

# Die Internet-Standards der Zukunft

Internet-Expo 2000

7. Februar 2000

Andreas Göldi (Andreas.Goeldi@delta-consulting.com)  
Jürg Stuker (Juerg.Stuker@delta-consulting.com)

Frankfurt, Genf, Konstanz, Lausanne, St.Gallen, Zug, Zürich

# 10 Standards für das Internet der (nahen) Zukunft



- » 10 Standards aus allen Technologiebereichen
- » ...von der Netzinfrastruktur bis zur clientseitigen Multimedia-Technologie...
- » ...einige schon etablierter, andere erst hoffnungsvolle Kandidaten



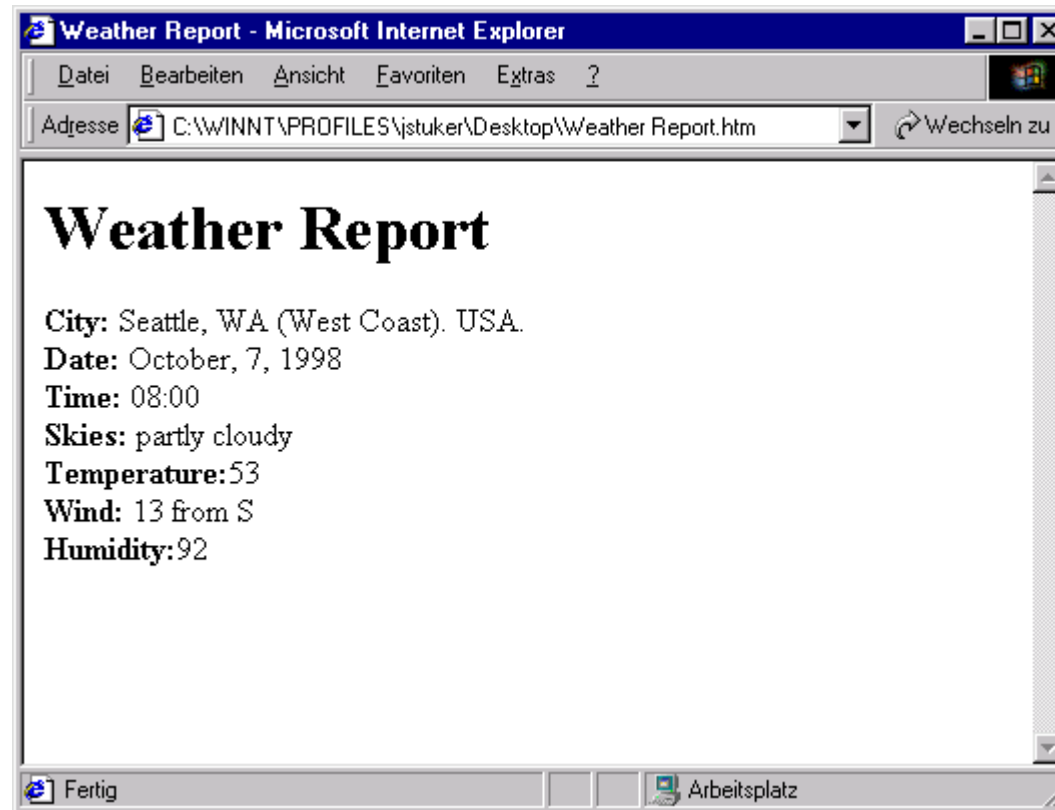
# XML (eXtensible Markup Language)



- » Methode strukturierte Daten in Text-Datei zu speichern, zu transportieren, zu...
- » Gute lesbar, sprechend, keine vordefinierten Tags
- » Subset von SGML
- » Lizenzfrei, technologieneutral
- » Grundlage für ein Familie von Technologien



```
<HTML>
  <HEAD>
    <TITLE>Weather Report</TITLE>
  </HEAD>
  <BODY>
    <H1>Weather Report</H1>
    <B>City:</B> Seattle, WA (West Coast). USA.<BR>
    <B>Date:</B> October, 7, 1998 <BR>
    <B>Time:</B> 08:00 <BR>
    <B>Skies:</B> partly cloudy<BR>
    <B>Temperature:</B>53<BR>
    <B>Wind:</B> 13 from S <BR>
    <B>Humidity:</B>92
  </BODY>
</HTML>
```

