Sicherheit

```
<Workshop Name="XML">
 <Datum> 28 Nov 2002 </Datum>
  <Ort>  Darmstadt, FhG-IPSI </Ort>
        <Vortragende>
       <Name>  Prof. Dr. Claudia Eckert</Name>
       <Firma> TU Darmstadt, FhI-SIT </Firma>
       </Vortragende>
</Workshop>
```

Gliederung

1. Einführung
2. Schutzziele, Sicherheitsbedenken, Angreifertypen
3. Problembereich Kommunikationswege
4. Problembereich Endgeräte
5. Problembereich Dienste-Anbieter
6. XML und Sicherheit
7. Zusammenfassung

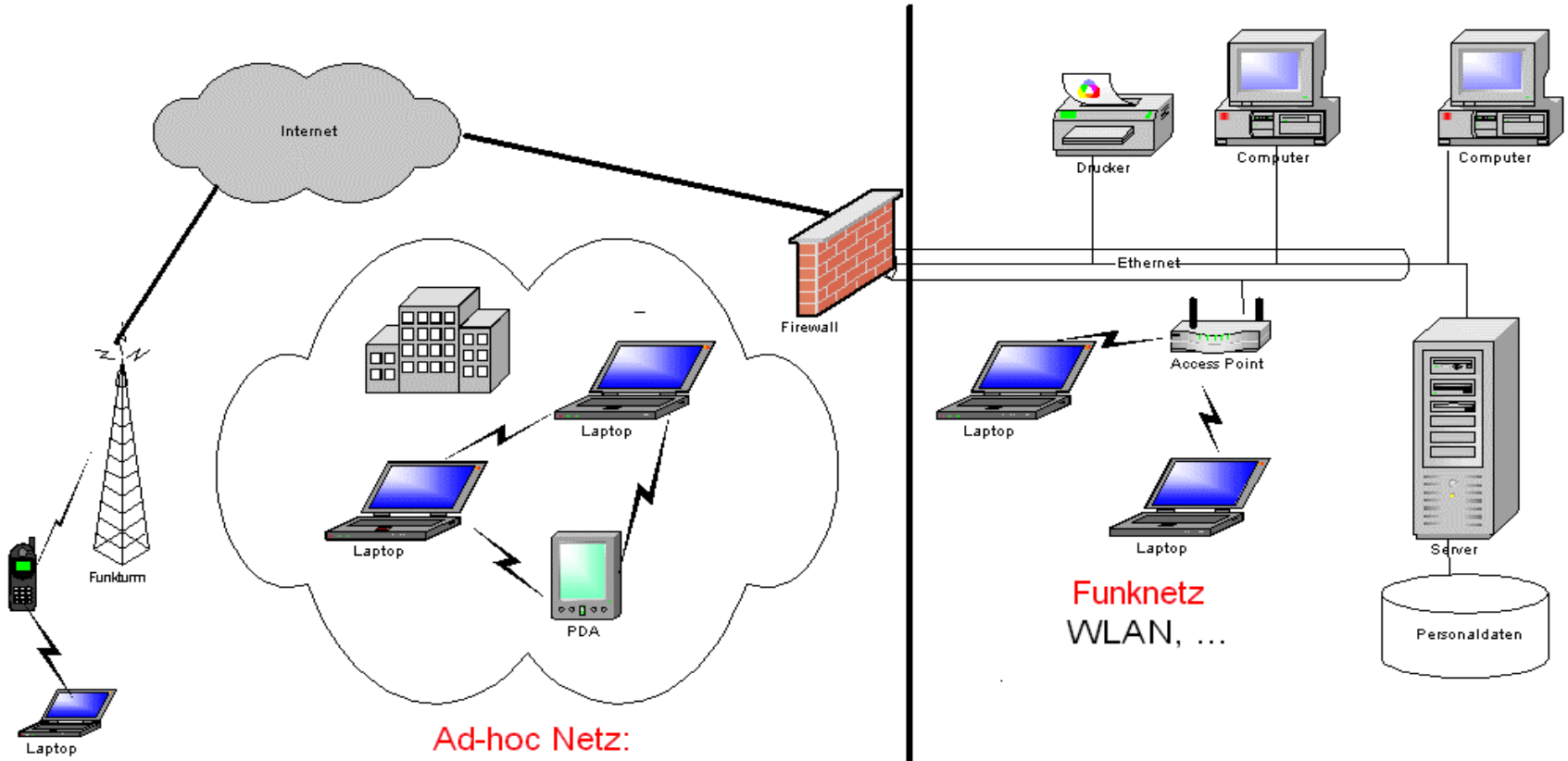
Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

