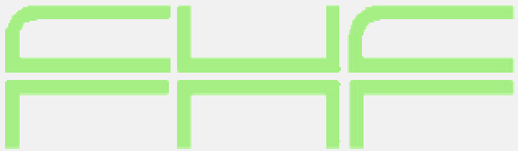
Security and Privacy mit XML

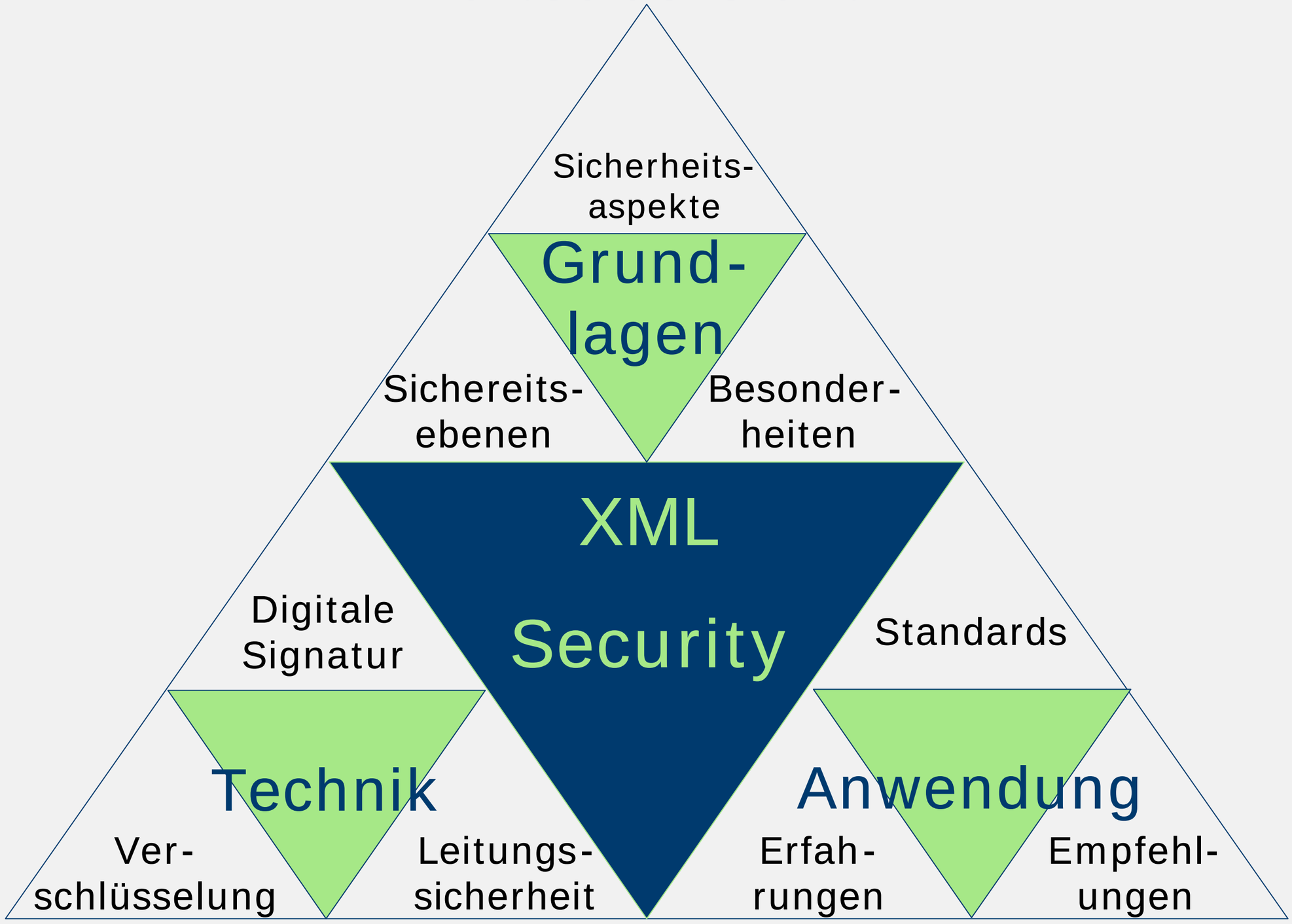


Prof. Mario Jeckle

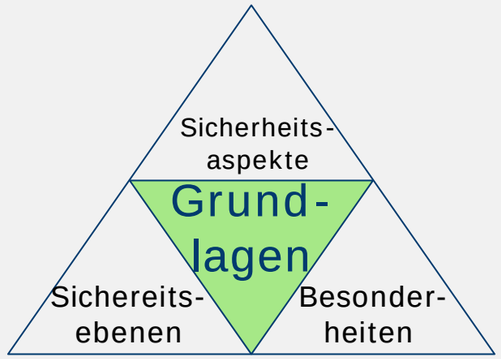
Fachhochschule Furtwangen
mario@jeckle.de
http://www.jeckle.de

sd&m-Konferenz 2003: Web Services

Inhaltsübersicht

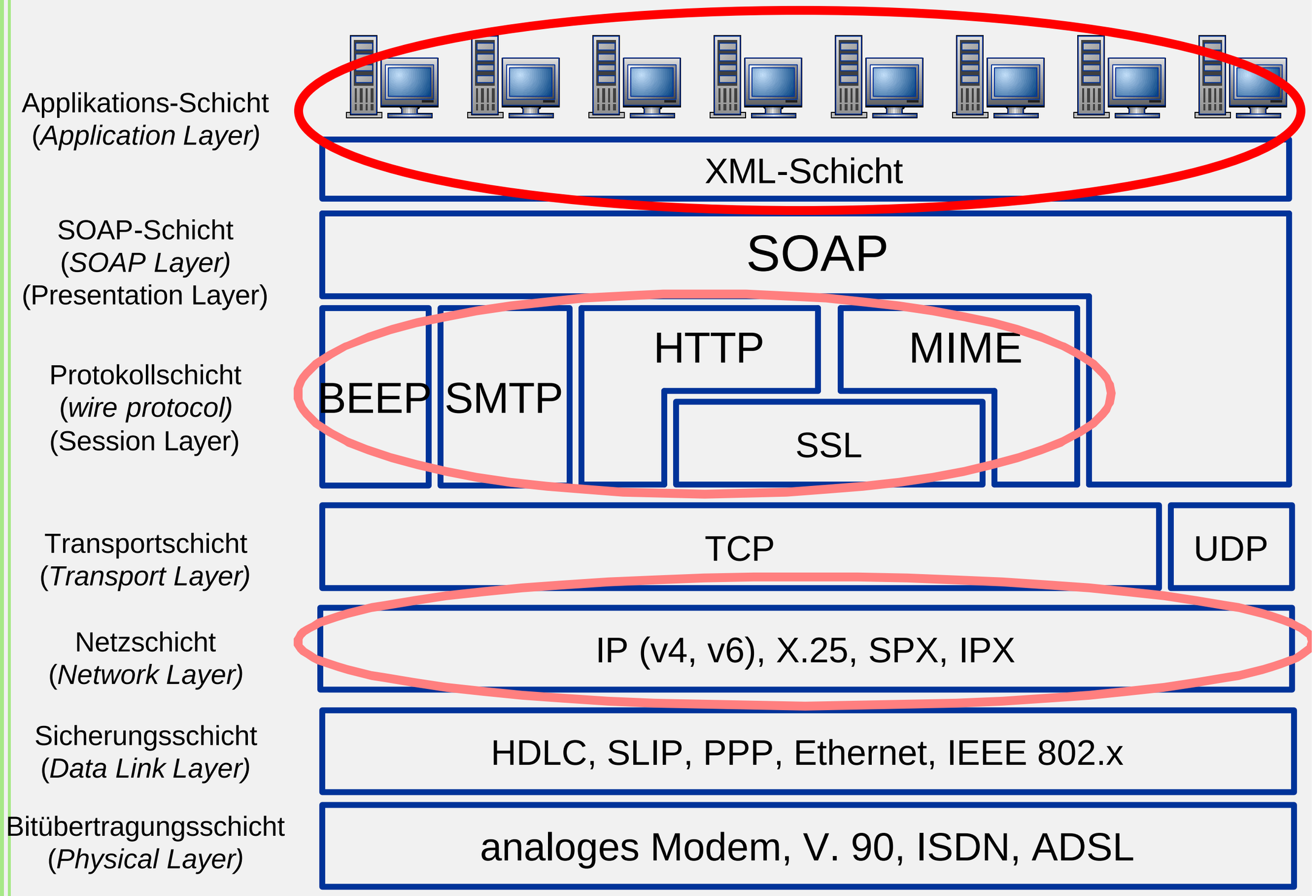


Sicherheitsaspekte

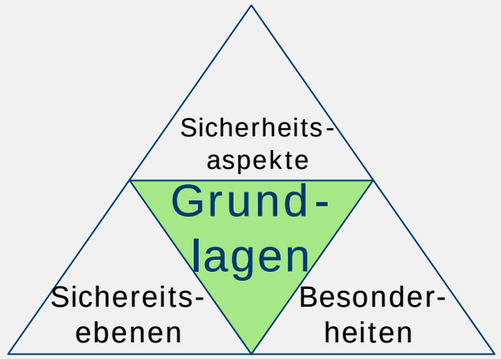


- **Vertraulichkeit** (confidentiality)
  Schutz der Daten vor dem (lesenden) Zugriff unbefugter Dritter
- **Berechtigung** (authorization)
  Gewährleistet Befugnis des Anforderers zur Nutzung des Diensten
- **(Daten-)Konsistenz** (data integrity)
  Verlangt modifikationsfreies Eintreffen der versandten Daten
- **Glaubwürdigkeit des Ursprungs**
  (message origin authentication)
  Garantiert, daß eine Nachricht willentlich durch einen Sender erstellt wurde
- **Verbindlichkeit** (non-repudiation)
  Stellt sicher, daß der Sender die Autorenschaft nicht leugnen kann

Sicherheitsebenen

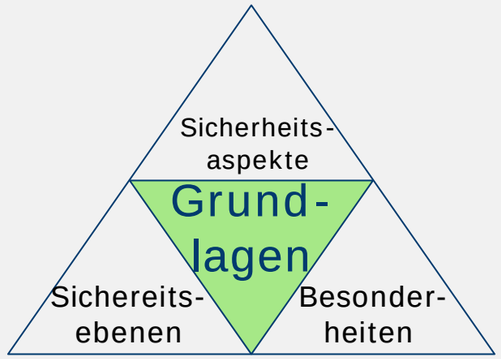


Besonderheiten



- Wunsch nach Erfüllbarkeit der klassischen Sicherheitsanforderungen
- Berücksichtigung der spezifischen Eigenschaften von XML
  - Unicode-basiert
  - Infoset-Struktursemantik
  - Lexikalische XML-Struktur
  - Struktur optional durch DTD oder XML-Schema definiert

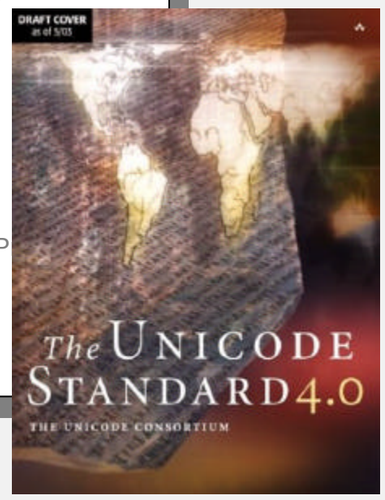
Besonderheiten



- Berücksichtigung der spezifischen Eigenschaften von XML
  - Grundfrage:
    Soll gesichertes XML noch XML sein?
    – Erhalt der Unicode-basiertheit