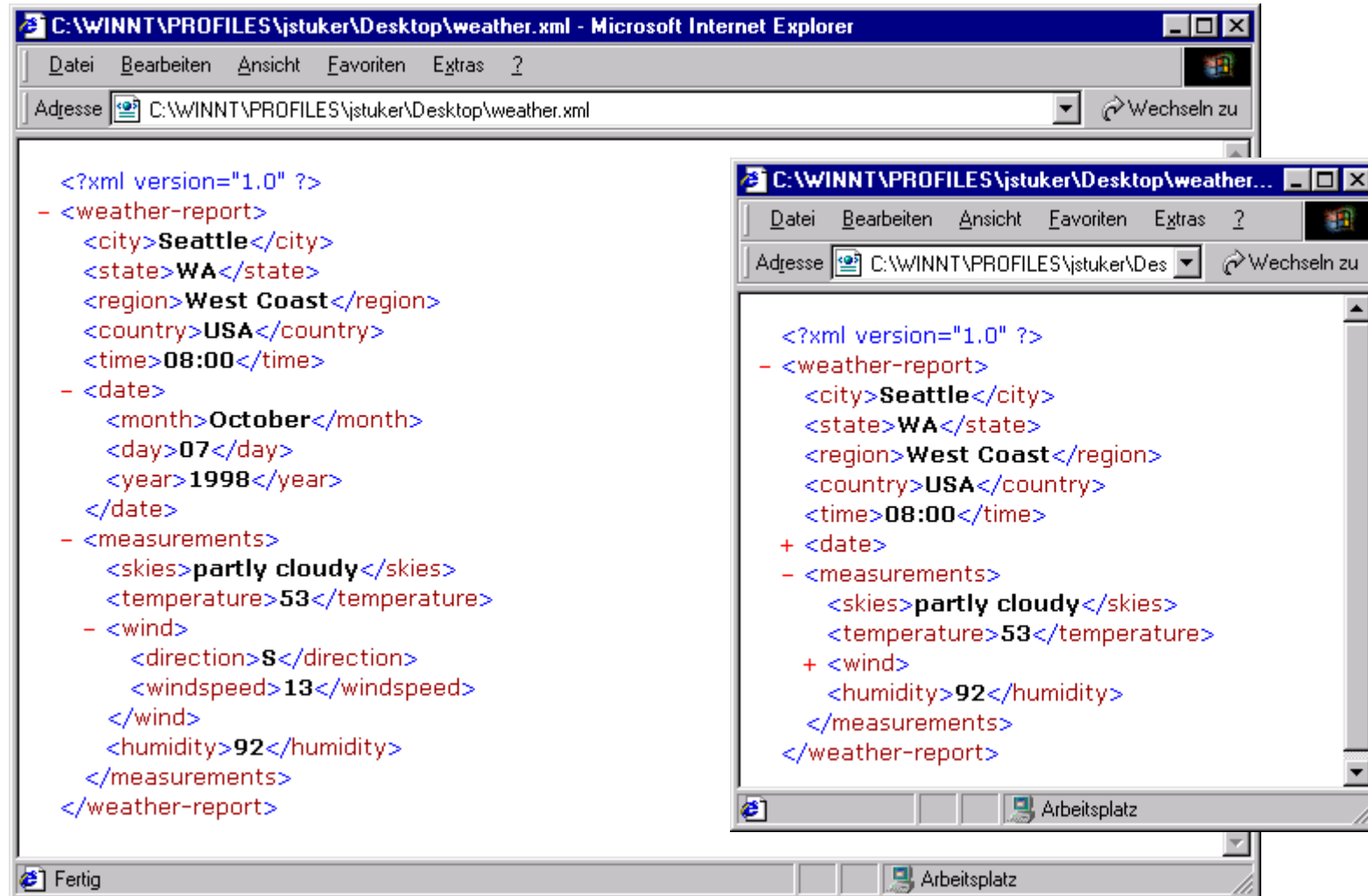




## Wettermessung „Seattle“ in XML

```
<?xml version="1.0"?>
<weather-report>
  <city>Seattle</city>
  <state>WA</state>
  <region>West Coast</region>
  <country>USA</country>
  <time>08:00</time>
  <date>
    <month>October</month>
    <day>7</day>
    <year>1998 </year>
  </date>
  <measurements>
    <skies>partly cloudy</skies>
    <temperature>53</temperature>
    <wind>
      <direction>S</direction>
      <windspeed>13</windspeed>
    </wind>
    <humidity>92</humidity>
  </measurements>
</weather-report>
```

# Darstellung in IE5 (unformatiert)





# Darstellung durch Anwendung

namics



**The Weather Channel - Seattle, WA - Microsoft Internet Explorer**

Address: <http://www.weather.com/weather/>

weather.com

Go Shopping | Interact | Inbox Weather | Wireless Weather | Weather on Your S

Customize My Weather

Local Weather

Any City or US Zip

Weather Information

Weather Maps  
US City Forecasts  
World Weather

News Center

Weather Headlines  
Tropical Season '99

Weather and...

Fall Foliage  
Travel  
Driving  
Outdoors  
Golf  
Home & Garden  
Health  
Sporting Events  
Schoolday Forecast

Featured This Week: [Fall Foliage](#) | [Golf Condi](#)

**FORECAST AND CURRENT COND**

**Seattle, Washington**

current conditions as reported at Seattle, WA  
Thursday, October 7th  
last updated at 9:14 pm PDT

**Sunrise:** 7:16 am PDT  
**Sunset:** 6:36 pm PDT

[check the weather](#) [Maps & Directions](#) [Dining R](#)  
[Lotto](#) [TV](#) [cool LIVE cams](#) [local events](#) [Mo](#)

**Want the most useful site in Se**

[detailed local forecast](#)

**5-day forecast** for Seattle, WA and vicin  
last updated Thursday, October 7th at 7:18 am F

**Weather Page - Microsoft Internet Explorer**

Address: <http://www.msnbc.com/ne>

We invented internet banking. **SECURITY FIRST NETWORK BANK** GO

**Invest in Information**  
MSNBC Investor Toolkit

**Weather**

• [sidewalk.com](#) Your personalized Seattle guide to entertainment

**Seattle, WA** Updated 09:00 ET October 7, 1999

**current conditions**

WIND	<b>s 13 mph</b>	BAROMETER	<b>30.07</b>	HUMIDITY	<b>92</b>
UV	<b>0</b>	REALFEEL	<b>42</b>	VISIBILITY	<b>6</b>

**53°** RAIN

**4 day forecast**

	THU	FRI	SAT	SUN
SHO	SHOWERS	SHOWERS	PARTLY SUNNY	PARTLY SUNNY
HIGH	<b>62°</b>	<b>62°</b>	<b>63°</b>	<b>63°</b>
LOW	<b>54°</b>	<b>49°</b>	<b>48°</b>	<b>52°</b>

**Regional Conditions**

- Precipitation
- Radar
- Satellite

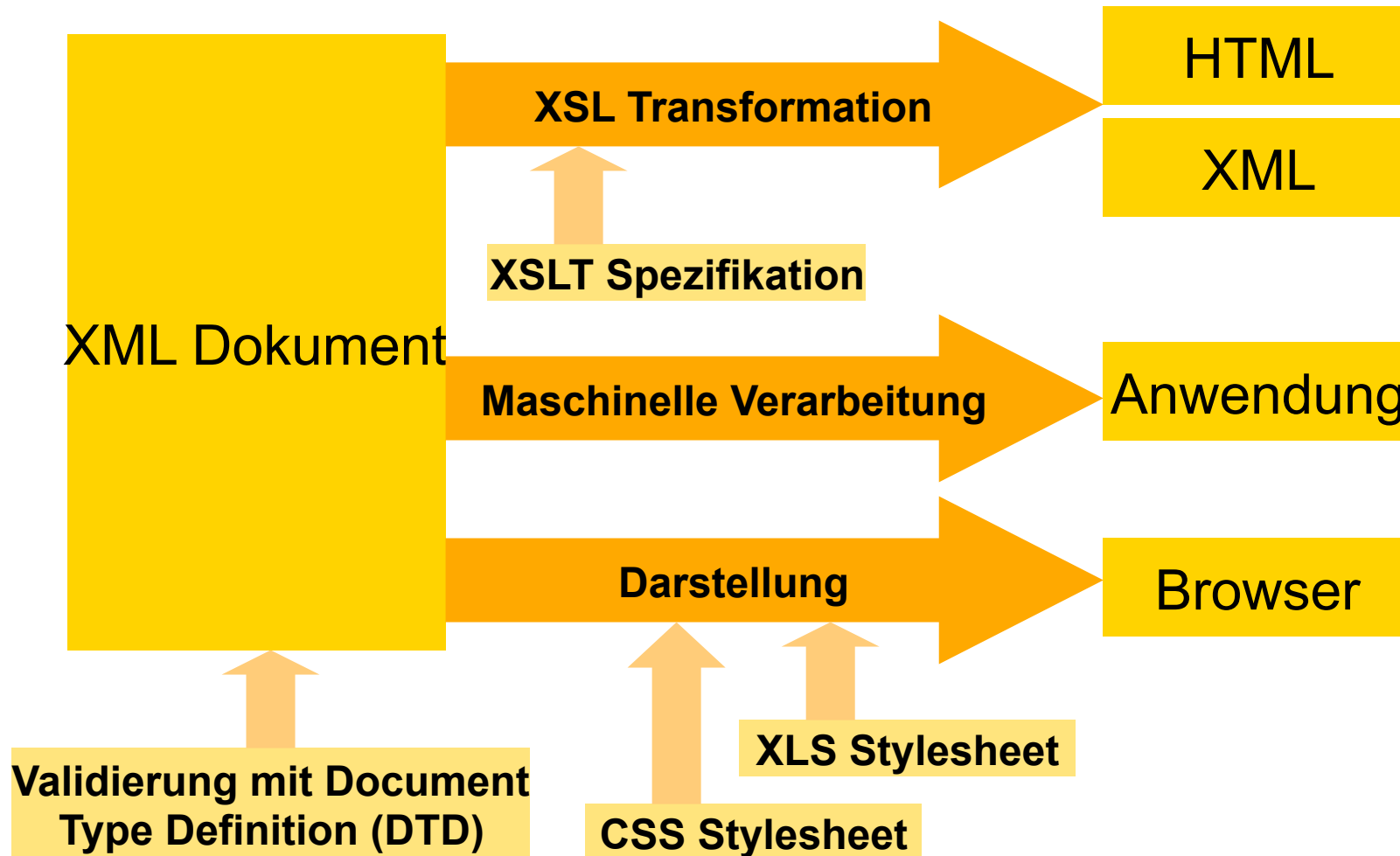
MSNBC Weather is provided by [AccuWeather](#)