1. Einführung

IT-Systeme: heute und morgen

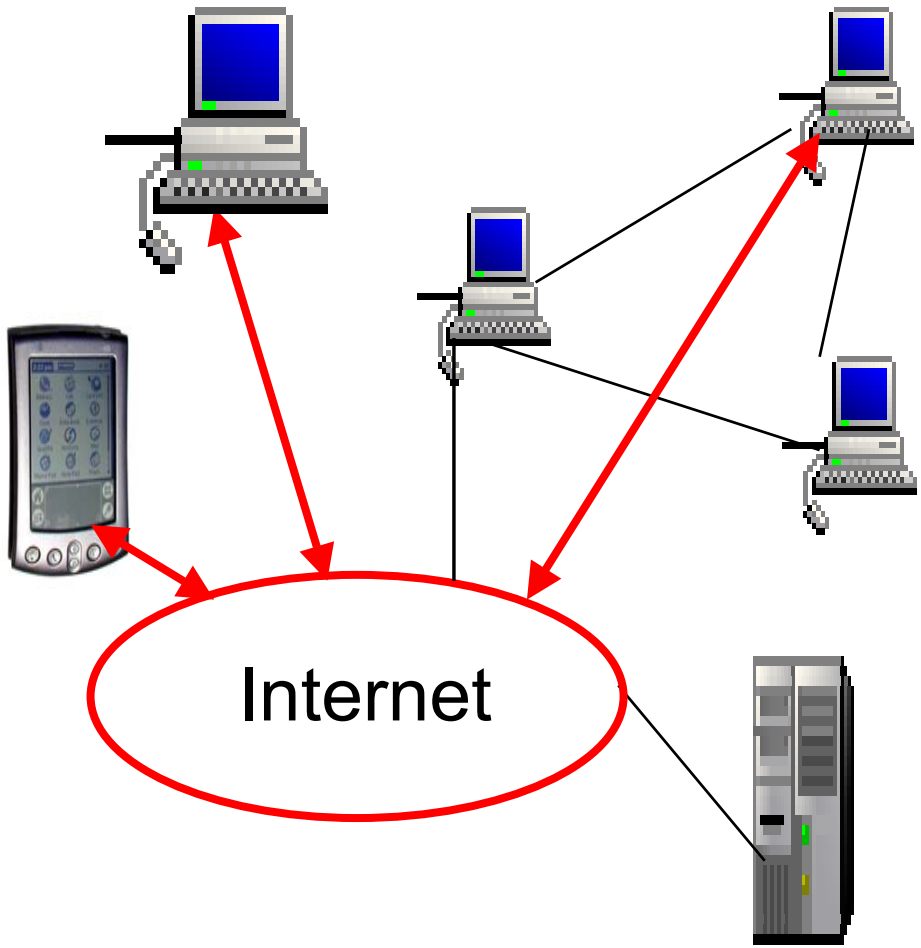


Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Nutzungsszenarien:



Mails: Versenden/Empfangen

Web-Services: Informationen, Content (XML, SOAP)

Download von Software

E-Commerce: Einkaufen, Verkaufen von Gütern, Content, ...

E-Business: XML-basierter Dokumentenaustausch

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

2. Schutzziele, Sicherheitsbedenken, Angreifertypen

Schutzziele:

- Authentizität: Glaubwürdigkeit eines Benutzers/Dokuments
- Vertraulichkeit: keine unautorisierte Informationsgewinnung
- Integrität: keine unautorisierte Datenmanipulation
- Verbindlichkeit: kein Abstreiten von Aktionen im Nachhinein
- Verfügbarkeit: keine Verhinderung berechtigter Zugriffe
- Privatheit: keine unautorisierte Profilbildung, Privatsphäre

Zu klären: welche Sicherheitsprobleme- u. bedenken bestehen?
wie wirksam sind die vorhandenen Lösungen?
Ende der Geschichte oder unendliche Geschichte?
Zusammenhang XML und Sicherheit?

Fraunhofer SIT Institut Sichere Telekooperation

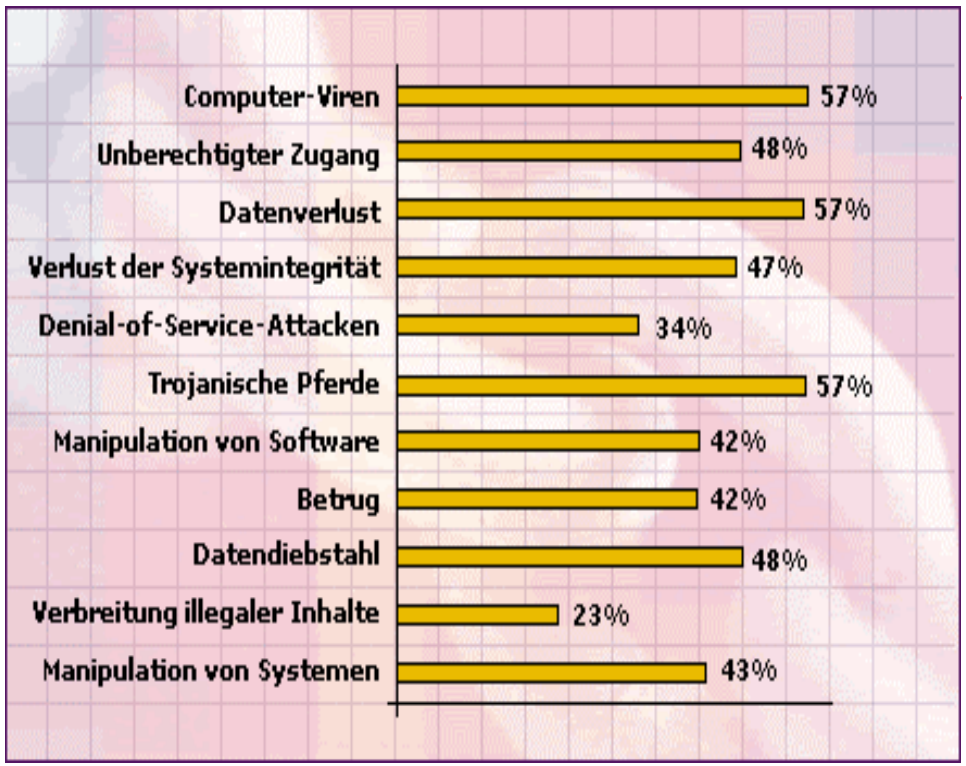
TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

