META Suche auf verschlüsselten Daten durch öffentliche Datenblöcke

Vorteile des Konzepts

Mehrwert zu bisherigen Ansätzen

- Sichere Datenablage auf beliebigen Cloud-basierten Speicherdiensten
- Sichere Etablierung einer Gruppenkommunikation
- Vollständige Kontrolle über die Daten durch Gruppenteilnehmer
- Keine Vertrauensbeziehungen zwischen Nutzern und Diensteanbietern

Technologieübersicht

Bausteine basierend auf etablierten Technologien

- XML – eXtensible Markup Language

  Daten-Strukturierung
- XML Signature

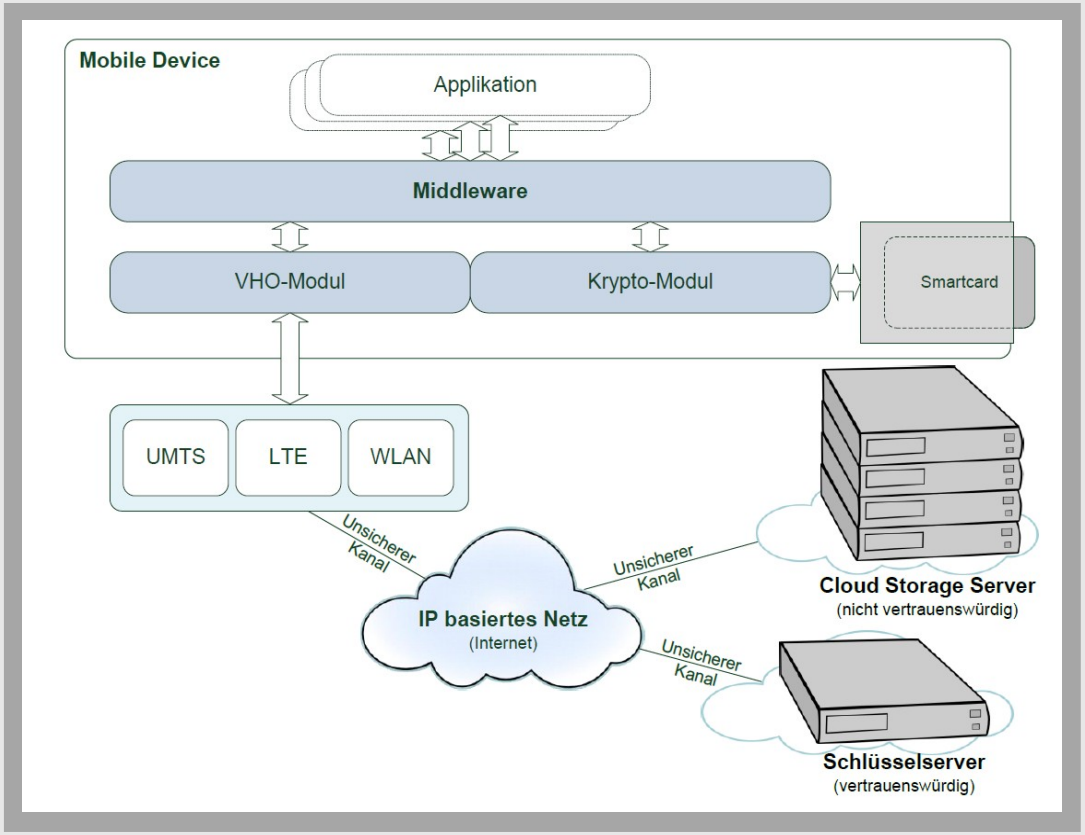
  Digitale Signaturen
- XML Encryption

  Ver- / Entschlüsselung
- SAML – Security Assertion Markup Language

  Modellierung von Sicherheitsaussagen

Architektur
Modulübersicht 1/2

- Applikation
  - *Endnutzer Anwendung*
- Middleware
  - *XML Verarbeitung*
  - *Schlüsselbeschaffung*
- Krypto-Modul
  - *Kryptografische Operationen*
  - *SmartCard Kommunikation*
- SmartCard
  - *Sicherer Schlüsselspeicher*