Save as my default city for weather  Add to my MSNBC Cover page

[Show National Weather](#) Find other cities

Advertisement

*Tell someone*





## Anwendung von XML

- » In XML werden andere Formate beschrieben, z.B.:
  - Channel Definition Format (CDF)
  - Synchronized Multimedia Integration Language (SMIL)
  - Mathematical Markup Language
  - Wireless Markup Language (WML)
  
- » Datenaustausch, Middleware
  
- » Data Islands
  
- » Metadaten

- » Einfach
- » Es wird nie XML Ver. 2 geben
- » Sehr hohe Akzeptanz
- » Inhalt, Darstellung und Verarbeitung getrennt
- » Selbstbeschreibung
- » Schnittstellendefinition wird nicht einfacher

## Links

namics



- » [www.w3c.org](http://www.w3c.org)
- » [www.oasis-open.org](http://www.oasis-open.org)
- » [www.xml.com](http://www.xml.com)
- » [metalab.unc.edu/xml/](http://metalab.unc.edu/xml/)
- » [www.heise.de/ix/raven/Web/xml/](http://www.heise.de/ix/raven/Web/xml/)



# J2EE (Java 2, Enterprise Edition)

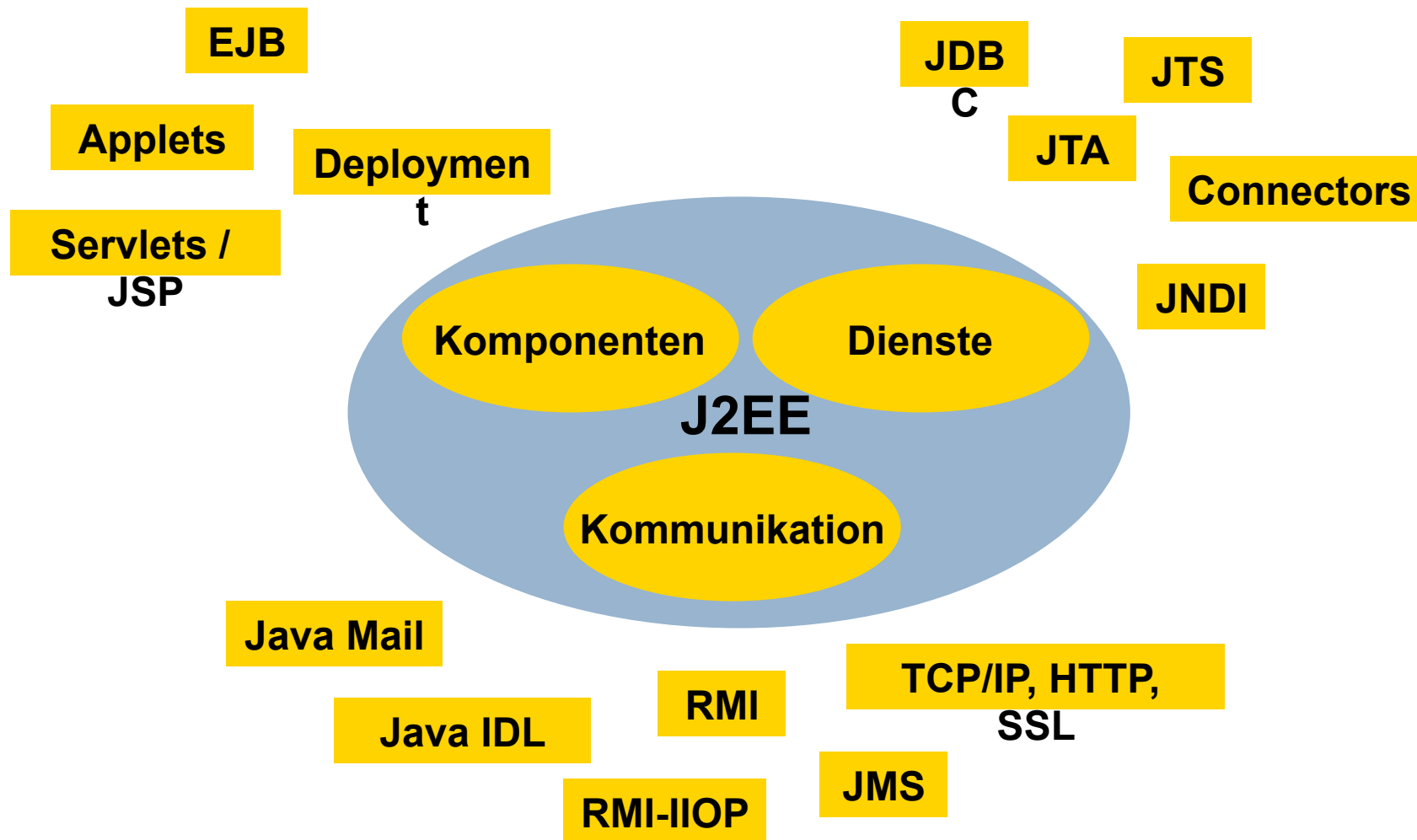


- » J2EE ist Spezifikation
  - Architektur (Application Model)
  - APIs und Richtlinien (Platform)
  - Testumgebung (Compatibility Test Suite)
  - Referenzimplementation
  
- » Fokus
  - 3-Tier Architektur, verteilte Anwendungen
  - Fokus „Existing Enterprise Application Systems“