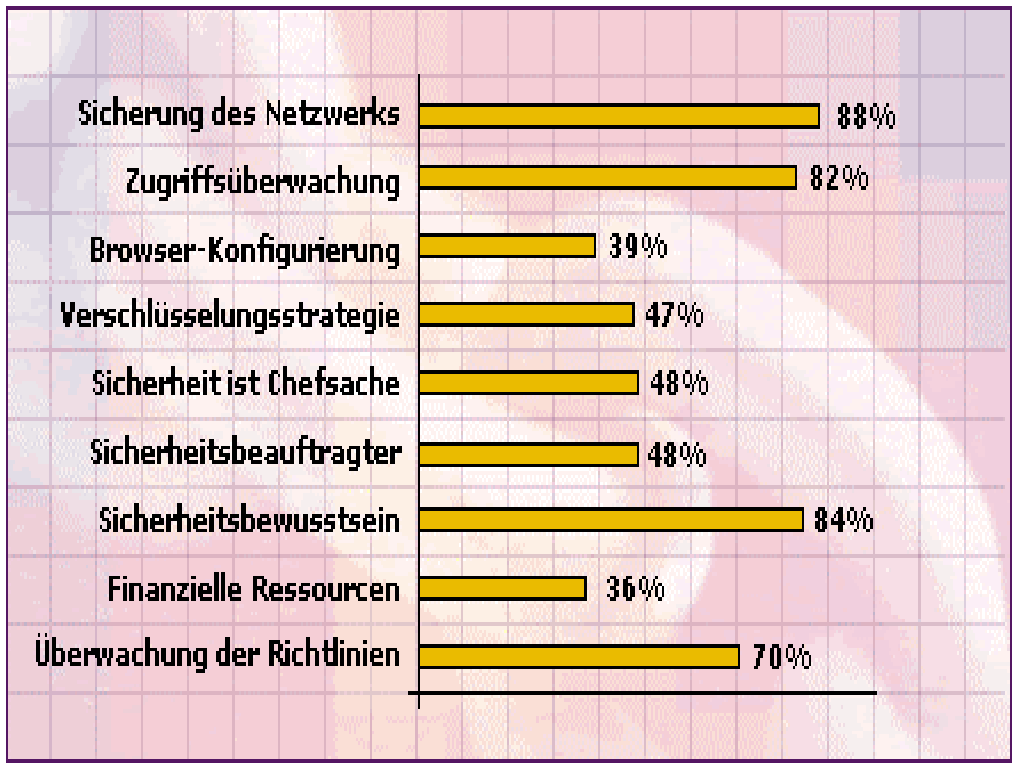
Was sind die größten Sicherheitsprobleme?

Ergebnisse einer Studie/Umfrage in 2002, 483 KMUs

Frage 1: was gefährdet die Sicherheit am meisten?



Frage 2: was sind die wichtigsten Faktoren für die Sicherheit?



Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Wer sind die typischen Angreifer?

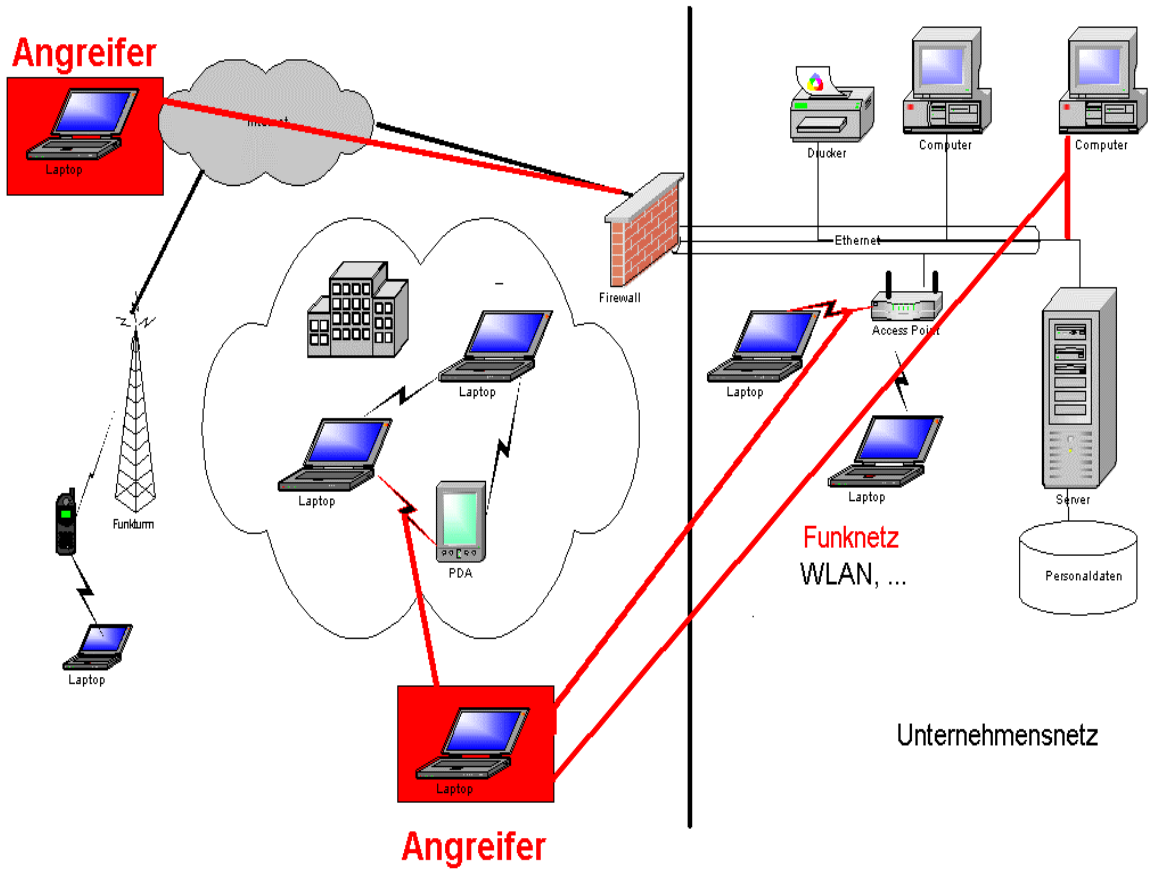
- über 50% aller Angriffe durch Mitarbeiter
- sehr häufig: durch Nachlässigkeit, Unwissenheit der Benutzer
  und der Administratoren
- Typische Beispiele: Passwort auf Zettel am Bildschirm
- Hacker: versierter Spezialist,
  Ziel: Lücken auffinden, warnen, selten Missbrauchsabsicht
- Cracker: versierter Spezialist i.d.R. mit Missbrauchsabsicht
  Ziel: Angriffe auf schlecht geschützte kleine Unternehmen,
  veraltete Systeme, Regierungsstellen
- Skript Kiddie: nutzt fertigte Exploits, wenige Kenntnisse, viel Zeit
  große Gefahr! Sehr großes Potential an Angreifern!