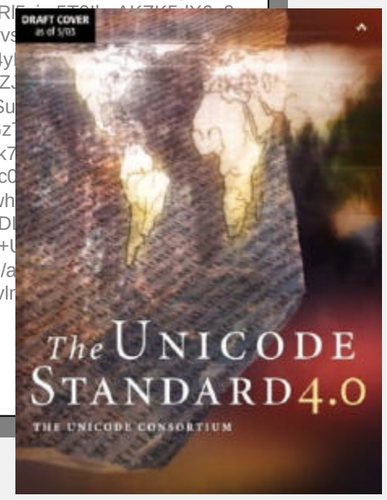
```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line>
      <Price currency="€">35264</P
      <Engine>220 CDI</Engine>
    </Vehicle>
  </Artikel>
</Bestellung>
```

Sicherung →

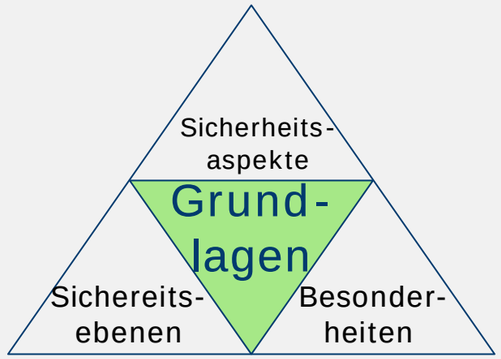



```
-----BEGIN PGP MESSAGE-----

qANQR1DBwk4DeAMSaxcCQrkQC/4wnHvmCnUGxT1izkGIGs/zfr6voDyrdjyNLTBR
62qOh5HlAH6OrKOHspnQVufZTh6LfdtGiyEhXxpjkfdQG7BKzZlE0AuzI3UDgE3+
UvZScFGuZV3me8RWsExaEqd/S+JUfUuSJKWlU6dzovlX4FvX9qvjbsPQd2NZHt93
Uik0MHAgcUmchDKeEbT9m8yKBgH7/P+1UvWnxd4mSThIoFdwXfX6xs1Io9m7jnoV
HwW3crqx1M6UPsKphayPHJlzy/uR+/ceMidPr9YvLWm3SLL2lS3oLAiXvj7+763i
fl+pN6OLTdknWfNfDwfXjJUWA2FduXbE/LMaxBA2yy+YNCDR8pNaOcO2eYkDg9Z5
v9b749VBunj4Gi5jEDAW1tyfAEsmCWPcwwZ+U96AnCzdhxkvCPcx9n5AKjIqMAOC
Ff1eUUIo8WMRULaMyMyzf8WjZBFkUpzk6LtwuwRO/5aaVnf+mrY6/gExH+gzxX+P
KHatSVIw5d02wvO+J9+EfDV65h0MAJX1TV02+BAJkNVGBKD/rYkoZzUbkegWJOcb
ObpD+0qOhF3PWb8+oB0llCvg7BAhdAiBxtvLIRWVGmRl
d0ycxMCsAn+Jb3RdMTRMD+SyoeGPNJEycVYyM2Jvyvs
9SXLZm1cQqmr4Yx327FNmJpwX4fTKIJ2oJMDpLPK74y
oslrRCb0SrbNIGcnFI7Q+hgCZkDhGb0Xe1PuHDFdDuzZ
h/FLPfkA1kAVyMZv0HFO+UxA+kmRD8wm5nhLY2HlVSu
8xU32oCKkFMq8euzimt9QwNTIbDq3m9RKYeg7ZsgqGz
H4YSgnTbPsKo0rbFQWJjsKmJ8t/bzdbkWRhHAhsfeFok
BjCKjnSzzHC4PJObqJHZ0mDOSWUgvcnAYH+iLWlikoc
QtfvCtOfac1v86W8tcpkPaw9NPqdYxlgSTsU2KNSvwYwh
6IfKLE2Y1oxL/klFXzqs7mYpUKy2t94HOKw1v8jtQyvgntD
/AUoi/r+ILIgxsD9mPpRZNBMN8Op0tADcYvn0c9+q1tkh+
K4rH9DEoxj26MUG8lbJbwaMlHN7LuX/HLQE2/MrfmZN/a
JBEzJjazCg2Nfqx2OMVS5WoBhkedhJyX7/4idkEyS+Wvl
1Xtyb12DX+7dbn2pNOP6cKOxweEcnX2FRw==
=oQHy
-----END PGP MESSAGE-----
```



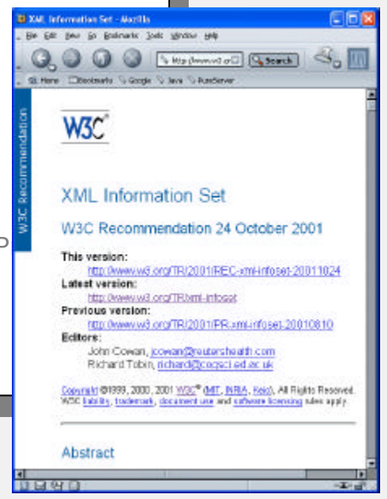
Besonderheiten



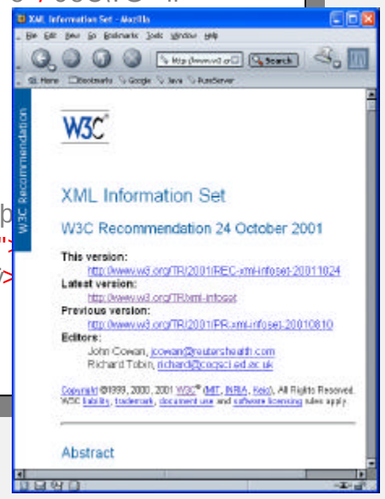
- Berücksichtigung der spezifischen Eigenschaften von XML
  - Grundfrage:
    Soll gesichertes XML noch XML sein?
    - Infoset-Struktursemantik

```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line>
      <Price currency="€">35264</P
      <Engine>220 CDI</Engine>
    </Vehicle>
  </Artikel>
</Bestellung>
```

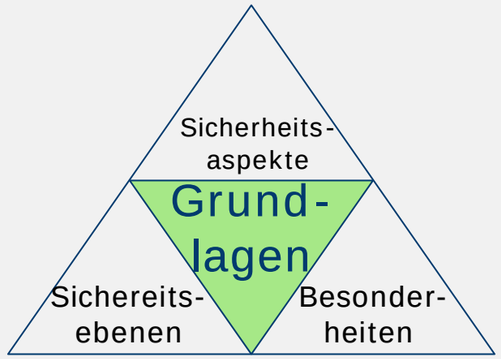
Sicherung →




```
<?xml version="1.0" encoding="UTF-8"?>
<n°]°Ú,z{¬»Ã+ î[- >
  <â)5ô  aÙoEÞ´-• ù , >
    <ü€t+f«}þ>
      <×R'r9…™4>Ý‡ot,Õìû</×R'r9…™4>
      <ƒÉ®µ½j9åP«C .•»   >Ý‡ot,Õìû</ƒÉ®µ½j9åP«C .•»   >
      <Ý‡ot,Õìû>a´ß]©Œ¥Ù½z´ nX»ý-</Ý‡ot,Õìû>
      <-9eÛ\?G  ïï>a¤q¨–ù›;  Övs"]  Xý~`è</-9eÛ\?G  ïï>
    </ü€t+f«}þ>
  </â)5ô  aÙoEÞ´-• ù , >
  <  š@´• ú     >
    <<&Õ[—ð2¨>
      <´90ž  ªŠ>ïÈ   -—Èw</´90ž  ªŠ>
      <ü€t+f«}þ>)ÑÖe J©   </ü€t+f«}þ>
      <4=¡1Ù¾™^>ñ¦ÉëY»ÒøÆ• {Õ#gÚþ
      <Àsª©,•Š À@·]à "  mM×ìB~•  ñ¡="€">
      <røûß˜rØÿ>w• ^D5ê>Éïï</røûß˜rØÿ>
    </<&Õ[—ð2¨>
  </  š@´• ú     >
</n°]°Ú,z{¬»Ã+ î[- >
```



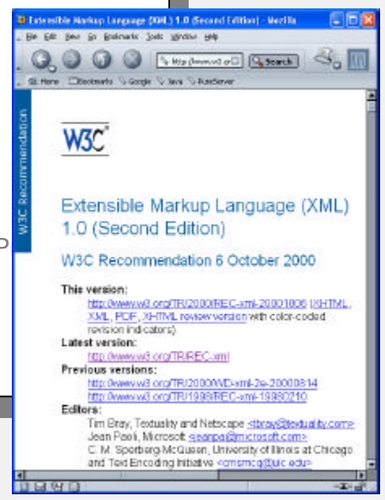
Besonderheiten



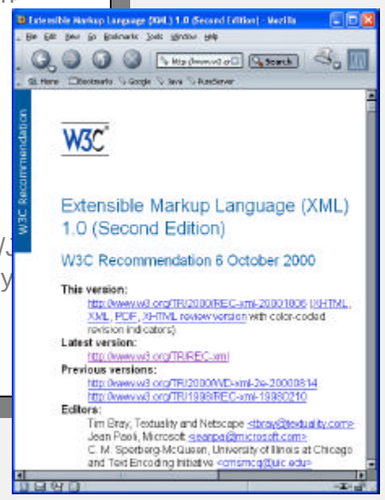
- Berücksichtigung der spezifischen Eigenschaften von XML
  - Grundfrage:
    Soll gesichertes XML noch XML sein?
    - Lexikalische XML-Struktur

```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line>
      <Price currency="€">35264</P
      <Engine>220 CDI</Engine>
    </Vehicle>
  </Artikel>
</Bestellung>
```

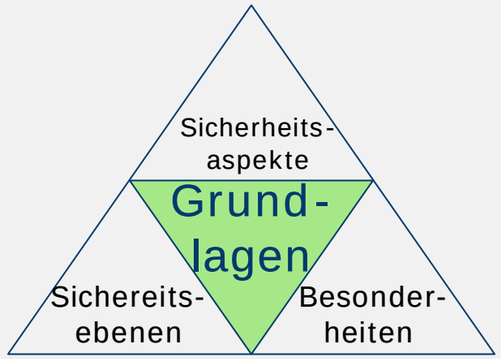
Sicherung →




```
<?xml version="1.0" encoding="UTF-8"?>
<Vymnyffoha>
  <Vymnyffyl>
    <Hugy>
      <Pilhugy>Gur</Pilhugy>
      <Huwbhugy>Gomnylguhh</Huwbhugy>
      <Mnlußy>Gomnylmnlußy__d_b</Mnlußy>
      <Iln>_a_b_c_d__Gomnylmnuxn</Iln>
    </Hugy>
  </Vymnyffyl>
  <Ulnceyf>
    <Pybcwfy>
      <Nsjy>Q_b_a_a</Nsjy>
      <Hugy>Y-Wfumm</Hugy>
      <Fchy>Upuhnaulxy</Fchy>
      <Jlcwy wollyhws="€">_c_e_b_f_d</J
      <Yhachy>_b_b__a__WXC</Yhachy
    </Pybcwfy>
  </Ulnceyf>
</Vymnyffoha>
```



Besonderheiten



- Berücksichtigung der spezifischen Eigenschaften von XML
  - Grundfrage:
    Soll gesichertes XML noch XML sein?
    – Struktur optional durch XML-Schema definiert

```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line
      <Price currency="€">352
      <Engine>220 CDI</Engi
    </Vehicle>
  </Artikel>
</Bestellung>
```