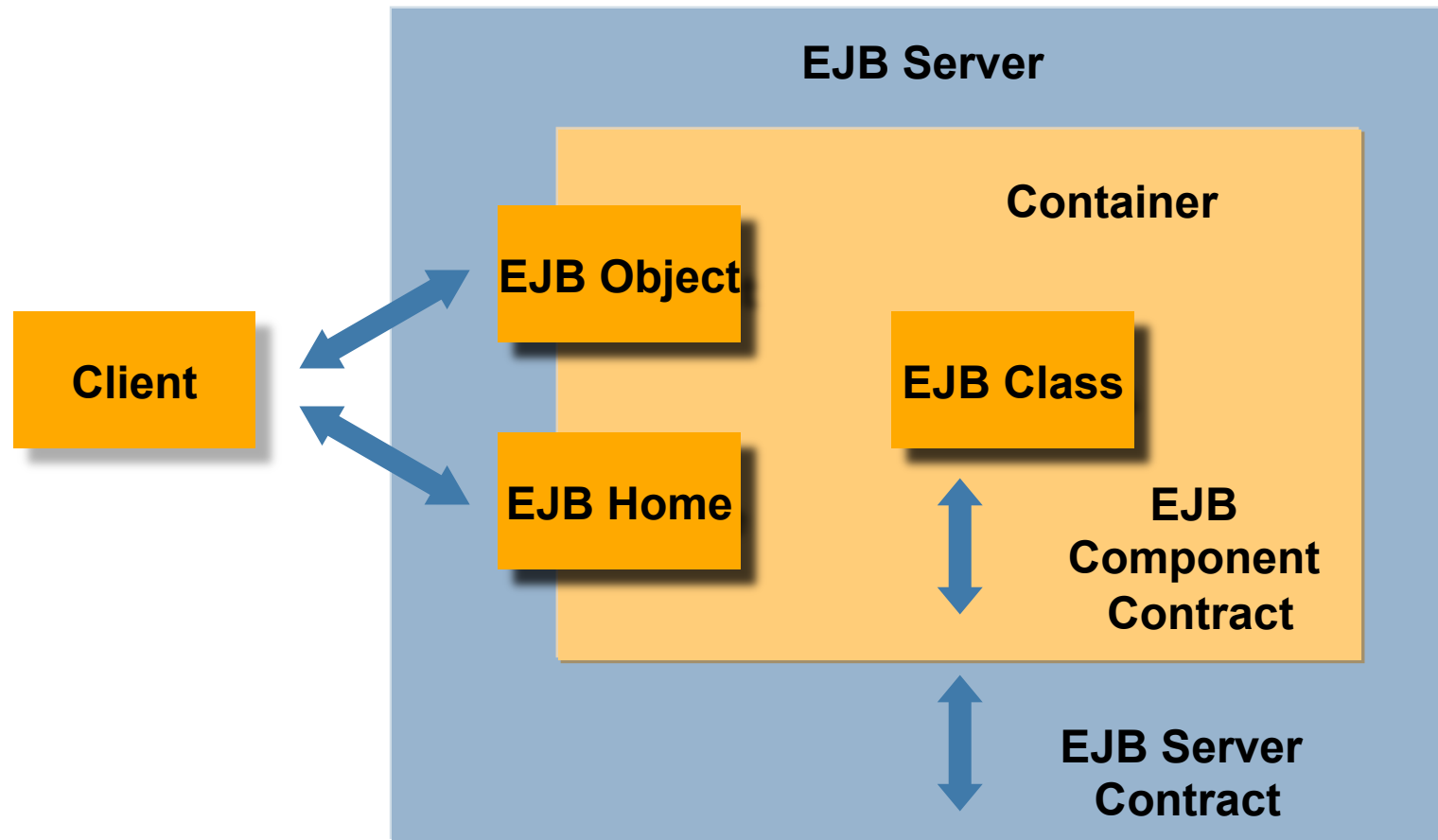


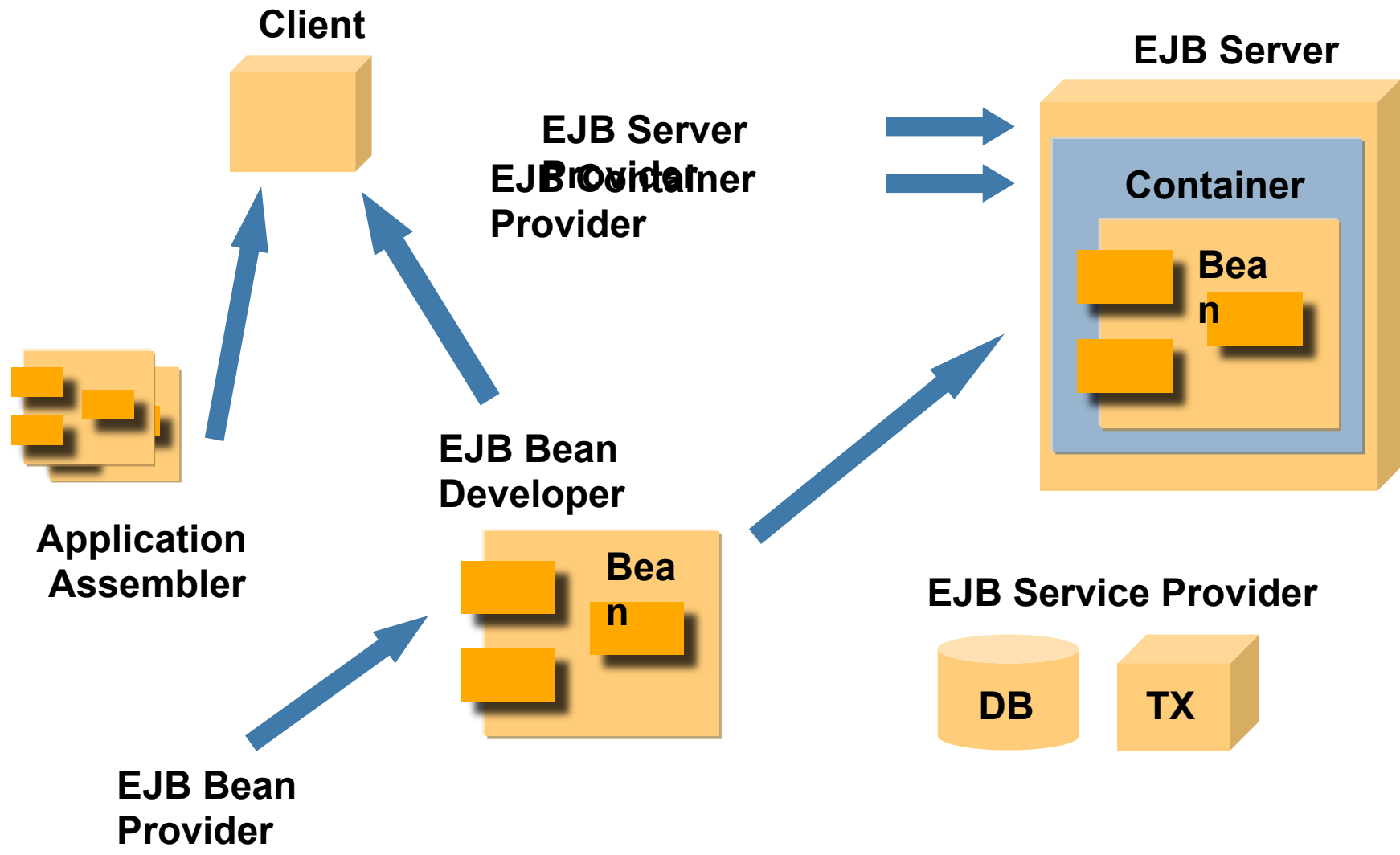
- » Middleware-Techniken sind vorhanden und bekannt
  
- » Standardfunktionen immer neu erfunden
  - Persistenz
  - Transaktionsmanagement
  - Sicherheit
  - Lastverteilung





- » Java als Sprache, JVM
- » Security (Definition bei der Ausbreitung)
- » Komponentenarchitektur und Schnittstellen auf dem „middle tier“ und dem „client tier“
- » Schnittstellen zum „EIS-tier“
- » Kommunikation
- » JDBC, JNDI, JMS, JavaMail







<b>EJB</b>	<b>Modell für Serverkomponenten</b>
<b>JNDI</b>	<b>Java Naming and Directory: DNS, NDS, LDAP, CORBA</b>
<b>RMI / IIOP</b>	<b>Java-to-Java und CORBA Kommunikation</b>
<b>JavaIDL</b>	<b>Java-to-CORBA inkl. IDL-to-Java Compiler und ORB</b>
<b>Servlets / JSP</b>	<b>Modell für Java in Webbrowser</b>
<b>JMS</b>	<b>Asynchrone Kommunikation. Queueing, Publish/Subscribe</b>
<b>JTA</b>	<b>Transaktionsmanagement auf Stufe Applikation</b>
<b>JTS</b>	<b>Verteiltes Transaktionsmanagement</b>
<b>JDBC</b>	<b>Datenbankzugriff</b>
<b>JavaMail</b>	<b>E-Mail</b>
<b>JAF</b>	<b>JavaBeans Activation Framework. Datenströme</b>