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

3. Problembereich Kommunikationswege



Angriffe: u.a.

- Abhören!
- Verändern!
- Maskieren!

Abwehr:

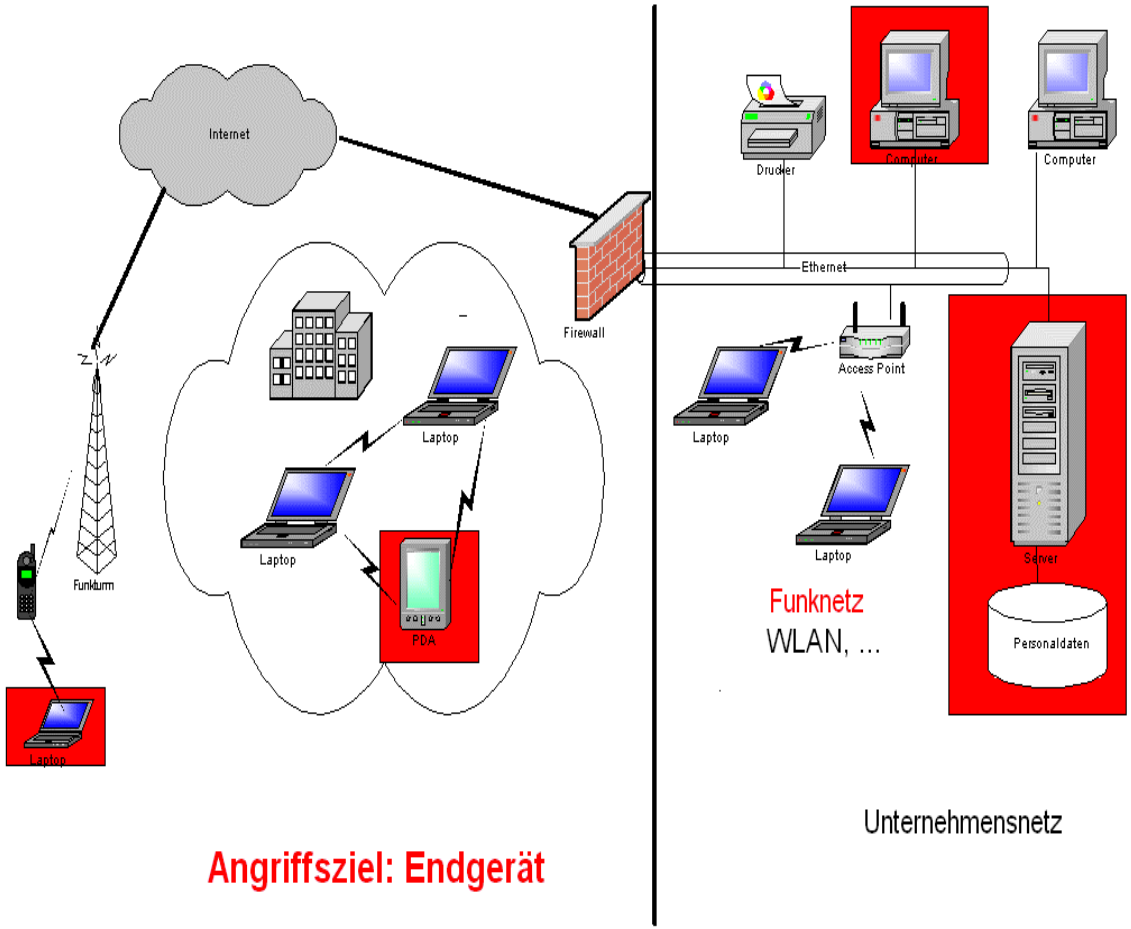
- Verschlüsseln,
- Hashwerte
- Digitale Signatur
- Protokolle:
  SSL, IPSec, SSH, ...

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

4. Problembereich Endgeräte



Angriffe: u.a.

- Viren, Würmer, Trojaner
- JavaScript, VBScript, ...
- Buffer Overflow Exploits,
- Datenspuren: Cookies, ...

Abwehr: u.a.