Architektur
Modulübersicht 2/2

- VHO-Modul

  Mediumübergreifende, nahtlose Kommunikation

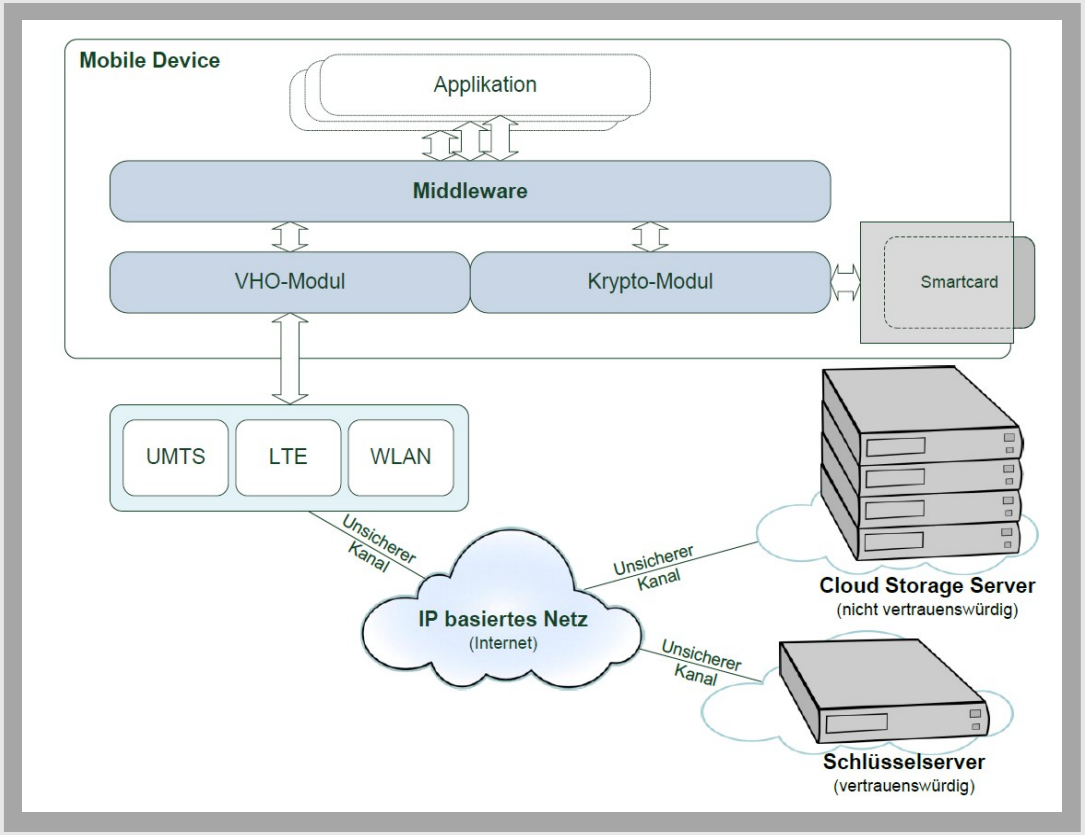
- Schlüsselserver

  Schlüsselspeicher für Gruppenschlüssel / öffentliche Teile der Benutzerschlüssel