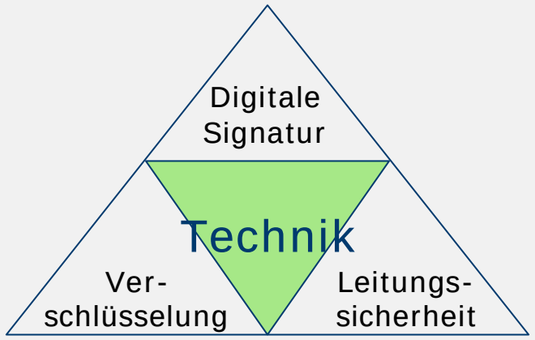
```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:complexType name="ArtikelType">
    <xs:sequence>
      <xs:element name="Vehicle" type="VehicleType"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="BestellerType">
    <xs:sequence>
      <xs:element name="Name" type="NameType"/>
    </xs:sequence>
  ...
```

Sicherung →

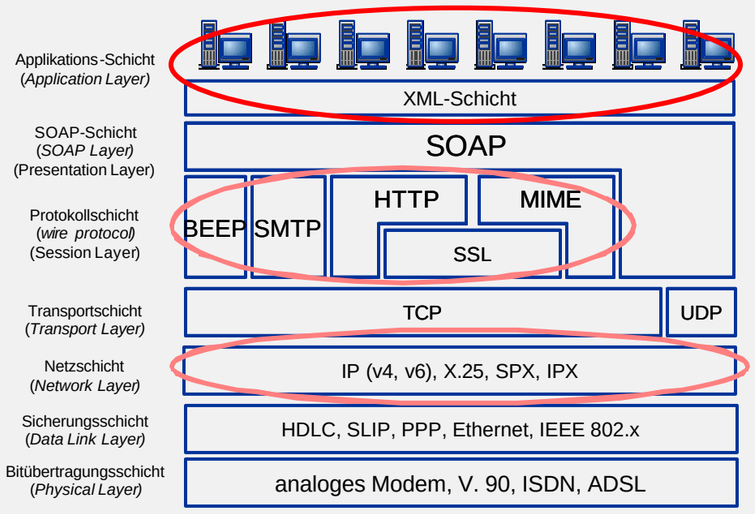
```
<?xml version="1.0" encoding="UTF-8"?>
<Vymnyffoha>
  <Vymnyffyl>
    <Hugy>
      <Pilhugy>Gur</Pilhugy>
      <Huwbhugy>Gomnylguhh</Huwbhugy>
      <Mnlußy>Gomnylmnlußy 68</Mnlußy>
      <Iln>98765 Gomnylmnuxn</Iln>
    </Hugy>
  </Vymnyffyl>
  <Ulnceyf>
    <Pybcwfy>
      <Nsjy>Q811</Nsjy>
      <Hugy>Y-Wfumm
      <Fchy>Upuhnaul
      <Jlcwy wollyhws=
      <Yhachy>880 WX
    </Pybcwfy>
  </Ulnceyf>
</Vymnyffoha>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:complexType name="ArtikelType">
    <xs:sequence>
      <xs:element name="Vehicle" type="VehicleType"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="BestellerType">
    <xs:sequence>
      <xs:element name="Name" type="NameType"/>
    </xs:sequence>
  ...
```

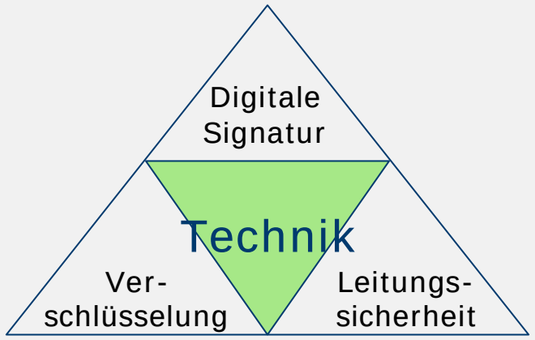
Techniken sicheren XMLs



- Prinzipiell sind Sicherungstechniken auf jeder Protokollschicht anwendbar …
- … jedoch nur Techniken der „XML-Schicht“ (=Anwendungsschicht) tragen den „XML-Besonderheiten“ Rechnung
  - *W3Cs XML Digital Signatures* zur Gewährleistung von
    - Verbindlichkeit
    - Berechtigung
    - Glaubwürdigkeit
    - (Daten-)Konsistenz
  - *W3Cs XML Encryption* fügt
    - Vertraulichkeit hinzu



Techniken sicheren XMLs: Digitale Signatur



Signatur

Einfache

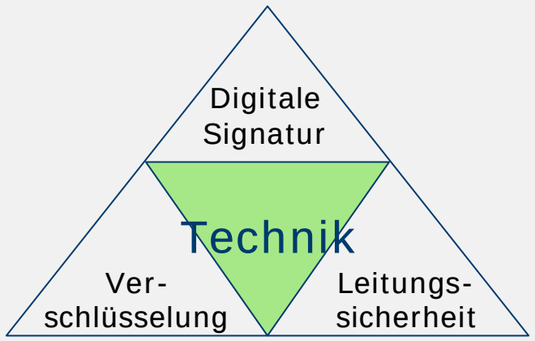
Elektronische

Fortgeschritte

Qualifizierte

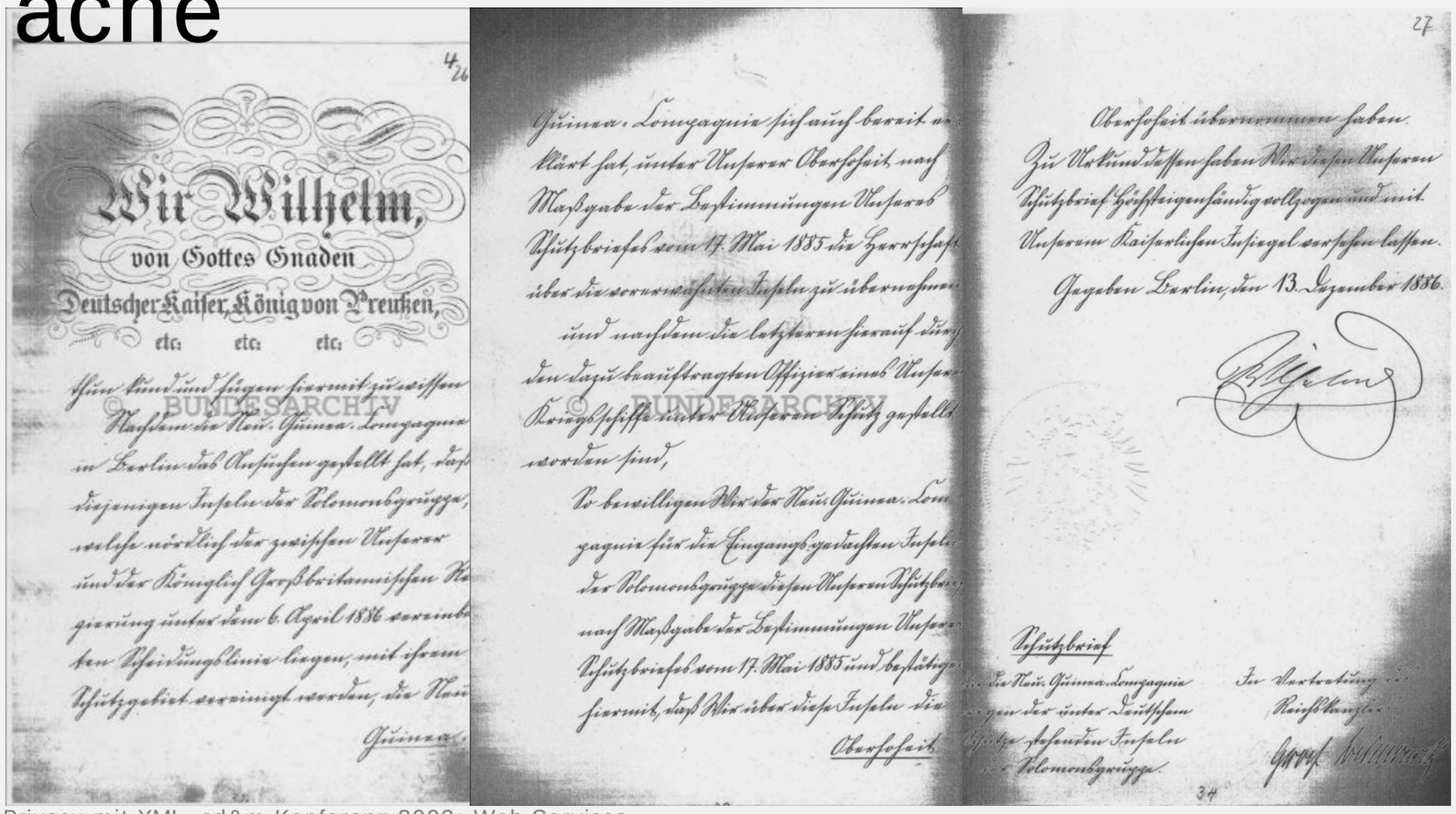
Akkreditierte

Techniken sicheren XMLs: Digitale Signatur



Signatur

Einfache



Wir Wilhelm,
von Gottes Gnaden
Deutscher Kaiser, König von Preußen,
etc. etc. etc.

thun kund und fügen hiermit zu wissen
Nachdem der Neu-Guinea-Compagnie
in Berlin das Ansuchen gestellt hat, daß
diejenigen Inseln der Salomonsgruppe,
welche nördlich der zwischen Unserer
und der Königlich Großbritannischen Re-
gierung unter dem 6. April 1886 vereinbar-
ten Abgrenzungslinie liegen, mit ihrem
Schutzgebiet vereinigt werden, die Neu-
Guinea-

Guinea-Compagnie sich auch bereit er-
klärt hat, unter Unserer Oberhoheit, nach
Maßgabe der Bestimmungen Unseres
Schutzbriefes vom 17. Mai 1885 die Herrschaft
über die vorerwähnten Inseln zu übernehmen
und nachdem die letzteren hierauf durch
den dazu beauftragten Offizier eines Unserer
Kriegsschiffe unter Unserem Schutz gestellt
worden sind,

So bewilligen Wir der Neu-Guinea-Com-
pagnie für die Eingeborenen Inseln
der Salomonsgruppe diesen Unseren Schutzbrief
nach Maßgabe der Bestimmungen Unseres
Schutzbriefes vom 17. Mai 1885 und bestätigen
hiermit, daß Wir über diese Inseln die
Oberhoheit

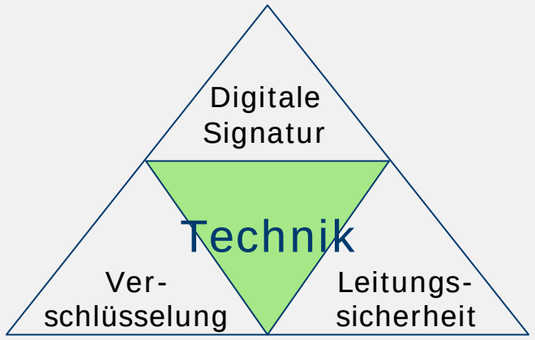
Oberhoheit übernommen haben.
Zu Urkund dessen haben Wir diesen Unseren
Schutzbrief höchsteigenhändig vollzogen und mit
Unserem Kaiserlichen Insiegel versehen lassen.
Gegeben Berlin, den 13. Dezember 1886.