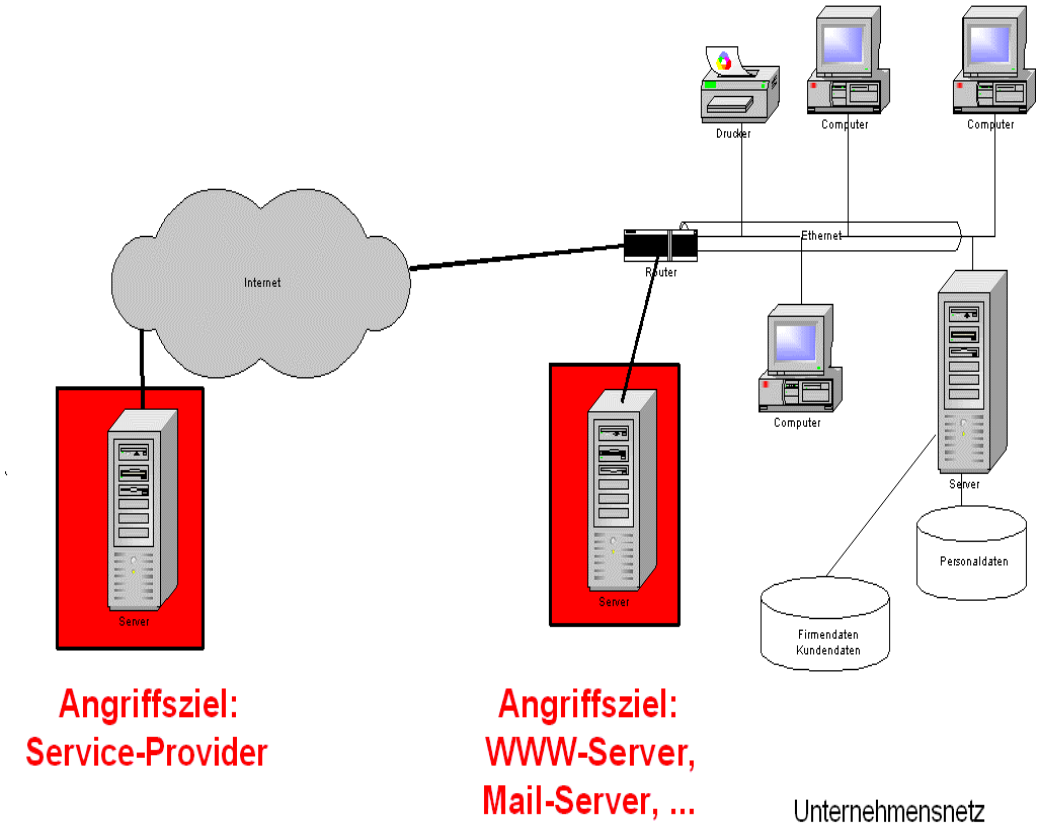
- Zugangskontrolle:
  Chipkarte, Biometrie, ...
- Zugriffskontrolle:
  Zugriffsbeschränkungen
- Überwachung:
  Viren-Scanner, Firewalls, ...

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

5. Problembereich Dienste-Anbieter



Angriffe: u.a.

- Unautorisierte Zugriffe
- CGI, Cross-Side Scripting
- Denial-of Service

Abwehr:

- Ports schließen,
- Programmiersicherheit,
- Monitoring, Intrusion Detection

Ende der Geschichte? Oder Geschichte ohne Ende?

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Angriffs-Trends (Quelle: u.a. CERT-CMU 2002)

- Automatisches Scannen/Verbreiten von Angriffscode (u.a. Würmer))
- Koordinierte Angriffe: u.a. Distributed Denial of Service (DDoS)
- Jährliche Verdopplung von gefundenen Schwachstellen:

  Zeitintervall Time-to-Patch ist sehr kurz
- Modulare, dynamisch sich ändernde Angriffsvarianten
- Zunahme von Web-Services : XML-Dokumente über SOAP

  - HTML-basiert: Öffnen von Port 80 bei Firewalls dafür notwendig!

  - kein Schutz der XML-Dokumente!

Frage: Vertraulichkeit, Authentizität, Verbindlichkeit auch für XML?

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

6. XML Security Standards

- Integrität, Verbindlichkeit und Signaturen: XML Digital Signature
- Vertraulichkeit: XML Encryption
- Schlüssel-Management: XML Key Management Spec (XKMS)
- Autorisierungs-Regeln: Access Control Markup Language (XACML)
- Privatheits-Regeln (Poliy): Platform for Privacy Preferences (P3P)