- » Kompatibel mit CORBA
- » Integration von verschiedensten Technologien
- » Setzt auf bestehenden Diensten auf
- » Regelt auch „weiche“ Aspekte
- » WORA (write once, run anywhere)

## Links

namics

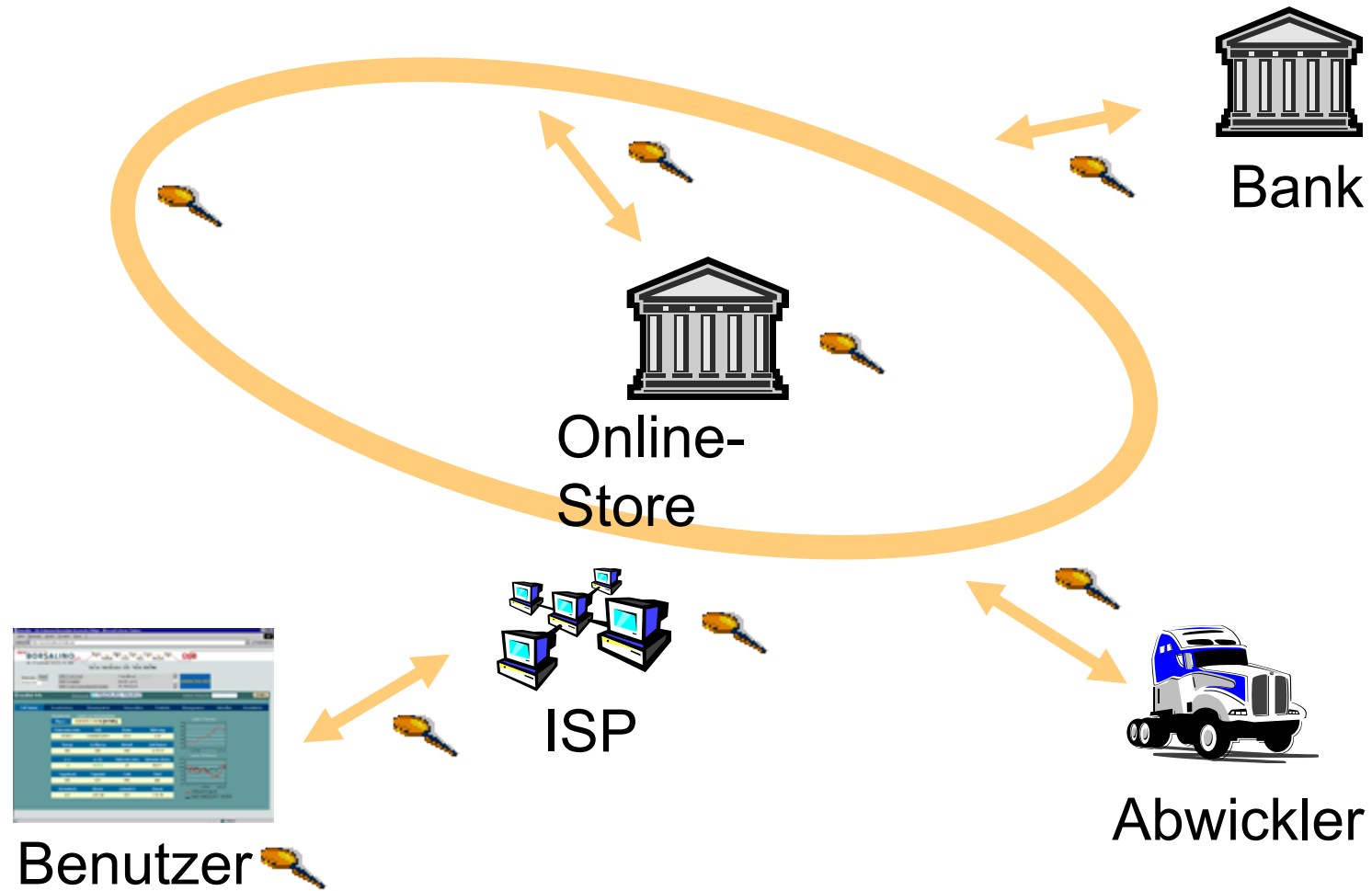


- » [www.sente.ch/cetus/software.html](http://www.sente.ch/cetus/software.html)
- » [java.sun.com/j2ee](http://java.sun.com/j2ee)
- » [www.ibm.com/developer/java](http://www.ibm.com/developer/java)
- » [www.gamelan.com](http://www.gamelan.com)



# PKI (Public Key Infrastructure)



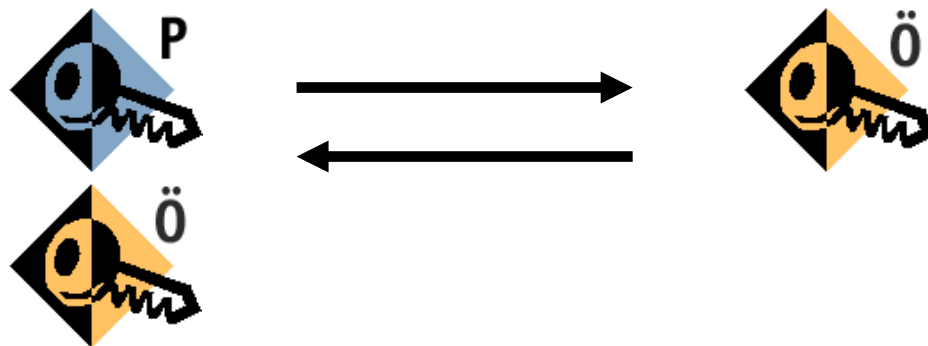




» Symmetrisch (z.B. DES, IDEA)

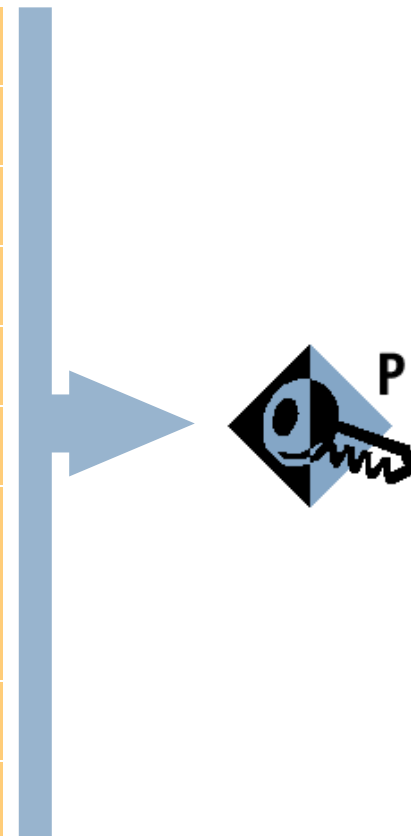


■ Asymmetrisch (z.B. RSA, ElGamal)



- » Symmetrische Verschlüsselung
  - Problem der sicheren Schlüsselverteilung
  - Spontane Transaktionen nicht möglich
  - Anzahl Schlüssel:  $m = n(n-1)/2$
  