  Gruppenverwaltung

- Cloud Storage Server

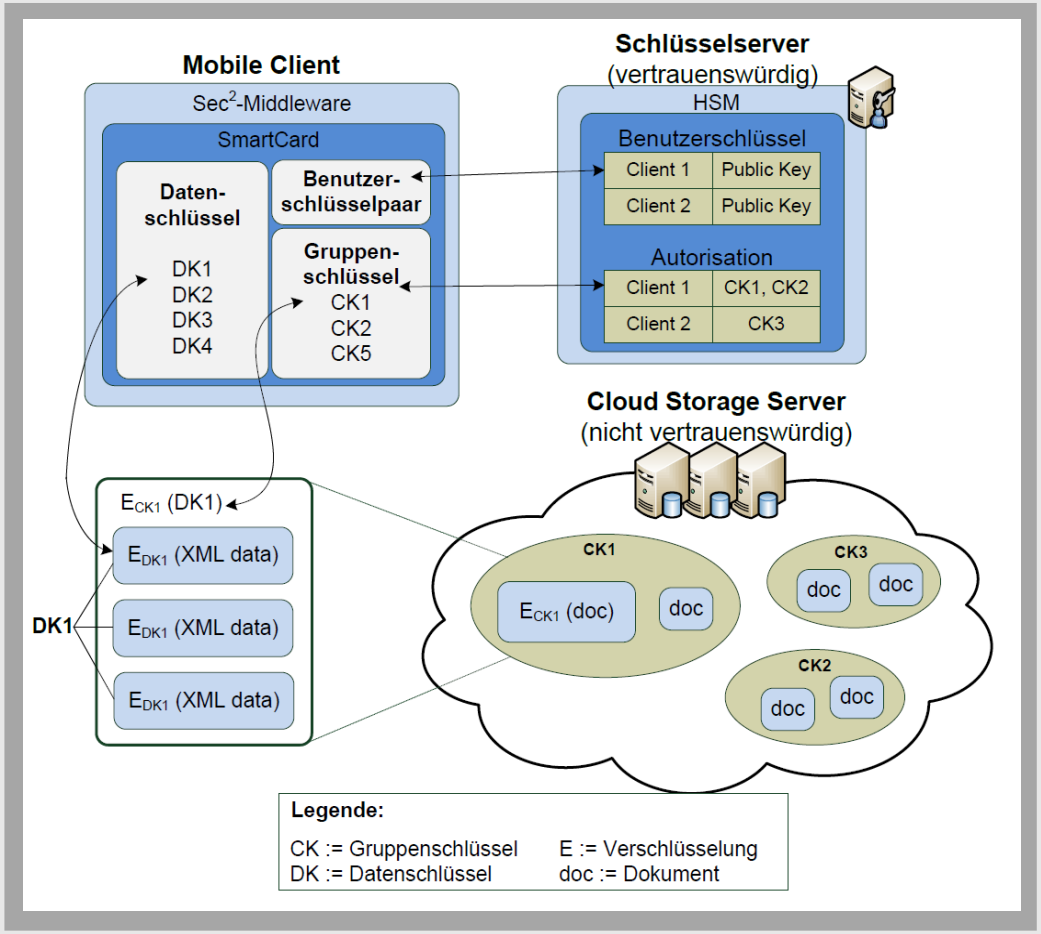
  Datenspeicher in der Cloud



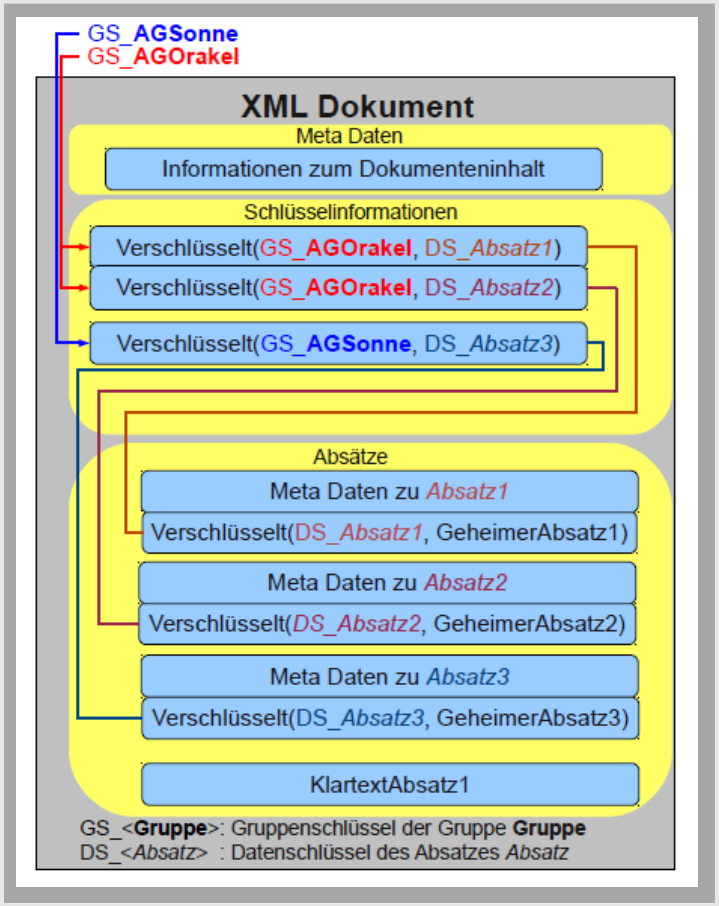
Hierarchisches Schlüsselkonzept

Schlüsseltypen