Schutzbrief
für die Neu-Guinea-Compagnie
wegen der unter Deutschem
Schutze stehenden Inseln
der Salomonsgruppe

Im Vertretung des
Reichskanzlers
Graf v. Wilmowski

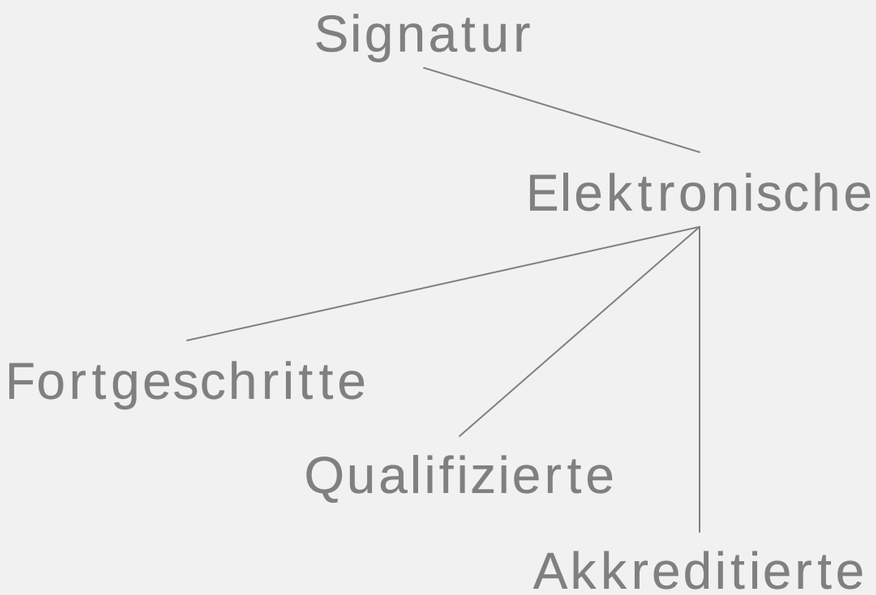
34

Techniken sicheren XMLs: Digitale Signatur

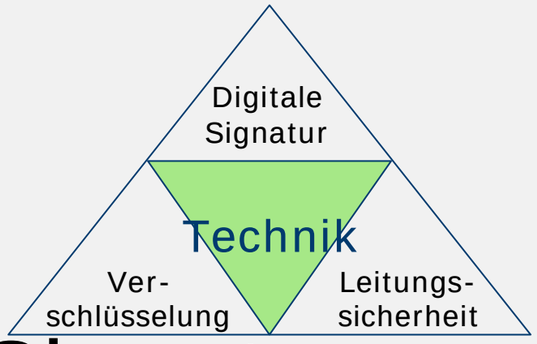


- Elektronische Signatur
  - § 2 Nr. 1 SigG
  - Keine Sicherheitsanforderungen
  - Beispiel:

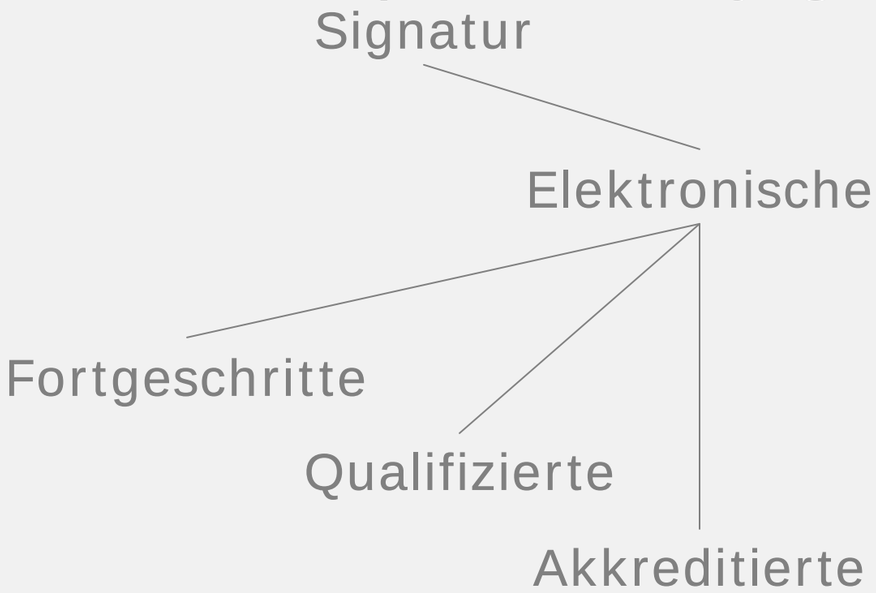
Max Mustermann



Techniken sicheren XMLs: Digitale Signatur

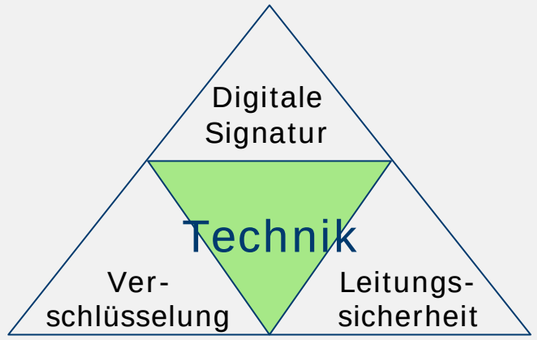


- Fortgeschrittene elektronische Signatur
  - § 2 Nr. 2 SigG
  - Ausschließliche Zuordnung an Unterzeichner
  - Identifizierung des Unterzeichners
  - Erzeugung unter alleiniger Kontrolle des Unterzeichners
  - Erkennbarkeit nachträglicher Veränderungen
  - Beispiel: Pretty good Privacy

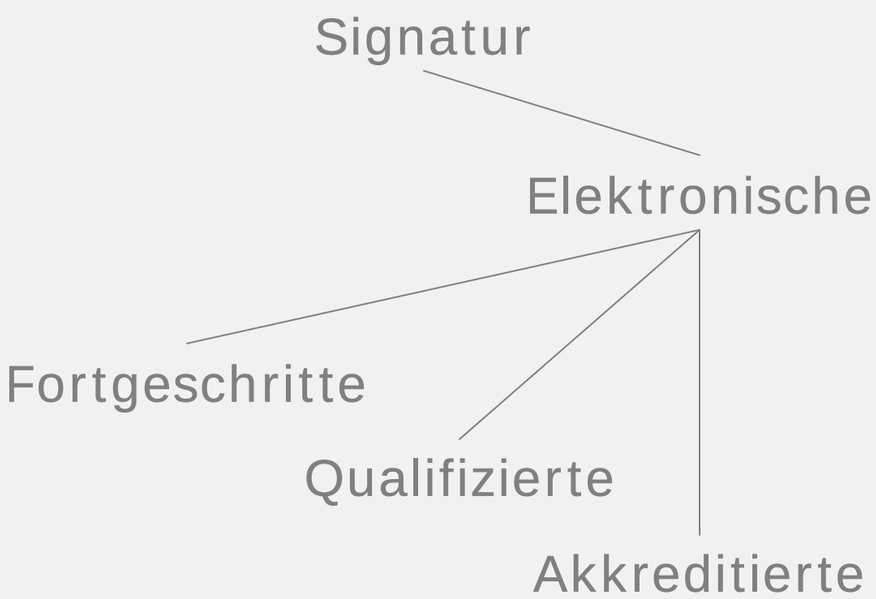


[Quelle: J. Bizer: „Rechtliche Anforderungen des elektronischen Signierens“]

Techniken sicheren XMLs: Digitale Signatur

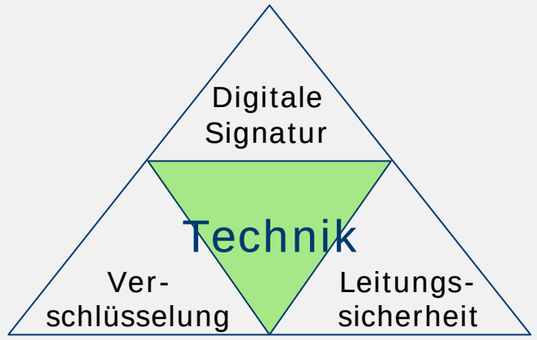


- Qualifizierte elektronische Signatur
  - § 2 Nr. 3 SigG
  - Beruhen auf gültigem qualifziertem Zertifikat
  - Inhaltliche Anforderungen an Zertifikat
  - Staatliche Aufsicht aber genehmigungsfrei
  - Haftung

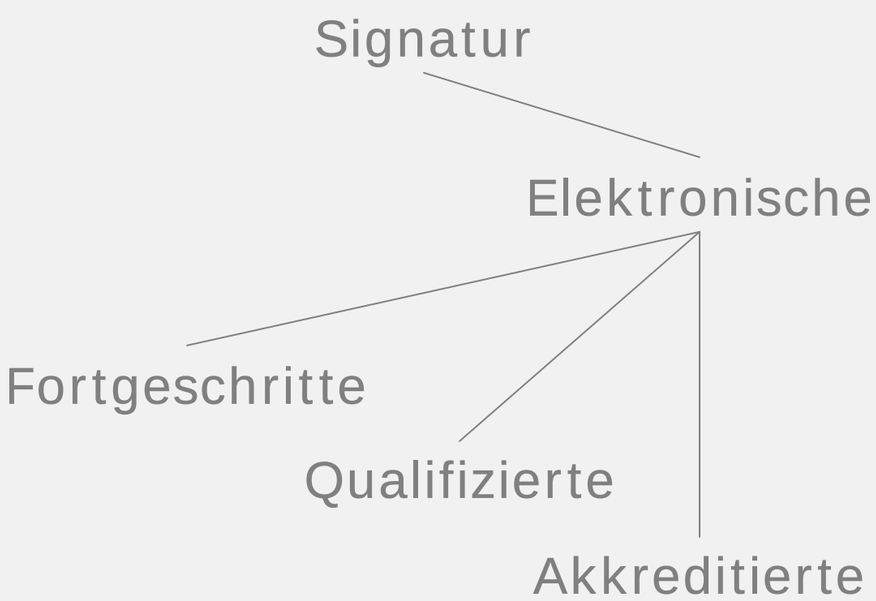


[Quelle: J. Bizer: „Rechtliche Anforderungen des elektronischen Signierens“]

Techniken sicheren XMLs: Digitale Signatur

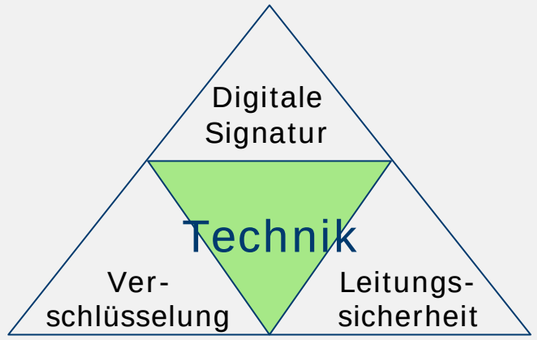


- Akkreditierte elektronische Signatur
  - § 15 SigG
  - Wie qualifizierte Signatur
  - Vorabprüfung durch Zertifizierungsdienstanbieter
  - Gesonderte Prüfung der technischen Komponenten
  - RegTP stellt Wurzelzertifikat aus
  - Beispiel: Signtrust



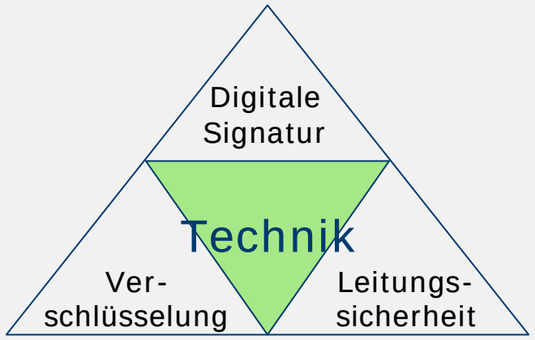
[Quelle: J. Bizer: „Rechtliche Anforderungen des elektronischen Signierens“]