6.1 XML Signaturen nach W3C (xmldsig)

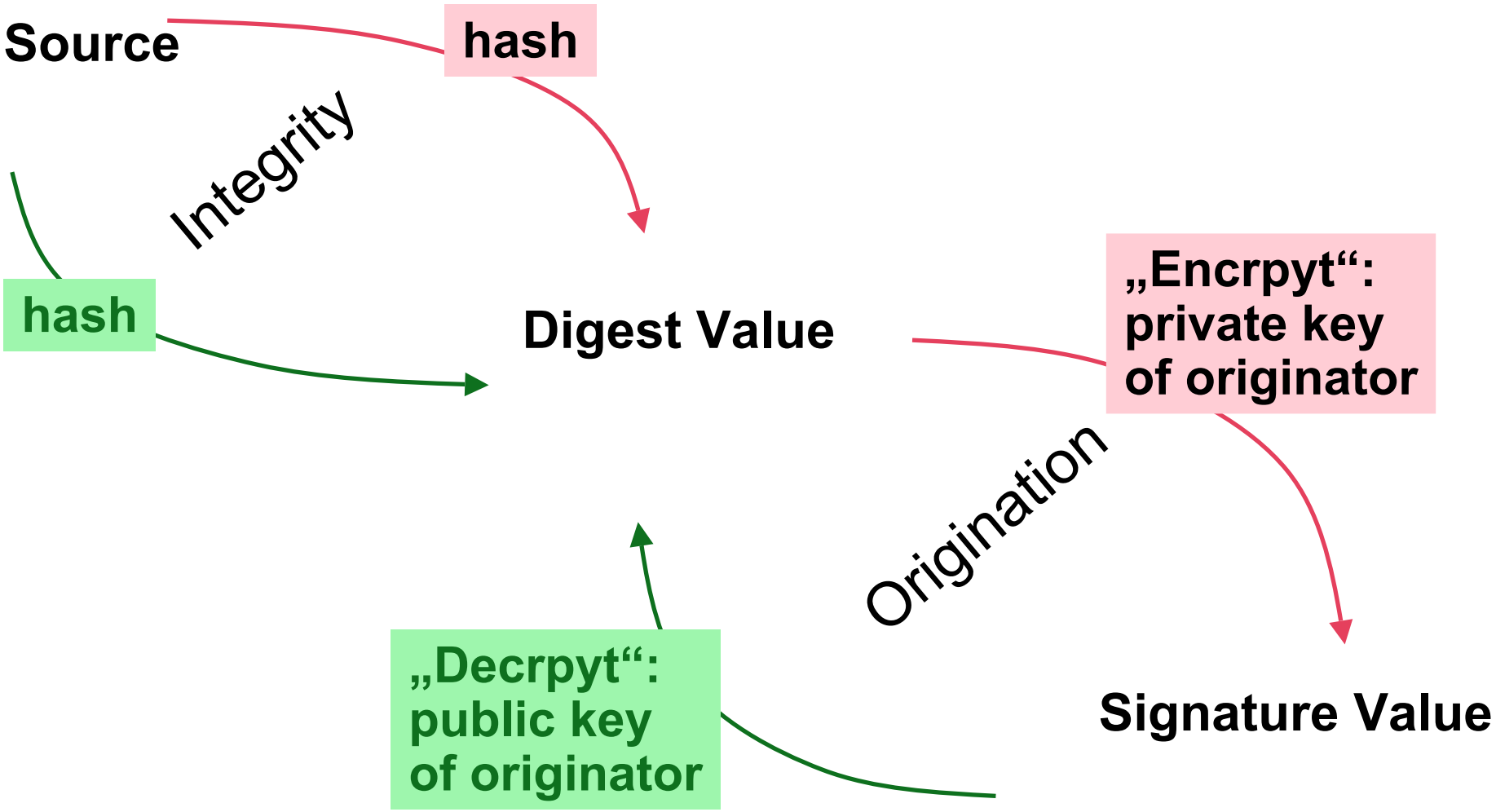
- Signieren entfernter Datenobjekte via URI oder lokale Datenobjekte
- Speicherung:
  - getrennt vom signierten Content: detached signature
  - eingebettet in den signierten Content: enveloped signature
  - signierter Content in Signatur: enveloping signature

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Technischer Einschub: Source (Content), Hashwert, Signatur



Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Beispiel: Enveloped Signature

```
<PatientRecord xmlns="http://www.medical.org/">
        <Name>John Doe</Name>
        <Account> 123456 </Account>
        <Visit date="10pm March 10, 2002"> ...  </Visit>
        <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'>
          <SignedInfo> ...
            <SignatureMethod> Algorithm = „http://www.w3org/2000/07/xmldsig#rsa-sha1“/>
             ...
            <DigestValue> <!– Hashwert des zu signierenden Items --> </DigestValue>
          </SignedInfo>
          <SignedValue> <!– Signatur des Hashwerts --> </SignedValue>  ...
          <KeyInfo> <KeyName> Signierschlüssel von Alice </KeyName>
          </KeyInfo>
        </Signature>
    </PatientRecord>
```


Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

6.2. XML Verschlüsselung nach W3C (xmlenc)

XML-Document versenden:

- Verschlüsseln eines XML-Elements mit symmetrischem Verfahren
- Ersetzen des Klartextes durch <EncryptedData> Element
- das <EncryptedData> Element spezifiziert u.a.:
  - den verwendeten Algorithmus

    <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
  - den verschlüsselten Content

    <CipherData> <CipherValue> a17xj2z</CipherValue> </CipherData>
  - den zur Entschlüsselung benötigten symmetrischen Schlüssel, der mit dem Public-Key des Empfängers verschlüsselt wird

```
<ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
    <ds:KeyName> Dr Kutter's public key pair </ds:KeyName>
</ds:KeyInfo>
<CipherData><CipherValue>xyzabc</CipherValue></CipherData>
<CarriedKeyName> Dr Kutter's symmetric key </CarriedKeyName>
```


Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Beispiel: Signiertes und verschlüsseltes XML-Dokument

```
<PatientRecord xmlns="http://www.medical.org/"
                    xmlns:lab="http://www.lab.org/">
  <Name> John Doe </Name>
  <Account> 123456 </Account>
  <EncryptedData Type='element'>
    ...
  </EncryptedData>
  <Signature>
    <SignedInfo> ...
      <Reference URI=""> ... </Reference>
    </SignedInfo>
  </Signature>
</PatientRecord>
```

Beachten: erst Klartext signieren, dann verschlüsseln!

