Integritätssicherung in XML-Dokumenten (für mobile Geräte)

Überblick XML Security

08.07.2002

Agenda

- **Einführung**
  - Motivation
  - Ziele der Arbeit
- Kryptographie
- XML-Signature
- Intermedate Modell
- Vertrauenskonservierung
- Übersicht und Erweiterungen

Motivation

- Warum diese Arbeit?
  - Grundlage für Reputationen sind signierte Dokumente
  - Mobile Systeme Vertiefungsschwerpunkt
- Warum ist sie wichtig?
  - E-Commerce benötigt Zertifikate
  - XML-Standard in mobilen Systemen
    - eröffnet Kompatibilität
    - schafft Vertrauen
    - erschließt ein enormes Marktsegment in dem mobile Geräte und XML-Standard zusammengeführt werden
- Idee dazu?
  - Mangel an zur Verfügung stehenden Ressourcen ☺

Agenda

- Einführung
- **Kryptographie**
  - Hashwert
  - Digitale Signaturen
  - Zertifikate
- XML-Signature
- Intermedate Modell
- Vertrauenskonservierung
- Übersicht und Erweiterungen

Einwegfunktionen

Berechnung f(x) = a ist einfach
Berechnung x von bekannten f()=a schwierig

Bsp.Primfaktorzerlegung:
f(a,b) = 667
Problem finde a,b ϵ Primzahlen, a * b = 667

Bsp. Diskretes Logarithmusproblem
a^x=b mod p, p ϵ Primzahl, a=3, p=17
Problem finde x aus: 14 mod 17 = 3^x

Einweghashfuntionen

Sind Einwegfunktionen, welche Texte beliebiger Länge auf einen Hashwert fester Länge abbilden

Forderungen Claude Shannon:

Konfusion: Statistische Eigenschaften Zufallsfolgen anpassen
Diffusion: Klartextzeichen auf möglichst viele Chiffrezeichen

Schwierig zwei Text zu finden, mit gleichem Hashwert!

Digitale Signaturen

Digitale Signatur soll handschriftliche Ersetzen:

- nicht fälschbar
  - Signierte Daten
  - Signatur selbst
- einfach überprüfbar
- nicht abstreitbar

Sinn:

Authentifikation/Authorisation

Integrität

Verbindlichkeit

Digitale Signaturen

Gebräuchliche Verfahren benutzen

- diskretes Logarithmusproblem
- Primfaktorenzerlegungsproblem

Asymmetrische Verfahren sind Zeitaufwendig

Statt Nachricht wird Hashwert signiert.

Forderung:

$$D_g(E_ö(M)) = D_ö(E_g(M))$$

Unterschrift und öffentlicher Schlüssel decken nicht den privaten Schlüssel auf.

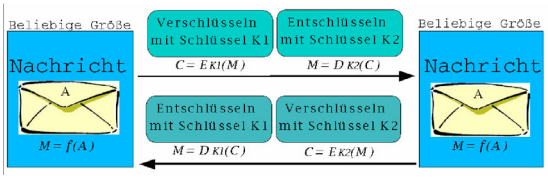
Digitale Signaturen

Unterschrift generieren

1. Hashen einer Nachricht
2. mit privaten Schlüssel den Hashwert chiffrieren

Unterschrift verifizieren

1. Hashen einer Nachricht
2. mit öffentlichem Schlüssel den Hashwert prüfen



Zertifikate

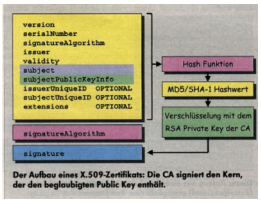
Definition: Ein Zertifikat ist ein elektr. Ausweis TcTrust

Definition: Ein Zertifikat nichts anderes als ein signierter Datensatz W.Ertel: Angewandte Krypto.

- Bindung einer Signatur an eine Person
- Bindung einer Signatur an eine Rolle/Autorität
- Bereitstellung von Meta-Information

Zertifikate X.509

Aufbau



Der Aufbau eines X.509-Zertifikats: Die CA signiert den Kern, der den beglaubigten Public Key enthält.