- » Asymmetrische Verschlüsselung
  - Schlüsselpaar, ein Schlüssel öffentlich
  - Neue Anwendungen: Digitale Signatur
  - Hauptproblem: Richtige Zuordnung des öffentlichen Schlüssels zu seinem Besitzer

<b>Versionsnummer</b>	
<b>Zertifikatsnummer</b>	
<b>ID des verwendeten Signaturalgorithmus</b>	
<b>Name der CA nach X.500</b>	
<b>Gültigkeitszeitraum</b>	
<b>Name des Besitzers nach X.500</b>	
<b>Informationen zum öffentlichen Schlüssel des Besitzers</b>	<b>ID des Schlüsseldaten</b>
<b>ID der CA</b>	
<b>Zertifikatserweiterungen (0...N)</b>	
<b>Digitale Signatur des Trust Centers (CA)</b>	



# Schlüsselzertifikat in IE5

**Zertifikat** [?] [X]

Allgemein | Details | Zertifizierungspfad

 **Zertifikatsinformationen**

---

**Zwecke dieses Zertifikats:**

- Bestätigung von Windows-Systemkomponenten
- Windows-Hardware-Treiberbestätigung
- Ermöglicht die Verschlüsselung der Daten auf dem Datenträger
- Ermöglicht gesicherte Kommunikation im Internet
- Ermöglicht es Ihnen, einer Zertifikatsvertrauensliste digital zu

---

**Ausgestellt für:** Swiskey ID CA 1024

**Ausgestellt von:** Swiskey Root CA

**Gültig ab** 06.07.98 **bis** 01.01.06

[Ausstellereklärung...](#)

OK

**Zertifikat** [?] [X]

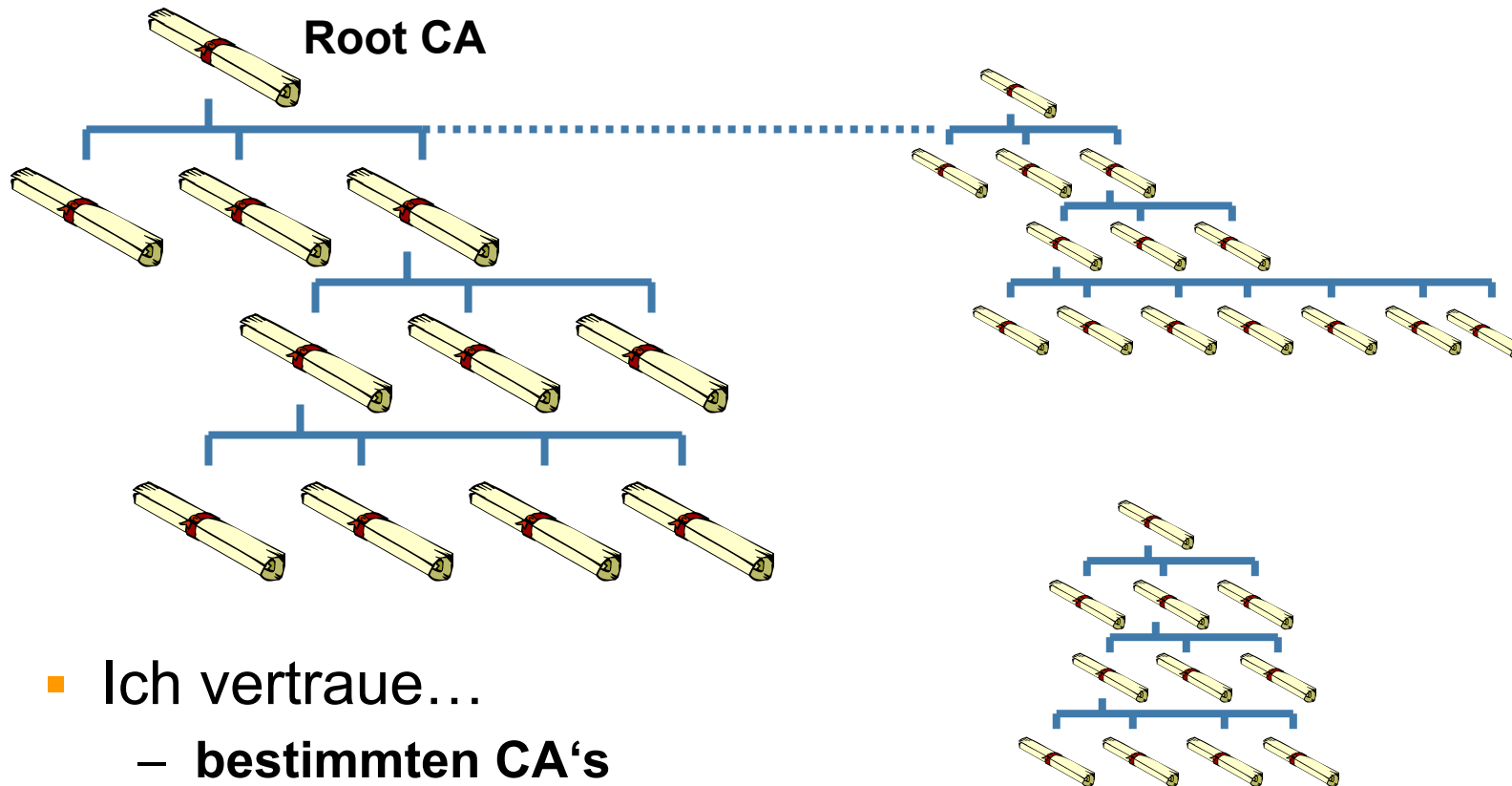
Allgemein | Details | Zertifizierungspfad

Anzeigen: <Alle>

Feld	Wert
Version	V3
Seriennummer	01
Signaturalgorithmus	md5RSA
Aussteller	Swiskey Root CA, Zuerich, Public CA Se...
Gültig ab	Montag, 6. Juli 1998 13:02:07
Gültig bis	Sonntag, 1. Januar 2006 00:59:00
Antragsteller	Swiskey Root CA, Zuerich, Public CA Se...
Öffentlicher Schlüssel	RSA (1024 Bits)
Basiseinschränkun...	Typ des Antragstellers=Zertifizierungsstell...
Schlüsselverwendu...	Zertifikatssignatur, Offline Signatur der Ze...
Fingerabdruckalgori...	sha1
Fingerabdruck	F14C 45C3 0C35 E751 B742 1BF1 A748 ...