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

6.3. XML Schlüsselmanagement nach W3C (xkms)

Protokolle für Trusted Services zur

- Erzeugung von Schlüsselpaaren,
- Registrierung und Zertifizierung von Public-Keys

  X-KRSS: The XML Key Registration Service Specification

  Request: *mein Name*

  Response: *Schlüsselpaar, Zertifikat (PKCS12)*

  <KeyBinding>-Element: Binden von Informationen an Schlüssel
- Speicherung und Wiedergabe von Public-Keys

  X-KISS: The XML Key Information Service Specification

  Request: <ds:KeyInfo>

  Response: *zugehöriger Public-Key (und Zusicherungen)*

  Server kann auch Gültigkeit des Zertifikats prüfen (vgl. PKI OCSP)

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

X-KISS: XML Key Informationsdienst

Rang 0:

GET Certificate
Extraktion Schlüssel durch Client
Zertifikatsprüfung durch Client

Rang 1:

GET KeyValue
Extraktion Schlüssel durch Trust Service
Zertifikatsprüfung durch Client

Rang 2:

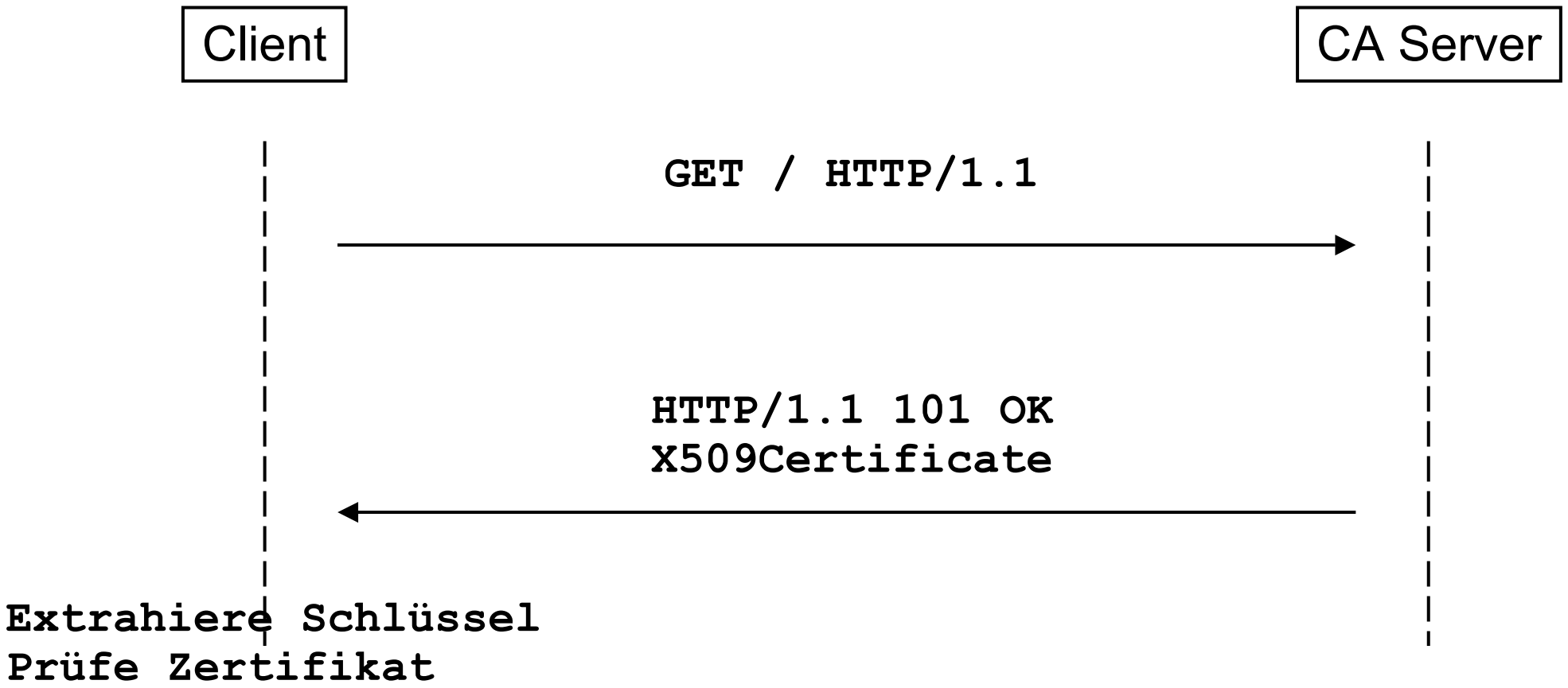
GET KeyValue and Validity Status
Extraktion Schlüssel durch Trust Service
Zertifikatsprüfung durch Trust Service