- Zertifikatsinhaber
- Zertifikatsausteller
- *Version, Ser.Number, Gülitgkeit, Sig.algorithmus*
- opt. Öffentlicher Schlüssel
- opt. Zertifikatsart - und klasse
- opt. Beliebige weitere Informationen (Version 3)

Agenda

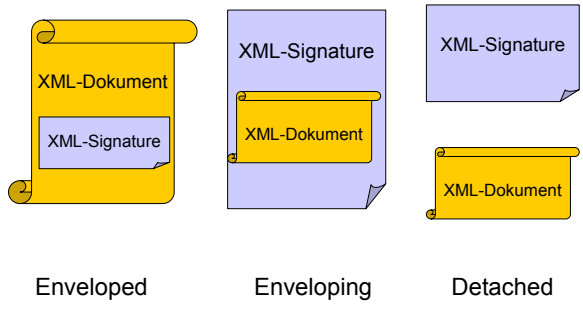
- Einführung
- Kryptographie
- **XML-Signature**
  - Arten
  - Aufbau
  - Technische Anforderungen
  - Ablauf Signaturverifikation XML-Sig
  - Canonicalization
- Vertrauenskonservierung
- Übersicht und Erweiterungen

Technische Anforderungen

Prüfsummenverfahren (Hashverfahren) (MD5, SHA-1)
Signaturen (DSA,RSA,ECDSA)
Zertifikate (X.509,..), Zertifikatsketten
Widerrufszertifikate [PKI, OCSP, ..]

XML-Parser	- Verarbeitung
XSLT	- Transformationen
XPATH	- Selektionen
XML-Signature	- Digitale Signaturen
XKMS	- „Abfragesprache" PKI

XML-Signature: Arten



XML-Signature: Aufbau

```
<Signature>
  <SignedInfo>
        <CanonicalizationMethode>  <Signature Method>
        <Reference (URI=)?>+
              <Transforms>?   <Transform>*
              <DigestMethod>  <DigestValue>
        </Reference>
       <Signature Value>
  </SignedInfo>
  (<KeyInfo>)?
  (<Object>)*
</Signature>
```


XML-Signature: Beispiel

```
<?xml version="1.0" encoding="UTF-8" ?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
  <CanonicalizationMethodAlgorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
    <Reference URI=""> <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>K8M/IPbKnuMDsO0Uzuj75lQtzQI=</DigestValue>
    </Reference>
  <SignatureValue>DpEylhQoiUKBoKWmYfajXO7...Q==</SignatureValue>
  </SignedInfo>
</Signature>
```


Ablauf Signaturprüfung

- Canonicalizierung XML-Dokument
- Transformation XML-Dokument
- Hashwertbildung aller Ressourcen
- Validierung Hashwerte
- Validierung Signatur über Hashwerte

- opt. Widerruf prüfen — XKMS?
- opt. Zertifizierungskette

Canonicalization Problem

1. Repräsentationen müssen normalisiert werden!
   - Zeichensubstitution (#x9,#xA,#0xD,#0x20,Spaces etc.)
   - Darstellbare Zeichenreferenzen substituieren &szig;
   - Werte normalisieren
2. CDATA Elemente / Deklarationen substituieren
3. Fehlende Standard Attribute einfügen
4. Namespace Erweitern ! (Problem)

Drei (zwei) Standards:

- Unterschiedliche Versionen
- mit/ohne Kommentaren
- unterschiedlicher funktionaler Unterstützung (XPATH)

Canonicalization: Example

Bespiel einer XML-Zeile:

<n1:elem1 xmlns:n1="http://b.example"> content </n1:elem1>

Eingefügt als Kindelement

<n0:pdu xmlns:n0="http://a.example">
<n1:elem1 xmlns:n1="http://b.example">
content </n1:elem1>
</n0:pdu>

Resultat, wenn <n1...> aus einem Canonical XML Dokument entnommen wird:

<n1:elem1 xmlns:n0="http://a.example"
xmlns:n1="http://b.example">content
</n1:elem1>

Agenda

- Einführung
- Kryptographie
- XML-Signature
- **Intermediate Modell**
- Vertrauenskonservierung
- Übersicht und Erweiterungen

Szenario: Reduzierte Funktionalität

Vorteile:

- kein Vertrauensproblem
- Kein Bandbreitenproblem

Nachteile:

- Nur selektive/vortransformierte XML-Dokumente!
- Welche Funktionen reduzieren?
- Aubau eines mobile XML-Sig?

Optimal ist Kombination aus reduzierter Funktionalität und Surrogaten!