[Eigenschaften bearbeiten...](#) [In Datei kopieren...](#)

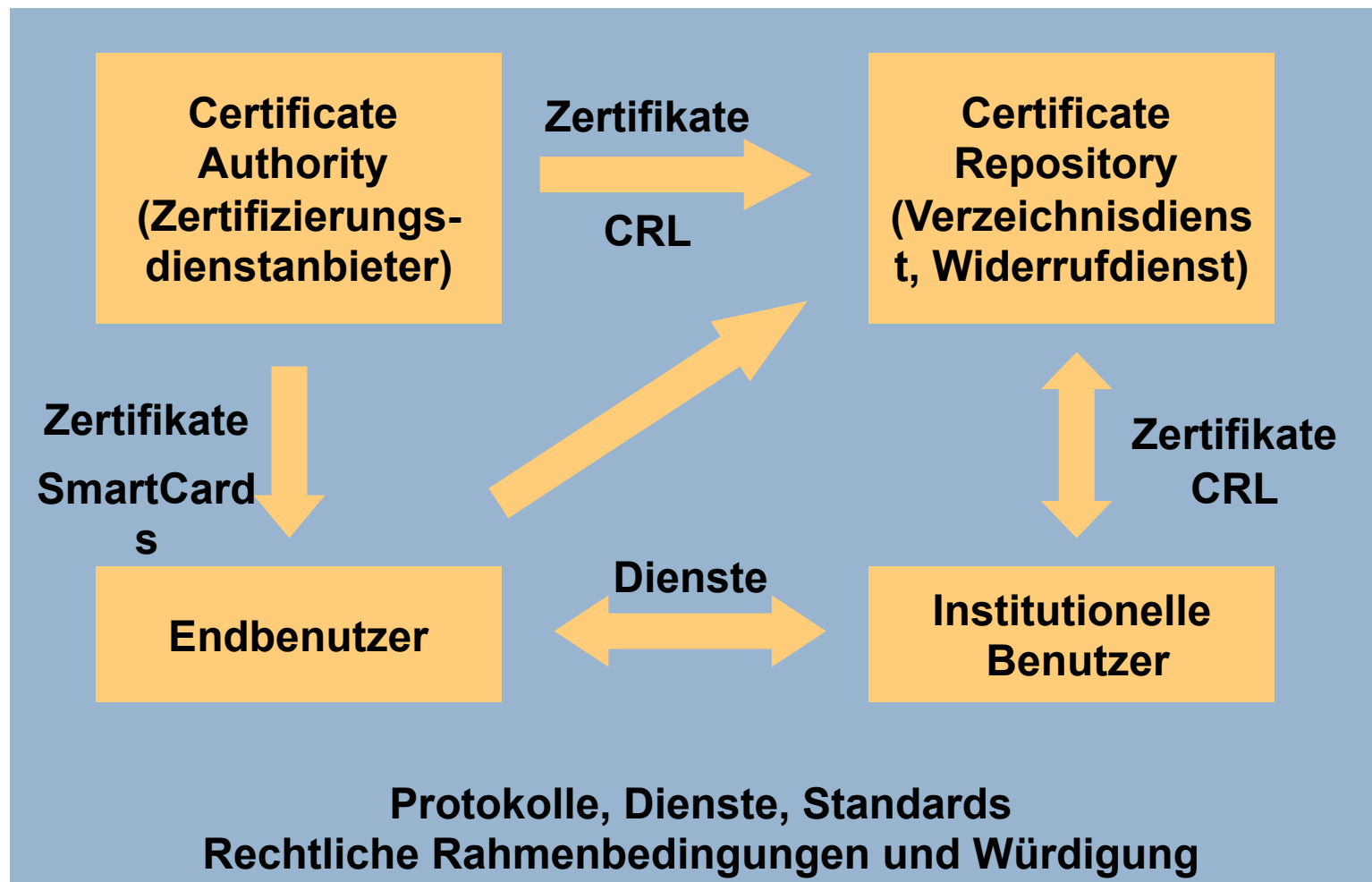
OK



- Ich vertraue...
  - bestimmten CA's
  - einzelnen Zertifikaten
  - für bestimmte Zwecke

- » Protokolle, Dienste und Standards
- » Technische Anforderungen
  - Erstellen von Schlüsselpaaren / Zertifikaten (X.509)
  - Widerrufen von Zertifikaten (CRL)
  - Auffinden und anbieten gültiger öffentlicher Zertifikate (LDAP, X.500)
  - Verwalten von sicherheitsrelevanten Zusatzinformationen
  - Schlüsselrückgewinnung (?)
- » Rechtliche Rahmenbedingungen
  - Anforderungen an PKI
  - Rechtliche Würdigung







- » Standards: X.509v3, X.500, LDAP, PKCS, PKIX, CRLv2
- » Kryptoalgorithmen und Schlüssellängen nach Stand der Forschung
- » Schlüsselaufbewahrung: SmartCards
- » Leistungsfähige CAs...

- » Kryptographie reguliert (Staatsschutz)
- » Schweiz
  - BAKOM fast fertig mit PKI-Verordnung
  - Ziel Leitplanken für Zertifizierungsdienste
  - Problem Ausführungsbestimmungen
  - Rechtswirkung der digitalen Unterschrift...
- » Europa
  - Richtlinie per 28. Juni 1999 Umsetzung 18 Monate
  - Signaturgesetze bereit: D, F, I, A...



- » PKI für E-Commerce unumgänglich
  - Vereinfachung der Abläufe
  - Verbindlichkeit, Vertraulichkeit, Anonymität
  
- » Keine technischen Probleme
  
- » Schweiz rechtlich im Rückstand



- » [www.bakom.ch/ger/subpage/?category\\_104.html](http://www.bakom.ch/ger/subpage/?category_104.html)
- » [www.ietf.org/html.charters/pkix-charter.html](http://www.ietf.org/html.charters/pkix-charter.html)
- » [www.semper.org/sirene/outsideworld/security.html](http://www.semper.org/sirene/outsideworld/security.html)
- » [www.ict.etsi.org/eessi/EESSI-homepage.htm](http://www.ict.etsi.org/eessi/EESSI-homepage.htm)
- » [www.rsasecurity.com/rsalabs/](http://www.rsasecurity.com/rsalabs/)



# XHTML



- » Offizielle nächste Generation von HTML
  
- » Heutiger Standard: HTML 4
  - Gültige W3C-Empfehlung seit Dezember 1997
  - Style Sheets
  - Verbesserungen bei Scripting, Tables etc.
  - Aktueller Update: HTML 4.01

- » Derzeit „Proposed Recommendation“ des W3C
- » Wichtigste Änderung: Angleichung an XML-Standard
- » Fokus:
  - Konsistent und automatisch prüfbar
  - Bessere Unterstützung verschiedenster Endgeräte
  - Modular und erweiterbar
  - Relativ problemloser Übergang von HTML 4.0



- » Dokument muss „Well-formed“ sein:
  - Korrekte Verschachtelung von Tags
  - Tags müssen immer abgeschlossen werden.  

```
<p><b>Dieser Text ist fett <i>und  
dieser auch noch schrägedruckt</  
i></b></p><br/>
```
  
- » Gross- und Kleinschreibung wird unterschieden
  
- » Attributwerte müssen „gequoted“ sein  

```
<table rows="3">
```

```
<html xmlns="http://www.w3.org/1999/xhtml"
  xml:lang="en" lang="en">
  <head>
  <title>Ein mathematisches Beispiel</title>
  </head>
  <body>
  <p>Der folgende Abschnitt stellt eine Formel dar:</p>
  <math xmlns="http://www.w3.org/1998/Math/MathML">
    <apply> <log/>
      <logbase>
        <cn> 3 </cn>
      </logbase>
      <ci> x </ci>
    </apply>
  </math>
  </body>
</html>
```

Konsistente Integration von  
anwendungsspezifischem  
Markup.

Voraussetzung: Browser muss  
die zusätzlichen Tags sinnvoll  
interpretieren können.