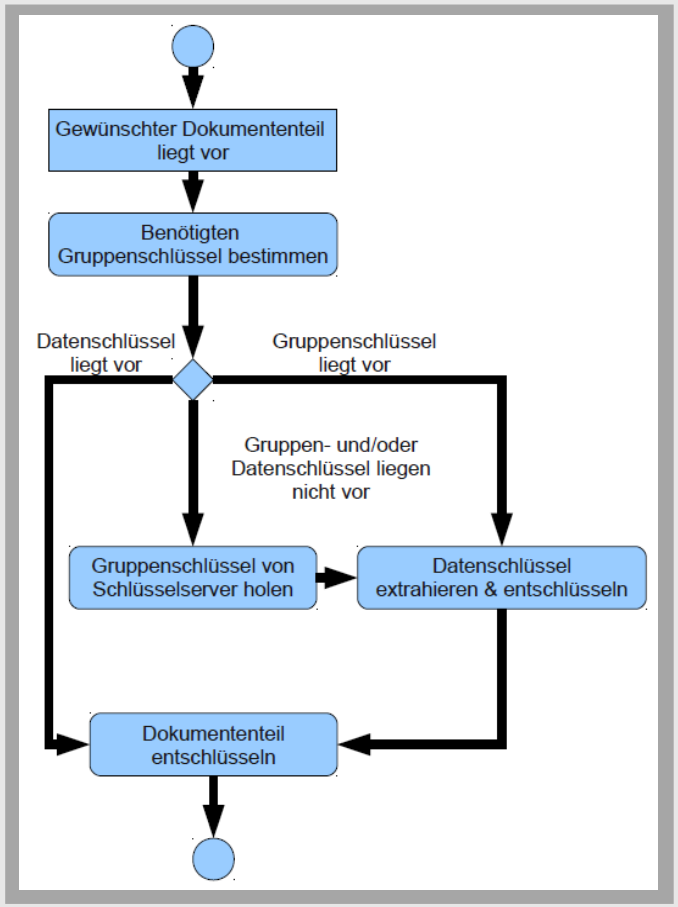
- Benutzerschlüssel (asym.)
  - *Schlüsseltransport*
  - *Authentifizierung*
- Gruppenschlüssel (sym.)
  - *Absicherung der Datenschlüssel*
- Datenschlüssel (sym.)
  - *Absicherung der Nutzdaten*