Szenario: Intermediate

Teilausführung durch Surrogate

Nachteil: Vertrauen!!, Bandbreite
Funktionszerlegung

Vorteil: Preis, Größe

Szenario: Intermediate (2)

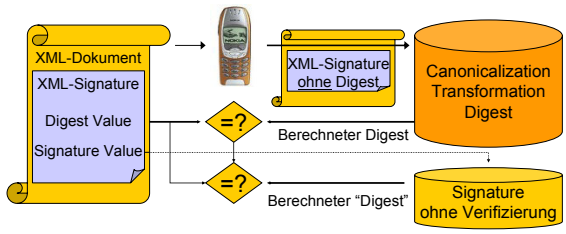
Vieles durch Surrogate ausführen

Kleine Teilausführung beim Gerät, um Vertrauen zu erhalten

Anforderungen:

- XML-Digest entfernen
- Teilberechnung einer Signatur
- org. XML-Dokument halten können
- RI-Forderung

Verifikation durch Mobiles System



- Verbergen des Vergleichwertes
- Täuschung eines orginären Dokuments nicht möglich

Agenda

- Einführung
- Kryptographie
- XML-Signature
- Intermediate Modell
- **Vertrauenskonservierung**
  - RI-Forderung
  - Connectivitätskonsum
  - Präferierte Lösungen
  - Vertrauensbildung durch multiple & iterative Distribution
- Übersicht und Erweiterungen

Laufende Arbeit: RI-Forderung

Problem des Vergleichs zwischen Betrug des Surrogaten und manipulierter Daten nicht möglich

Reversimplikative Forderung:

Ein orginäres Dokument darf als Falsifikant eingestuft werden.

Ein falsifikantes Dokument jedoch nie als Orginäres Eingestuft werden!

Täuschung einschränken!

Laufende Arbeit: RI-Forderung

Mittels RI-Forderung und Integritätssicherung kann Surrogatenlösung vertrauensvoll/gewiß sein!

Transformation:	*RI-Forderung + Integritätsicherung*
Integrität:	*Annahme gefälschtes Dokument*
	Org. Dokument/Hashwert darf nicht zur Verfügung stehen
Signatur:	*Annahme gefälschtes Dokument*
	Org. Dokument/Hashwert darf nicht zur Verfügung stehen

Laufende Arbeit: Surrogate

- Canonicalization, Transformation und Integritätssicherung durch einen Surrogat möglich!
  - Forderung: Entfernung der Prüfsumme
- Integritätssicherung durch Surrogat möglich:
  - Forderung: Teilberechnung Signatur (ohne Hashwertvergleich)

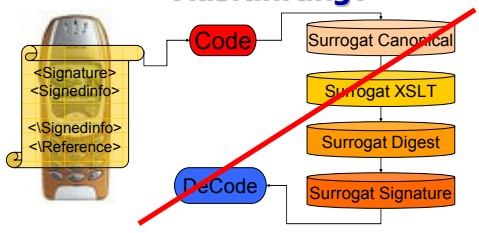
Vertrauen vs. Gewissheit

- Bei Vertrauen ist eine Ungewissheit, ein Betrug möglich
- Bei Gewissheit ein der Betrug ausgeschlossen

Ein „Basisvertrauen" (Gewissheit zugesprochen) bei:

- Eigenem Mobilen Gerät/Person
- Signierer / ordentlich signiertem Dokument
- Certification Authority (CA)

Vertrauen durch verschlüsselte Ausführung?

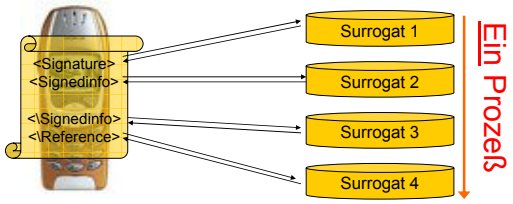


Kodierung zu rechenintensiv?!

Bei kryptographischen Verfahren ist eine minimale Änderung fatal!

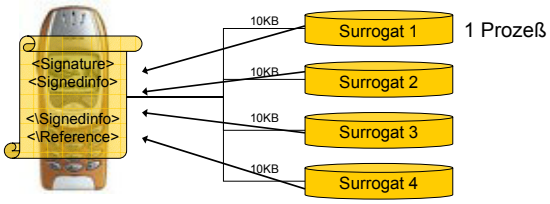
Diffussion Forderung von Claude Shannon'49!