Techniken sicheren XMLs: Digitale Signatur



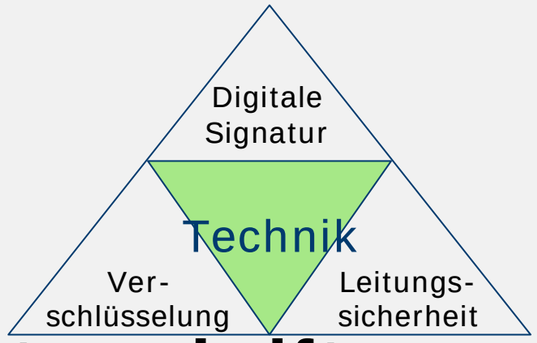
- Ziele:
  - Aufdeckung potentieller Datenverfälschung
  - Unbestreitbare Autorenschaft
  - Rechtliche Verbindlichkeit
- Ablauf:
  - Sender „unterschreibt“ zu übertragende Daten
  - Übertragung von Daten und Unterschrift
  - Empfänger prüft Unterschrift

Techniken sicheren XMLs: Digitale Signatur




```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line>
      <Price currency="€">35264</Price>
      <Engine>220 CDI</Engine>
    </Vehicle>
  </Artikel>
</Bestellung>
```

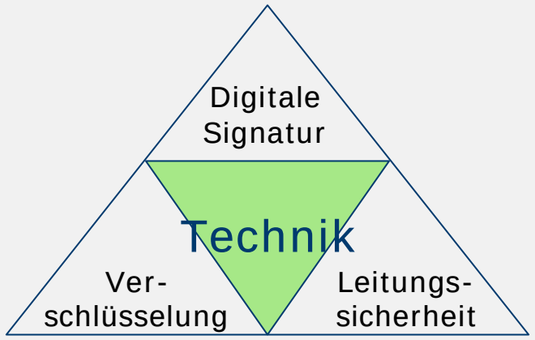
Techniken sicheren XMLs: Digitale Signatur



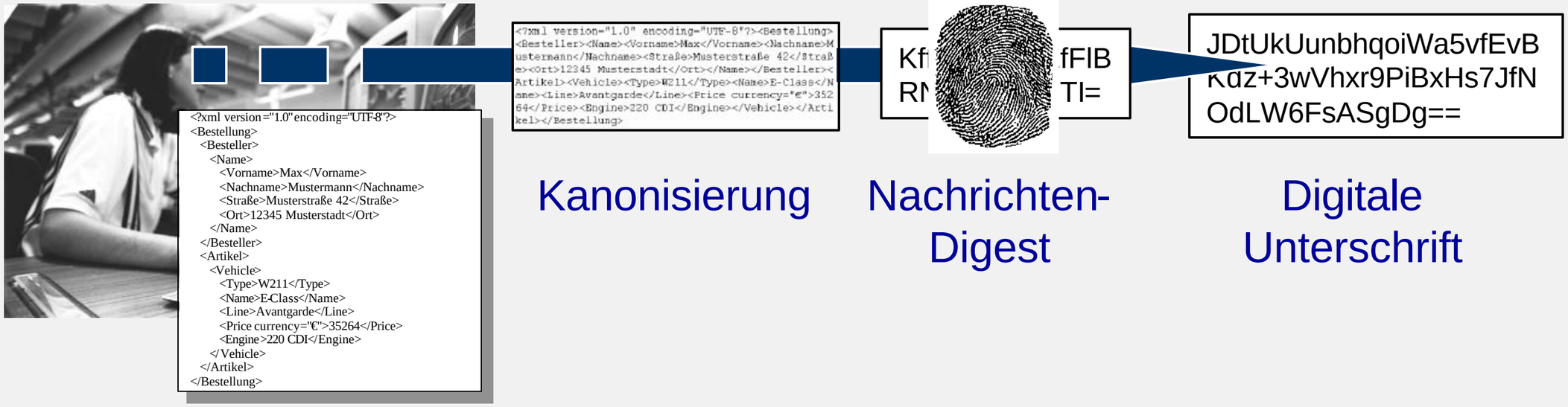
Technische Eigenschaften der digitalen Unterschrift

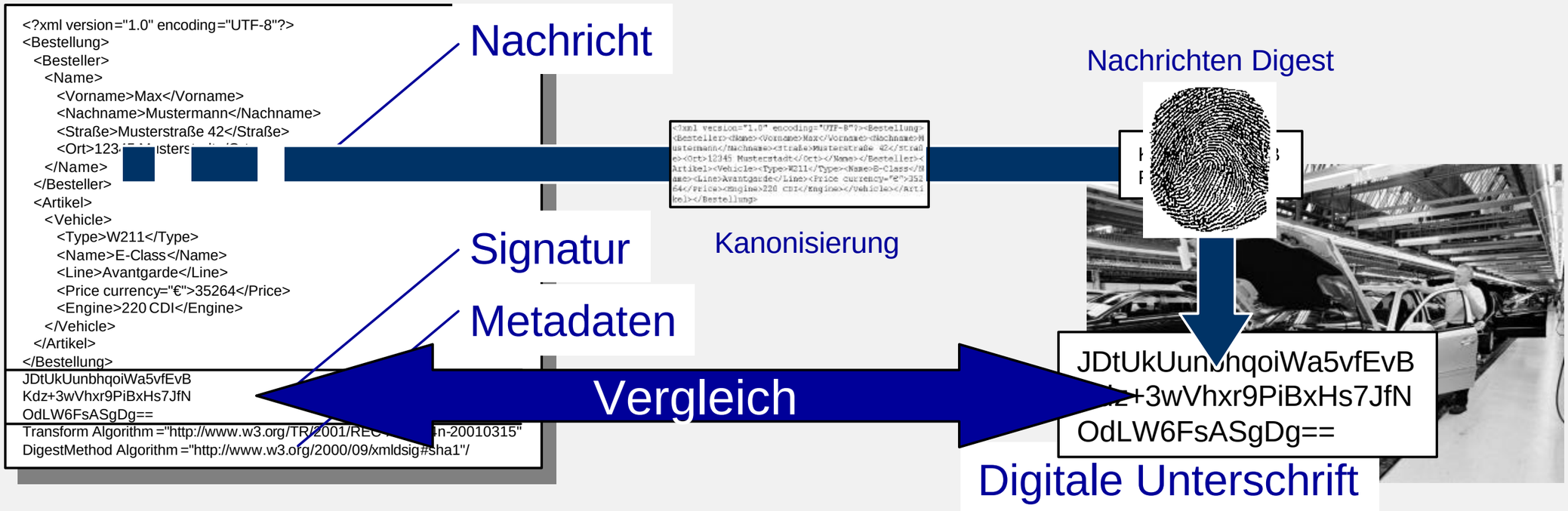
- Glaubwürdigkeit (willentliche Unterschrift)
- Fälschungssicherheit
  (Unterschrift kann nicht durch Dritte erzeugt werden)
- Transienz (Unterschrift ist nicht wiederverwendbar)
- Unveränderbarkeit
  (Unterschrift und Dokument bilden Einheit)
- Dauerhaftigkeit
  (Unterschrift kann nicht zurückgezogen werden)

Techniken sicheren XMLs: Digitale Signatur

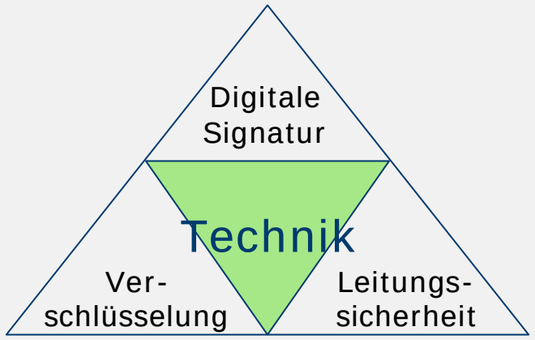


Technische Realisierung der digitalen Unterschrift





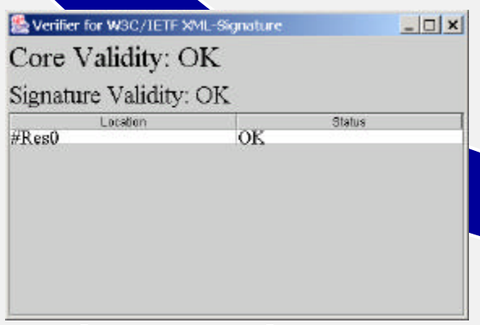
Techniken sicheren XMLs: Digitale Signatur

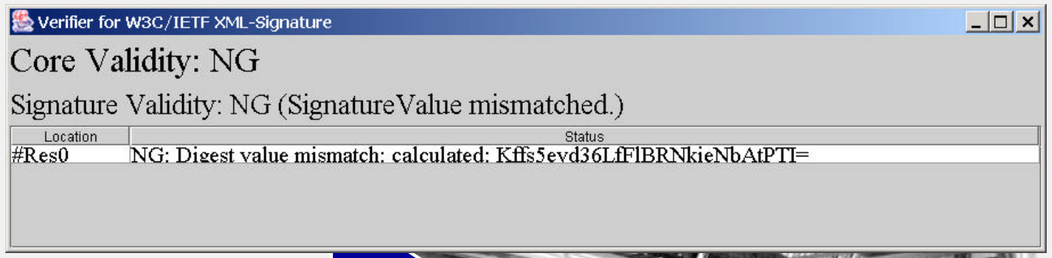


Aufdeckung nachträglicher Modifikationen

- Modifikationen an
  - Nutzdaten
  - Unterschrift
  - Metadaten
  - ...

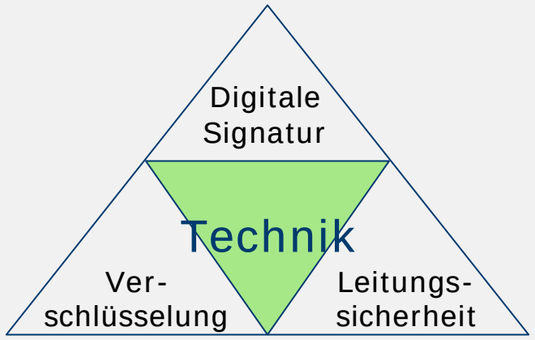
... können erkannt werden





Dokument trifft unverändert ein:

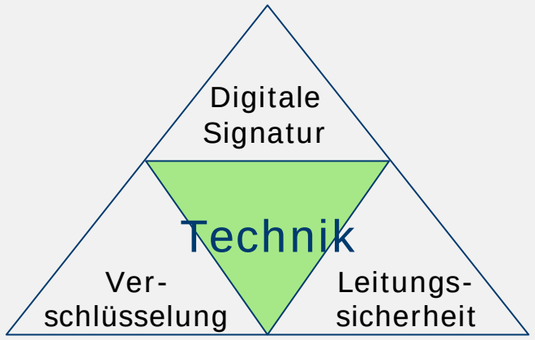
Techniken sicheren XMLs: Digitale Signatur



Zusammenfassung

- Erreichung des gesteckten Ziels: Aufdeckung potentieller Datenverfälschungen
- Keine Veränderung des Nutzdateninhaltes (Insbesondere bleiben sie lesbar!)
- Mathematisch erzeugter Nachrichten-Digest ist Grundlage des Signaturvorganges
- Gemeinsame Übertragung von Dokument, beschreibenden Metadaten und Signatur
- Durch bestehende Umsetzungen (teilweise sogar als Open-Source verfügbar) leicht in existierende XML-Lösungen integrierbar