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

XML Key Informationsdienst, Rang 0

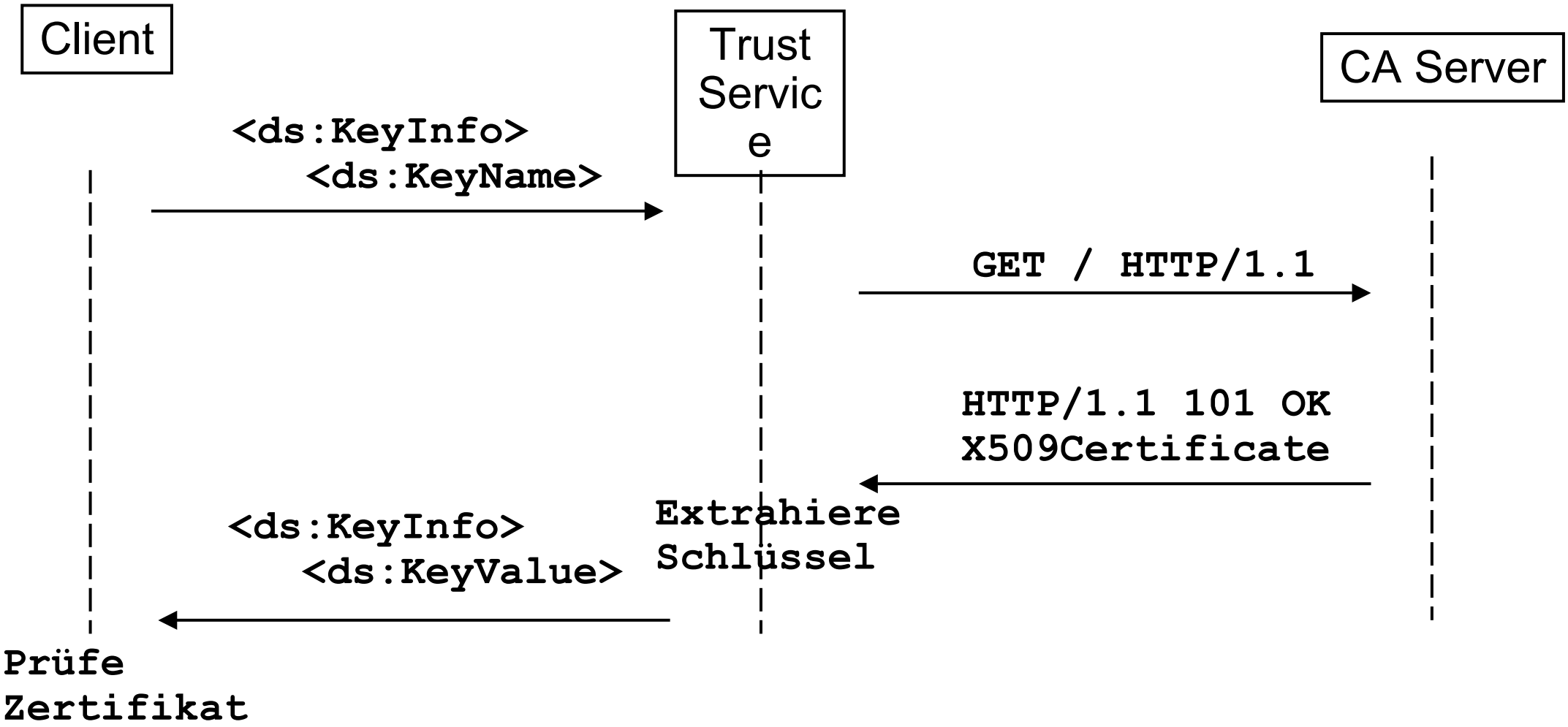


Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

XML Key Informationsdienst, Rang 1



Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

6.4 XML Privacy Policy nach W3C (p3p)

- Beschreiben von Privacy Policies (Service) u. Preferences (Client)

P3P Policy-Inhalte:

- Namen u. Kontaktinformationen des Betreibers (ENTITY DATA)
- Deklaration, ob personenbezogene Daten gespeichert werden, und
- Informationen über Zugriffsmöglichkeiten für User (ACCESS)
- Informationen über Schlichtungsstellen für Streitfälle (DISPUTES)

Pro Datengruppe (STATEMENT):

- Angaben über den Zweck der Erhebung (PURPOSE)
- Angaben über die Datenempfänger (RECIPIENT)
- Angaben über die Aufbewahrungsdauer (RETENTION)
- Art der erhobenen Daten (STATEMENT DATA)
- Vor- und Nachteile dieser Privacy Praxis (CONSEQUENCES)

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Beispiel: Auszug aus eines P3P Policy-Statements

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="forBrowsers" ...
 <ENTITY> <DATA-GROUP>  ...
  <DATA ref="#business.name">CatalogExample</DATA> </DATA-GROUP>
 </ENTITY>
 <ACCESS><nonident /></ACCESS>
 <DISPUTES-GROUP>
  <DISPUTES resolution-type="independent„ service="http://www.PrivacySeal.example.org" />
  <REMEDIES><correct /></REMEDIES> </DISPUTES>
 </DISPUTES-GROUP>
  <STATEMENT> <PURPOSE> <admin /> <develop /> </PURPOSE>
  <RECIPIENT><ours /></RECIPIENT>
  <RETENTION><stated-purpose /></RETENTION> ....
 </STATEMENT>
</POLICY> </POLICIES>
```


Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Zusammenfassung

Message: Datensicherheit ist mehr als Netzwerksicherheit!

(Un)Sicherheitskette bestehend aus vielen ‚Gliedern‘:

(1) (Un)Sichere Kommunikationswege: Internet, Funk-Netze, ...

(2) (Un)Sichere Endgeräte: PC, Workstation, mobile Geräte

(3) (Un)Sicherheit von/durch Dienste-Anbieter: Web-Server, -Services, ...

Merke: Schwächstes Glied der Kette bestimmt Sicherheitslevel!

XML-Sicherheit: versucht alle drei Bereiche zu adressieren:

- Verbindlichkeit, Vertraulichkeit : XML Digital Signature und Encryption
- Schlüssel-Management: XML Key Management Specification
- Aushandeln von Policies: Platform for Privacy Preferences (P3P)
- Autorisierungsregeln: Festlegen von Zugriffsbeschränkungen

Fraunhofer SIT Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert

Vielen Dank!

Fragen?!

Fraunhofer Institut Sichere Telekooperation

TECHNISCHE UNIVERSITÄT DARMSTADT

FB Informatik, FG Sicherheit in der Informationstechnik
Prof. Dr. C. Eckert