Schlüsselkonzept
Beispiel Dokument



Schlüsselkonzept
Ablaufdiagramm



Gemeinschaftsprojekt gefördert durch das BMBF

Koordiniert durch das DLR

hgi NDS — Lehrstuhl für Netz- und Datensicherheit *[www.nds.rub.de]*

Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit

hgi EMSEC — Lehrstuhl für Embedded Security *[www.crypto.rub.de]*

Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit

CNI — Lehrstuhl für Kommunikationsnetze *[www.cni.tu-dortmund.de]*

Technische Universität Dortmund

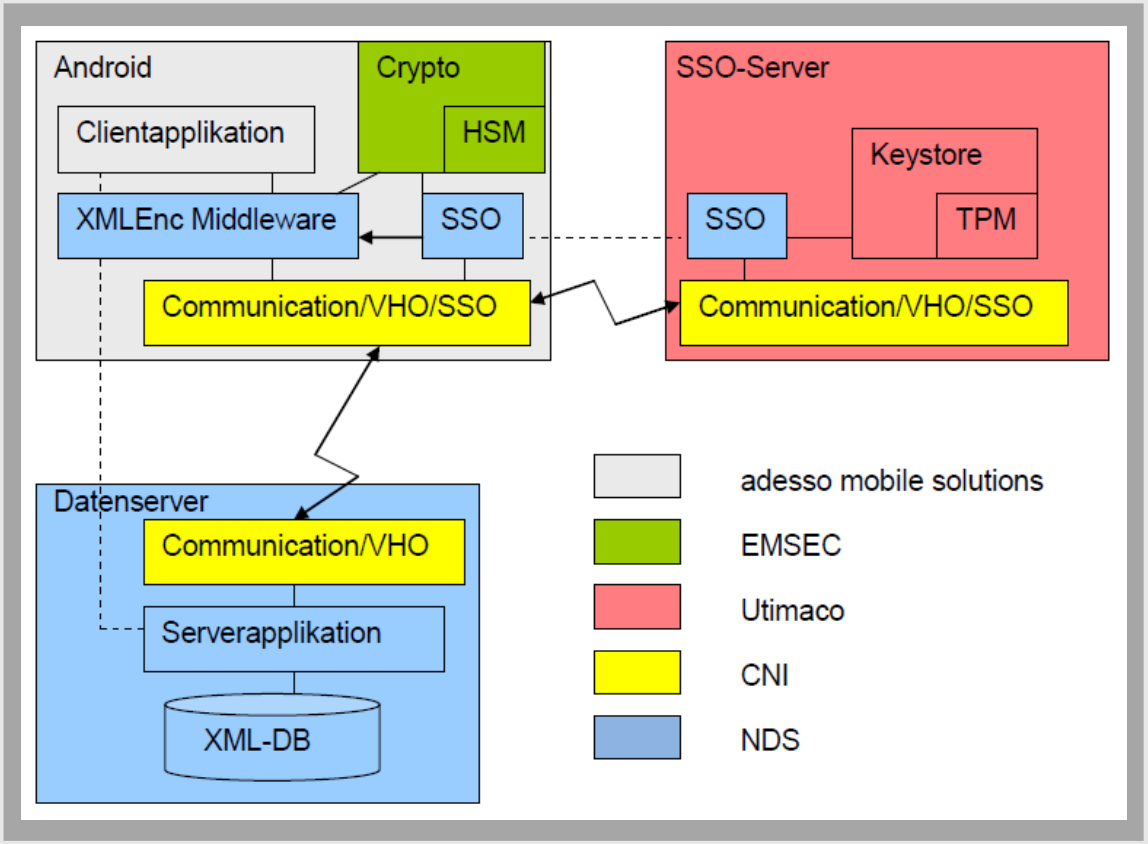
adesso mobile solutions — adesso mobile solutions GmbH *[www.adesso-mobile.de]*

Dortmund

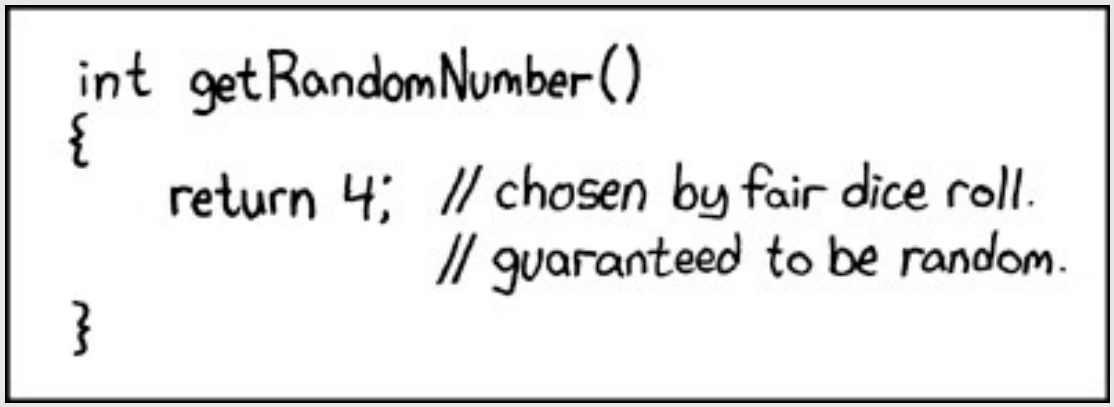
utimaco® a member of the Sophos Group — Utimaco Safeware AG *[http://hsm.utimaco.com]*

Aachen

Systemarchitektur
Aufgabenverteilung



Diskussion
Zeit für Ihre Fragen



Quelle: [www.xkcd.com]

gefördert vom
Bundesministerium für Bildung und Forschung (FKZ: 01BY1030)

Christopher Meyer
christopher.meyer@rub.de
http://www.nds.rub.de