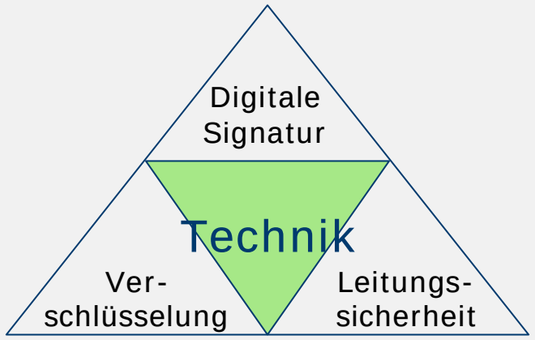
Techniken sicheren XMLs: Digitale Signatur



Erfahrungen und Einsatzempfehlungen

- Digitale Signatur kann eingesetzt werden zur Realisierung von ...
  - Berechtigung
  - Glaubwürdigkeit des Ursprungs
  - Verbindlichkeit
  - (Daten-)Konsistenz
- Einsatzfälle ...
  - Sicherung der Urheberschaft bei nicht-vertraulichen Inhalten (B2B-Anwendungen)
  - Sicherstellung der Unveränderbarkeit (RPCs, Business Transaktionen)
- Relevante Standards:
  - XML Digital Signatures (W3C Recommendation/IETF RFC 3072 seit 2002-02-12)
  - Web Service-Security (OASIS)

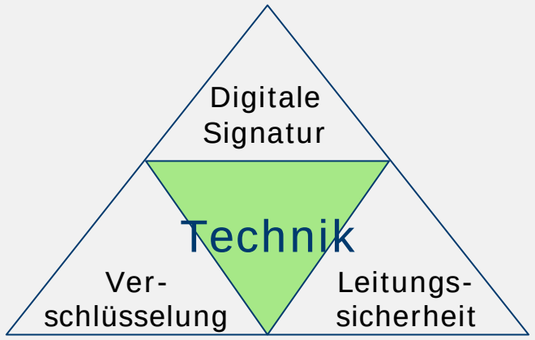
Techniken sicheren XMLs: Digitale Signatur



Gesetzliche Randbedingungen

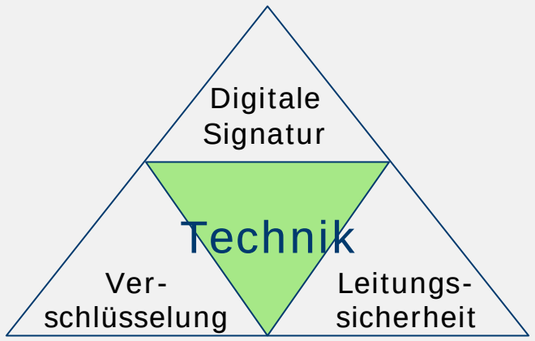
- Signaturgesetz vom 2001-05-16
- Signaturverordnung vom 2001-11-16
- EU-Signaturrichtlinie 1999/93/EG
- §§ 415 ff Zivilprozeßordnung (ZPO): Von eigener Hand unterschriebene Dokumente gelten als Urkunde.
  Elektronisch signierte Daten werden diesen gleichgestellt.

Techniken sicheren XMLs: Verschlüsselung



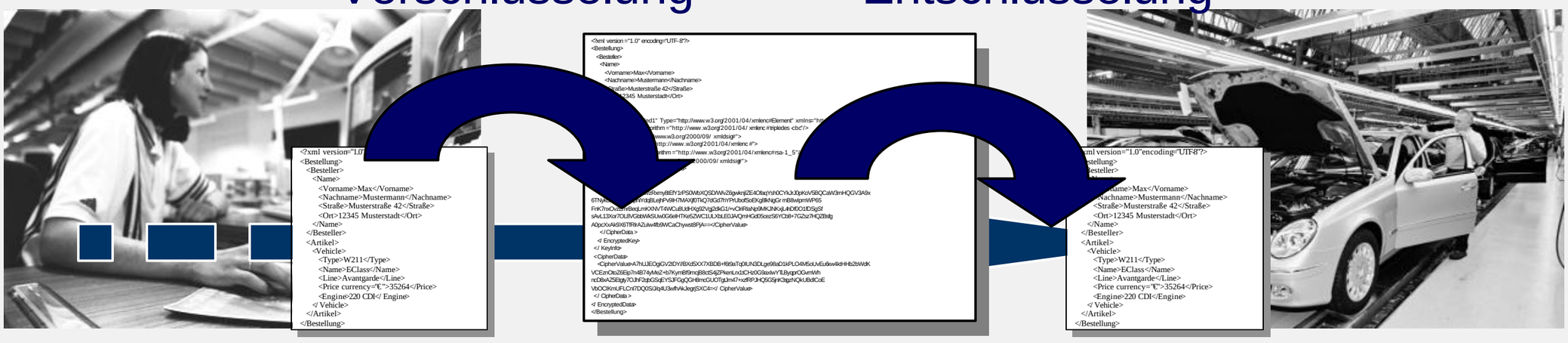

```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <Artikel>
    <Vehicle>
      <Type>W211</Type>
      <Name>E-Class</Name>
      <Line>Avantgarde</Line>
      <Price currency="€">35264</Price>
      <Engine>220 CDI</Engine>
    </Vehicle>
  </Artikel>
</Bestellung>
```

Techniken sicheren XMLs: Verschlüsselung

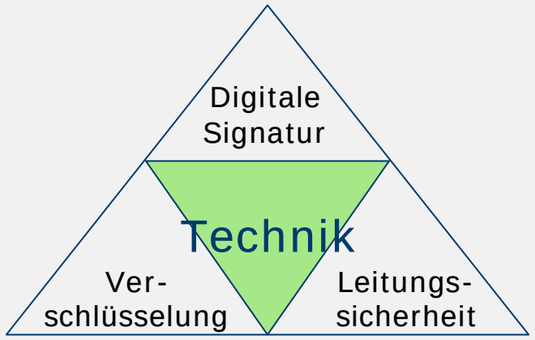


- Ziel:
  - Vertraulichkeitsschutz
- Ablauf:
  - Sender bearbeitet zu übertragende Daten so, daß sie ausschließlich für den intendierten Adressaten lesbar sind
  - Übertragung der so chiffrierten Daten
  - Empfänger entschlüsselt Daten

Verschlüsselung Entschlüsselung

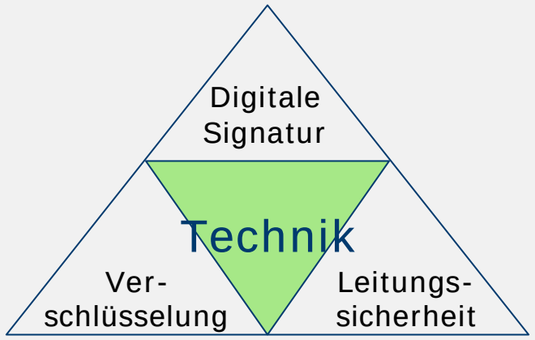


Techniken sicheren XMLs: Verschlüsselung




```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <EncryptedData Id="ed1" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>mjecklee</KeyName>
   </KeyInfo>
   <CipherData>
    <CipherValue>JRIvzRxmy8tEfY1rPS0WbXQSD/W/vZ6gwknjIZE4OfaqYsh0CYkJrJ0pKoV5BQCaW3rnHQGV3A9x
6TNyk0B4wTXN3phiYdqBLejhPv9IH7MAXjf0TkQ7dGd7hYPrUbofSoEKg8lkNgGrrnB8wIpmWP65
FnK7nxOvzLmrBeqLmKXNVT4WCu8UdHXg92Vgj2dkG1/+vClriRIaNp9MKJNKxjL4nDf0O1fDSgSf
sAvL13Xor7OL8VGbbWkSUw0G6eIHTKe5ZWC1ULXbLE0JA/QmHGd05cezS6YCb8+7GZsz7HQZBsfg
A0pcXxAk9X6TfRlrAZuIw4fb9WCaChywst8PjA==</CipherValue>
    </CipherData>
  </EncryptedKey>
 </KeyInfo>
 <CipherData>
  <CipherValue>A7hUJEOgiGV2IDY//BXd5XX7XBDB+f6t9aTq0IUN3DLge98aD1kPLO4M5oUvEu6xw4ktHHb2bWdK
VCEznOtoZ6Eip7n4B74yMeZ+b7KymBf9mcjB8ctS4jZPkenLrx1tCHz0G9axIwYTLByqprOGvmWh
ncD8xAZ5Etgty7OJhF2qbGSqEYSJFGgQGH8mcGUOTgtJm47+xzfRPJHQ5G5jnK3sgzNQkUBdlCoE
VbOCIKmUFLCnI7DQ0S/J/q4U3wfhAkJegrjSXC4=</CipherValue>
 </CipherData>
</EncryptedData>
</Bestellung>
```

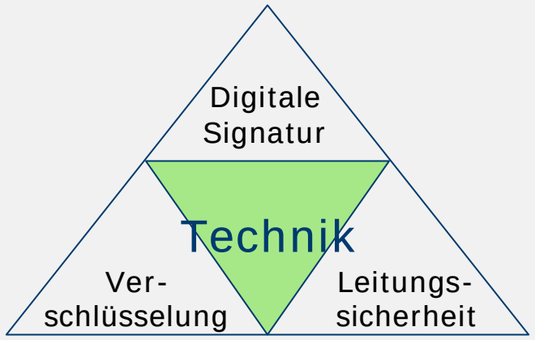
Techniken sicheren XMLs: Verschlüsselung




```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nac
      <Straße>Musterstraße 42</St
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <EncryptedData Id="ed1" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>mjecklee</KeyName>
   </KeyInfo>
   <CipherData>
    <CipherValue>JRIvzRxmy8tEfY1rPS0WbXQSD/W/vZ6gwknjIZE4OfaqYsh0CYkJrJ0pKoV5BQCaW3rnHQGV3A9x
6TNyk0B4wTXN3phiYdqBLejhPv9IH7MAXjf0TkQ7dGd7hYPrUbofSoEKg8lkNgGrrnB8wIpmWP65
FnK7nxOvzLmrBeqLmKXNVT4WCu8UdHXg92Vgj2dkG1/+vClriRIaNp9MKJNKxjL4nDf0O1fDSgSf
sAvL13Xor7OL8VGbbWkSUw0G6eIHTKe5ZWC1ULXbLE0JA/QmHGd05cezS6YCb8+7GZsz7HQZBsfg
A0pcXxAk9X6TfRlrAZuIw4fb9WCaChywst8PjA==</CipherValue>
    </CipherData>
   </EncryptedKey>
 </KeyInfo>
 <CipherData>
  <CipherValue>A7hUJEOgiGV2IDY//BXd5XX7XBDB+f6t9aTq0IUN3DLge98aD1kPLO4M5oUvEu6xw4ktHHb2bWdK
VCEznOtoZ6Eip7n4B74yMeZ+b7KymBf9mcjB8ctS4jZPkenLrx1tCHz0G9axIwYTLByqprOGvmWh
ncD8xAZ5Etgty7OJhF2qbGSqEYSJFGgQGH8mcGUOTgtJm47+xzfRPJHQ5G5jnK3sgzNQkUBdlCoE
VbOCIKmUFLCnI7DQ0S/J/q4U3wfhAkJegrjSXC4=</CipherValue>
 </CipherData>
</EncryptedData>
</Bestellung>
```