Szenario: Iterative Distribution



Vorteile: Vertrauen durch IV schaffen
Distribution der Aktion "sichert" vor Betrug
Nachteile: Zielverarbeitung muß validierbar sein
XML-Dokumente -> Surrogat Position bekannt -> Betrug

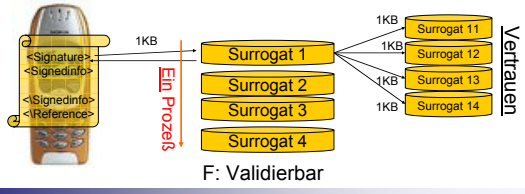
Szenario: Multiple Distribution



Vorteile: Zielverarbeitung kann ungewiß sein
Nachteil: Bandbreite!, Speicher?, CPU?
Welche Vertrauensberechnung?

LA: Kombination iterativer und multipler Verfahren:

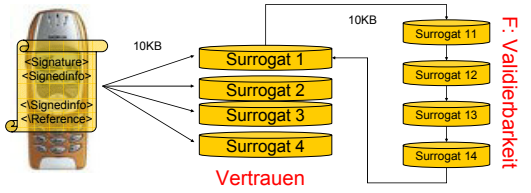
Vertrauen statt Gewissheit möglich! Sinn?
Surrogat/Deklarativ: Ein Vorteil? Bandbreite?
Warum kein reines multiples Verfahren?



F: Validierbar

LA: Kombination multiples und iteratives Verfahren

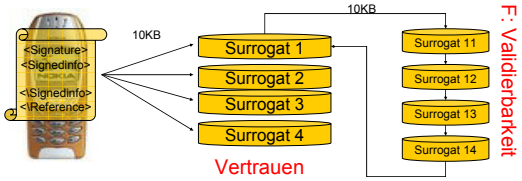
Gewissheit in Vertrauen möglich! Sinn?
Surrogat/Deklarativ: Ein Vorteil? Bandbreite?
Warum kein reines multiples Verfahren?



LA: Fazit Kombination iterativer und multipler Verfahren:

Vertrauen auf Kosten von Surrogatenzahl und Bandbreite

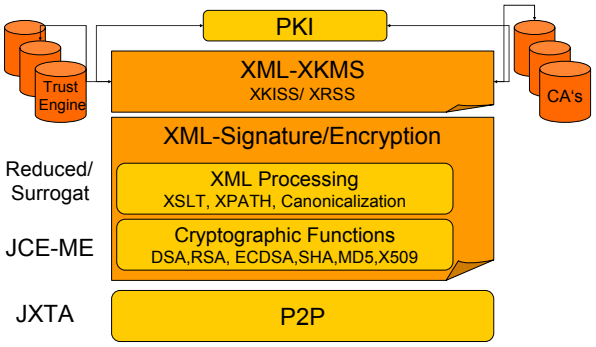
Vorteil?: Bandbreite des Surrogaten nutzen?
Nachteil: Ist Surrogat nicht vertrauensvoll, Ersparnis sinnlos



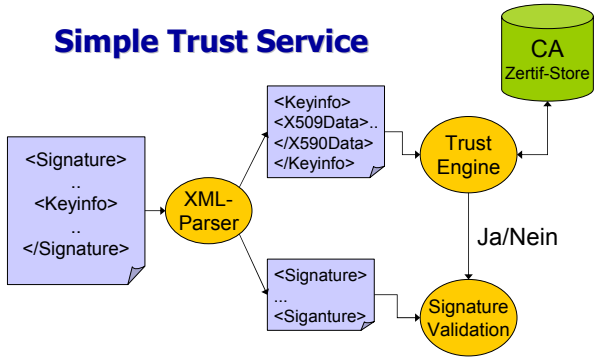
Agenda

- Einführung
- Kryptographie
- XML Signature
- Intermediate Modell
- Vertrauenskonservierung
- **Übersicht und Erweiterungen**
  - Nutzbare Technologien
  - Simple Trust Service

Nutzbare Technologien



Simple Trust Service



Stand der Arbeit

Schriftliche Ausarbeitung

Theoretische Grundlagen 2.Überarbeitung

Hauptteil: Beginn Rohentwurf

Praktisches

Aufbohren

XML- Signature Komplettlösung IXSIL von TU-Graz für die mobile Lösung

Fehlen: Zerlegung Signaturverfahren !!!

Zertifikate und Zertifikatsketten, incl. Widerruf (XKMS, PKI), P2P

Ende

Fragen?

Diskussion?

Feedback please!