Unchiffrierte Übertragung nicht-sensibler Inhalte

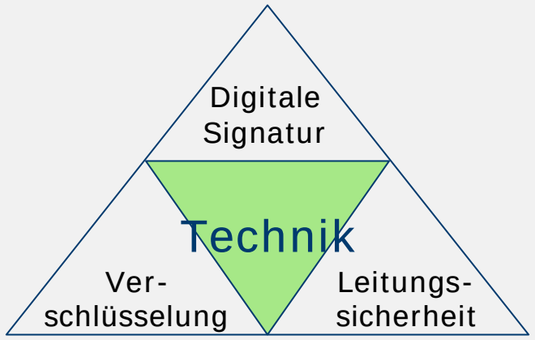
Techniken sicheren XMLs: Verschlüsselung




```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <EncryptedData Id="ed1" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>mjecklee</KeyName>
   </KeyInfo>
   <CipherData>
    <CipherValue>JRIvzRxmy8tEfY1rPS0WbXQSD/W/vZ6gwknjIZE4OfaqYsh0CYkJrJ0pK
6TNyk0B4wTXN3phiYdqBLejhPv9
FnK7nxOvzLmrBeqLmKXNV
sAvL13Xor7OL8VGbbWkSUw0G6eIHTKe5Z
C1ULXbLE0JA/QmHGd05cezS6YCb8+7GZs
A0pcXxAk9X6TfRlrAZuIw4fb9WCaChywst8PjA==</CipherValue>
   </CipherData>
  </EncryptedKey>
 </KeyInfo>
 <CipherData>
  <CipherValue>A7hUJEOgiGV2IDY//BXd5XX7XBDB+f6t9aTq0IUN3DLge98aD1kPLO4M5oUvEu6xw4ktHHb2bWdK
VCEznOtoZ6Eip7n4B74yMeZ+b7KymBf9mcjB8ctS4jZPkenLrx1tCHz0G9axIwYTLByqprOGvmWh
ncD8xAZ5Etgty7OJhF2qbGSqEYSJFGgQGH8mcGUOTgtJm47+xzfRPJHQ5G5jnK3sgzNQkUBdlCoE
VbOCIKmUFLCnI7DQ0S/J/q4U3wfhAkJegrjSXC4=</CipherValue>
 </CipherData>
</EncryptedData>
</Bestellung>
```

Metainformation

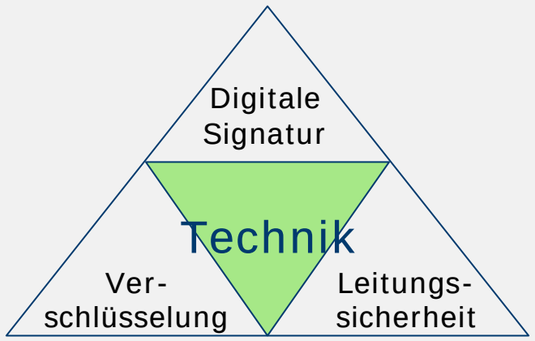
Techniken sicheren XMLs: Verschlüsselung




```
<?xml version="1.0" encoding="UTF-8"?>
<Bestellung>
  <Besteller>
    <Name>
      <Vorname>Max</Vorname>
      <Nachname>Mustermann</Nachname>
      <Straße>Musterstraße 42</Straße>
      <Ort>12345 Musterstadt</Ort>
    </Name>
  </Besteller>
  <EncryptedData Id="ed1" Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
   <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
    <KeyName>mjecklee</KeyName>
   </KeyInfo>
   <CipherData>
    <CipherValue>JRIvzRxmy8tEfY1rPS0WbXQSD/W/vZ6gwknjIZE4OfaqYsh0CYkJrJ0pKoV5BQCaW3rnHQGV3A9x
6TNyk0B4wTXN3phiYdqBLejhPv9IH7MAXjf0TkQ7dGd7hYPrUbofSoEKg8lkNgGrrnB8wIpmWP65
FnK7nxOvzLmrBeqLmKXNVT4WCu8UdHXg92Vgj2dkG1/+vClriRIaNp9MKJNKxjL4nDf0O1fDSgSf
sAvL13Xor7OL8VGbbWkSUw0G6eIHTKe5ZWC1ULXbLE0JA/QmHGd05cezS6YCb8+7GZsz7HQZBsfg
A0pcXxAk9X6TfRlrAZuIw4fb9WCaChywst8PjA==</CipherValue>
    </CipherData>
   </EncryptedKey>
 </KeyInfo>
 <CipherData>
  <CipherValue>A7hUJEOgiGV2IDY//BXd5XX7XBDB+f6t9aTq0IUN3DLge98aD1kPLO4M5oUvEu6xw4ktHHb2b
VCEznOtoZ6Eip7n4B74yMeZ+b7KymBf9mcjB8ctS4jZPken
ncD8xAZ5Etgty7OJhF2qbGSqEYSJFGgQGH8mcGUOTgtJm4
VbOCIKmUFLCnI7DQ0S/J/q4U3wfhAkJegrjSXC4=</CipherValue>
 </CipherData>
</EncryptedData>
</Bestellung>
```


Verschlüsselte Nutzdaten

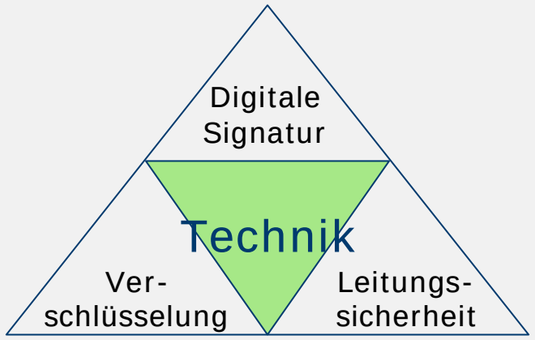
Techniken sicheren XMLs: Verschlüsselung



Zusammenfassung

- Erreichung des gesteckten Ziels: Schutz der Vertraulichkeit
- Kryptographische Veränderung des Nutzdateninhaltes (Bedarfsgesteuerte Anwendung möglich)
- Übertragung von verschlüsseltem Dokument und beschreibenden Metadaten
- Durch bestehende Umsetzungen (teilweise sogar als Open-Source verfügbar) leicht in existierende XML-Lösungen integrierbar

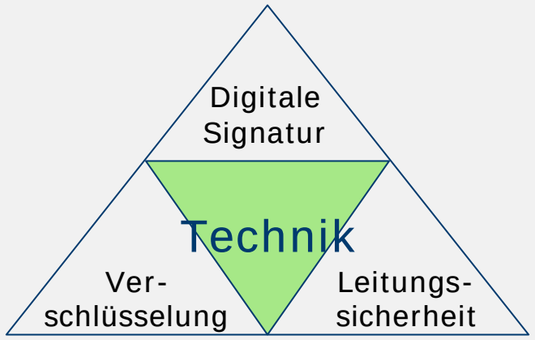
Techniken sicheren XMLs: Verschlüsselung



Erfahrungen und Einsatzempfehlungen

- Verschlüsselung kann zum Schutz der Vertraulichkeit bei der Übertragung sensibler Daten eingesetzt werden
- Einsatzfälle ...
  - Transfer sensibler Daten aller Art (z.B. Finanzdaten, Personaldaten, Gesundheits-bezogene Daten ...)
- Relevante Standards:
  - XML Encryption Syntax and Processing (W3C Recommendation seit 2002-12-10)
  - Web Service-Security (OASIS)

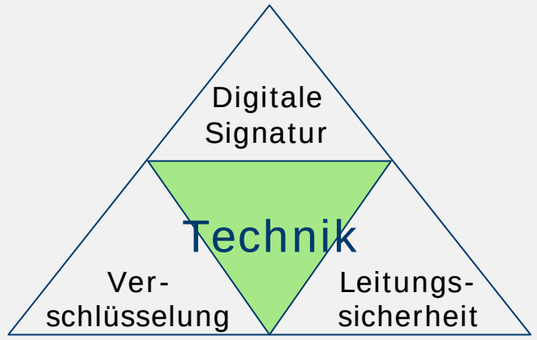
Techniken sicheren XMLs: Zusammenfassung

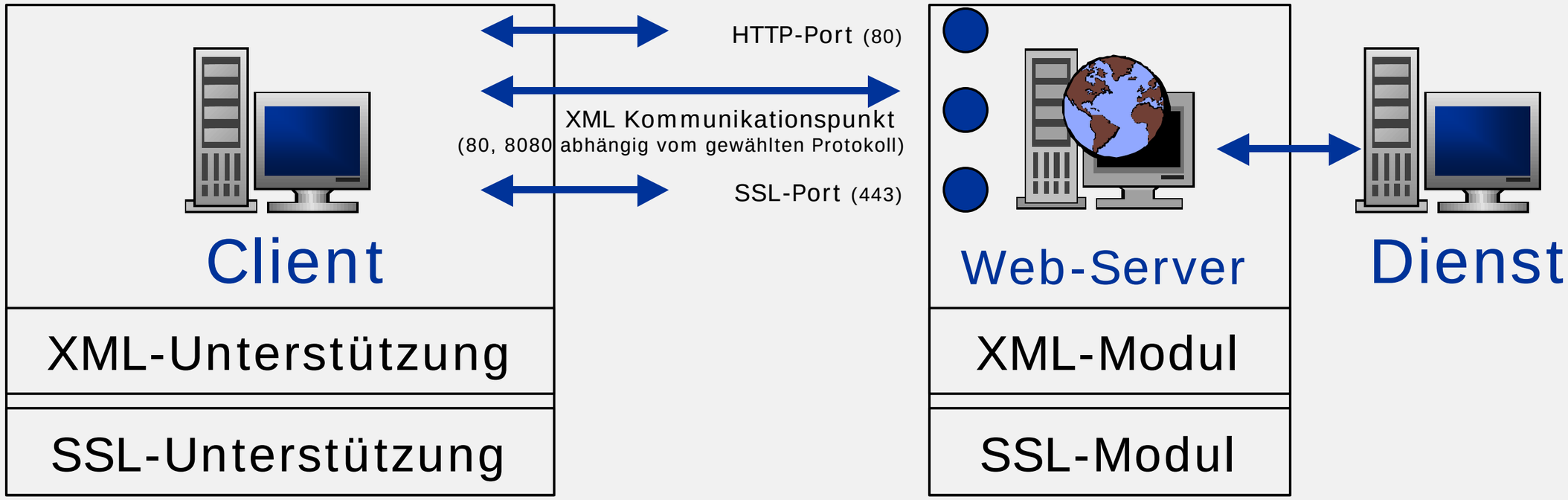


Technische Umsetzungen

- operieren ausschließlich auf der Applikationsebene und sind daher netzwerkseitig transparent
- bilden ein Rahmenwerk
- sind um Algorithmen erweiterbar
- sind interoperabel (Signatur nach Verschlüsselung möglich und getestet)
- XML Encryption gestatten auch super-encryption (d.h. Verschlüsselung bereits verschlüsselter Inhalte)
- lassen Infrastruktur (z.B. PKI RFC 2459) außer Acht

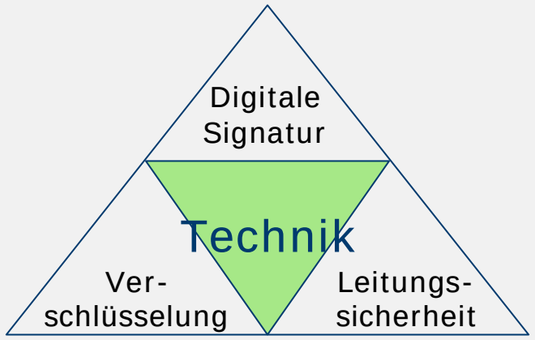
Techniken sicheren XMLs: Leitungssicherheit





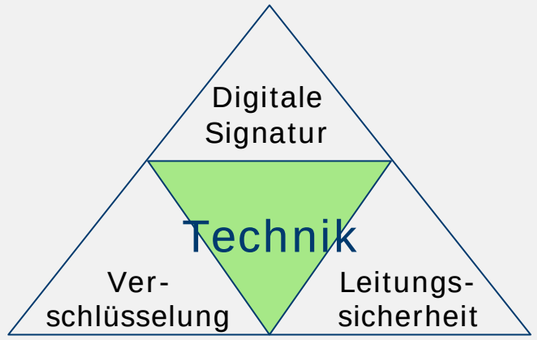
- Ziel:
  - Realisierung applikationstransparenter Sicherheit
- Voraussetzungen:
  - XML-Unterstützung (Client- und Server-seitig)
  - Freischaltung SSL-Port der Firewall
  - SSL-Unterstützung (Client- und Server-seitig)

Techniken sicheren XMLs: Leitungssicherheit

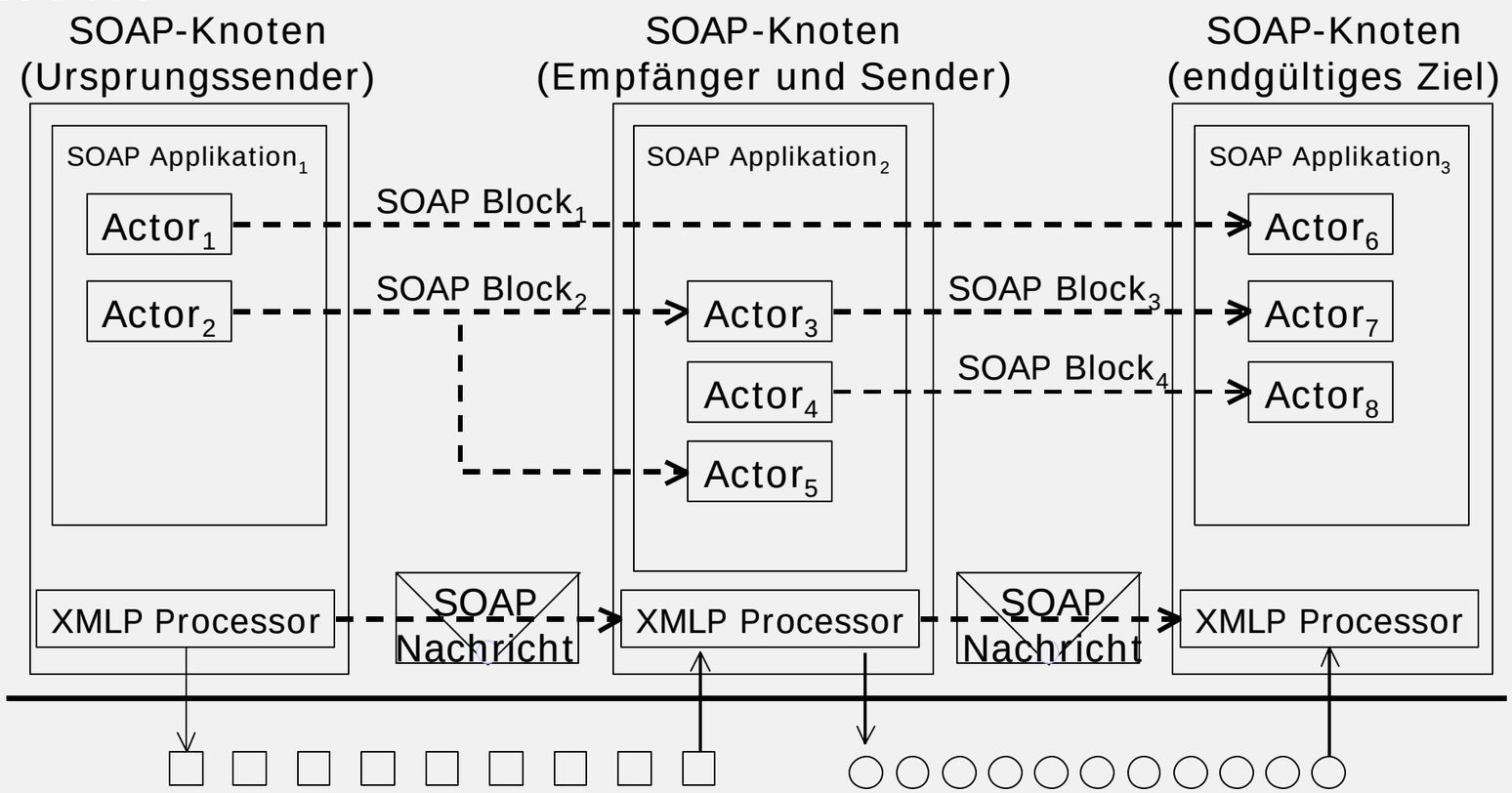


- Client-seitige Ablage der empfangenen Zertifikate im Unternehmensumfeld kaum effizient und sicher handhabbar.
  - Wer akzeptiert Zertifikate?
  - Auf wen wirkt sich diese Akzeptanz aus?
  - SSL ist inhärent für längerfristige Kommunikations-beziehungen konzipiert

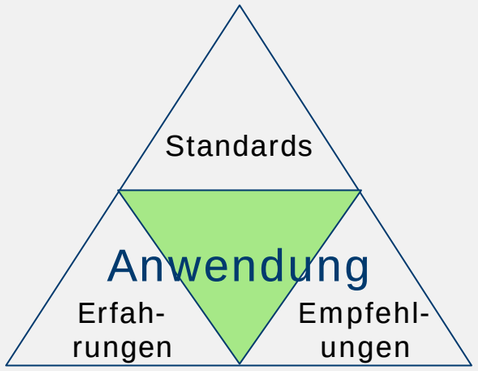
Techniken sicheren XMLs: Leitungssicherheit



- SSL/TLS für Ende-zu-Ende-Sicherung nicht einsetzbar, wenn aktive SOAP-Zwischenknoten (*SOAP Intermediäre)* benutzt werden sollen.

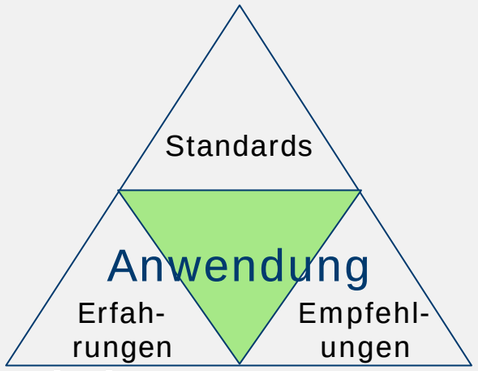


Standards



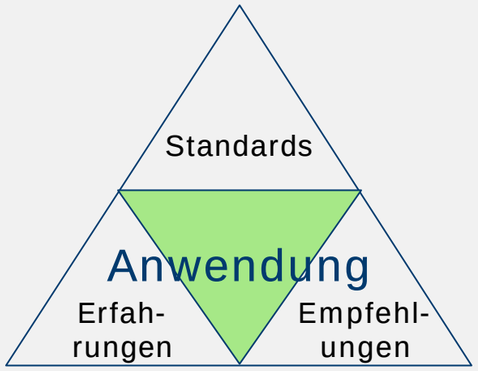
- W3C-Basisstandards
  - *XML Encryption Syntax and Processing* (W3C Recommendation seit 2002-12-10)
  - *XML Digital Signatures* (W3C Recommendation/ IETF RFC 3072 seit 2002-02-12)
  - *XML Key Management* (XKMS) Zugriffsprotokoll auf Schlüsselverwaltungsdienst
- OASIS-Anwendungsstandards
  - *Web Service-Security* Umfaßt Anwendungsprofil für XML Digital Signatures und XML Encryption
  - *Extensible Access Control Markup Language* (XACML) Richtlinien (*policies*) für den Datenzugriff
  - *Security Assertions Markup Language* (SAML) Darstellung und Austausch von Authentisierungsdaten.

Erfahrungen



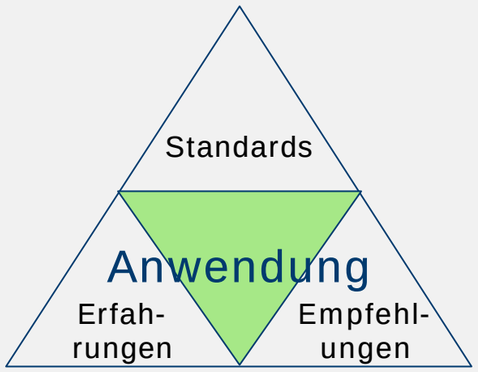
- SOAP-Toolkit unterstütz(t)en XML-Signaturen nicht (vollständig)
  - Manuelle Codemodifikationen notwendig zur korrekten Unterstützung von XML DSig. (Serialisierungsproblem für XML-Attribute eines Wurzelelements).
  - Race condition in AXIS Client Bibliothek. (Exceptions auf Mehrprozessormaschinen).
  - Unterschiedliche Interpretationen der gegenwärtig verfügbaren SOAP-Spezifikation.
- Transportsicherung (SSL/TLS) kaum sinnvoll
- XSS4J kaum praktisch einsetzbar.
  IBM favorisiert inzwischen *Web Service Toolkit* als Nachfolgelösung.
- API-Instabilität in .NET
- Interoperabilitätsprobleme Java -- .NET
- Anwenderakzeptanz und -toleranz

Erfahrungen



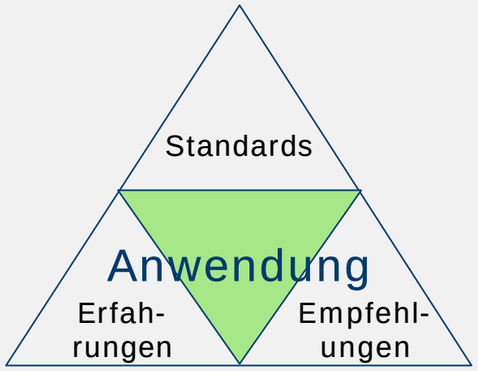
- Sicherheit ist ein soziotechnisches Problem.
- Sicherheit wird gefordert und ihr Vorhandensein generell begrüßt.
- Realisierte Lösung erfordert Identifikation durch tastaturbasierte Paßworteingabe.
- Manuelle Authentisierung und Autorisierung jedes entfernten Funktionsaufrufs nicht praktikabel.
- Sinnvollerweise Kopplung an Systemlogin (*single-sign-on*).

Empfehlungen



- Schulung und Sensibilisierung der Stakeholder.
- Bereitstellung der notwendigen Applikationsschnittstellen
- Identifikation der organisatorischen Ansatzpunkte
  (Bereiche, Prozesse, Datenflüsse)
- Festlegung des notwendigen Sicherheitsgrades
- Auswahl geeigneter Verfahren für Signatur und Verschlüsselung
- Prozeßimplementierung
  Schlüssel- und Zertifikatsverwaltung
- Faustregel: Mindestens fortgeschrittene elektronische Signatur – Notwendigkeit von Verschlüsselung prüfen.

Empfehlungen



- Gleichzeitige Realisierung von Sicherheitsmechanismen auf verschiedenen Kommunikationsschichten ist kein Widerspruch
- SSL zwar weit verbreitet aber inadäquat für serviceorientierte Verarbeitung bzw. in der technischen Realisierung zuweilen lückenhaft => Einsatz von TLS und/oder S-HTTP
- Sollte Existenz der Kommunikation bereits ein sicherheitsrelevantes Datum darstellen => Einsatz von Netzsicherheitsmaßnahmen wie IPSec oder VPN