## Jetzt schon migrieren?

- » Existierende HTML-4.0-Browser verstehen XHTML 1.0 (relativ) problemlos
- » Tools wie „HTML Tidy“ generieren automatisch korrekten XHTML 1.0-Code aus bestehenden HTML-Seiten.
- » Editor-Tools sollten XHTML in den nächsten Versionen auch unterstützen.
- » Darum: Abwarten, bis der Standard freigegeben ist, dann aber relativ schnell migrieren



- » In Vorbereitung: XHTML 1.1/2.0, XHTML Profiles, Extended Forms
- » Weitere Infos: [www.w3c.org](http://www.w3c.org)



# Macromedia Flash

- » De-facto-Standard für multimediale, vektororientierte Online-Animationen
  - Herstellerangaben: 88% der Internet-User haben Flash-Plug-In
  - Semi-offener Standard: Fileformat und Player-Sourcecode sind publiziert
  - Aktuelle Version: Flash 4
  
- » Player gratis als Plug-In für fast alle Plattformen, Editor als kostenpflichtige Software



### Vorteile:

- » Relativ schnelle Ladezeiten auch für längere Animationen dank optimiertem Streaming
- » Grosse Gestaltungsfreiheit (Effekte, Schriften, Sound usw.)
- » Skaliert automatisch auf Auflösungen und grafische Möglichkeiten

### Nachteile:

- » Player nötig
- » Eher langsam über Modems
- » Kein wirklich offener Standard
- » Animationsdesign will gelernt sein...



## Flash: Erweiterte Möglichkeiten

- » Flash Generator: Automatische Generierung von Flash-Movies per Programm
- » Ab Flash 4: Interaktivität mit Formularen
- » Export-Möglichkeiten in immer mehr Programmen
- » Standalone-Player
- » Weitere Infos: [www.flash.com](http://www.flash.com)





# Open eBook



- » Standardinitiative für HTML- und XML-basiertes eBook-Format
- » Unterstützt von vielen grossen Verlagen, Softwarefirmen (z.B. Microsoft) und eBook-Herstellern
- » Final specification für Open eBook 1.0 erhältlich



- » Eng verwandt mit HTML
- » XML-konform
- » Kann auch gut in gängigen Browsern dargestellt werden.
- » Jede Publikation wird geliefert in einem OEB-Package, das aus mehreren Files bestehen kann.
- » Mehrere Lesereihenfolgen („Tours“) können spezifiziert werden.

- » Nicht gelöst: Kopierschutz, Verrechnungsmechanismen
  - OEB ist nur Hintergrundstandard, eigentliche Publikationen bleiben derzeit abhängig von spezifischen Geräten.
- » Komplette Editiertools bestehen noch nicht
- » Endgeräte noch verbesserungswürdig, Reader-Software für PC angekündigt
  
- » Weitere Infos: [www.openebook.org](http://www.openebook.org)



# MP3



- » Eigentlich: MPEG-1, Audio Layer 3
- » Offener Standard für Kompression von digitalen Audio-Signalen



- » Kompressionsfaktor ca. 1:12
- » Normales CD-Signal: ca. 1400 Mbit/s  
MP-3 Stereo-Signal: ca. 128 Mbit/s
- » Prinzip: „Perceptual Noise Shaping“  
Herausfiltern von Klanginformation, die vom menschlichen Ohr sowieso nicht wahrgenommen werden.

## Software:

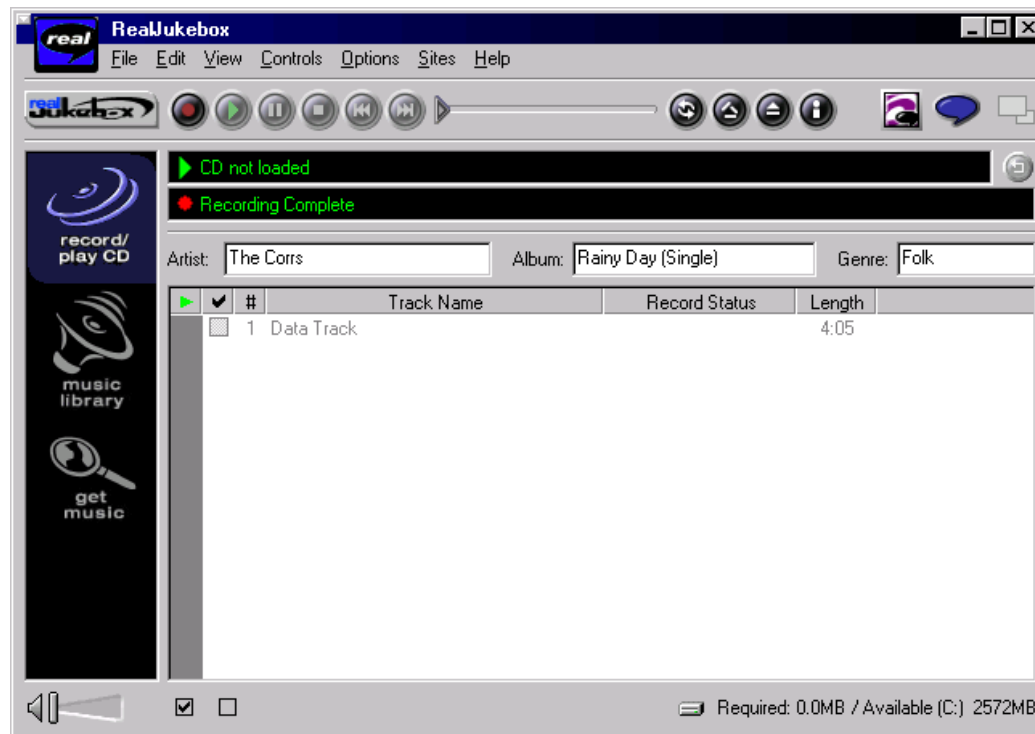


## Hardware:



Demnächst: Weitere Formen von Hardware-Playern, z.B. für Heimanlage, Handy und Auto





- » Verschiedene Programme für MP3-Recording auf dem PC sind erhältlich



## Secure Envelope: Verschlüsselung, Kopierschutz

Komprimiertes  
Audio-Signal  
in MP3

- » Problem: Wie verhindert man eine Trennung von Kopierschutz und digitalem Inhalt?



- » Heute dominierend: Verbreitung von Musik
  - Unbekannte Künstler, die sich bekanntmachen wollen
  - Relativ grosse Piratenszene, in der kommerzielle Musik verbreitet wird
  
- » Hörbücher
  
- » Sound-Unterstützung für Web-Applikationen



- » Secure Digital Music Initiative als übergeordneter Standard für Copyright-Schutz
- » Electronic Music Management System/Madison Project (IBM)
- » a2b Music (AT&T)
- » Windows Media (Microsoft)
- » Liquid Audio



## Pro:

- » Mit Abstand höchste Verbreitung
- » Viel Software und Hardware erhältlich

## Contra:

- » Verkäufe von Playern bisher relativ enttäuschend
- » Grosser Widerstand der Musikindustrie wg. Copyright-Problemen
- » Technisch bessere Standards existieren bereits

## Links

namics



- » [www.mp3.org](http://www.mp3.org)
- » [www.mp3.com](http://www.mp3.com)
- » [www.mpeg.org](http://www.mpeg.org)
- » [www.iis.fhg.de/amm/techinf/layer3/index.html](http://www.iis.fhg.de/amm/techinf/layer3/index.html)



# WAP

- » **Wireless Application Protocol (WAP):**  
Optimierte Protokolle für mobile Anwendungen, basierend auf Internet-Technologie
- » **Endgeräte:** Handy, PDA etc.
- » Seitendefinition mit **Wireless Markup Language (WML):**  
basiert auf XML





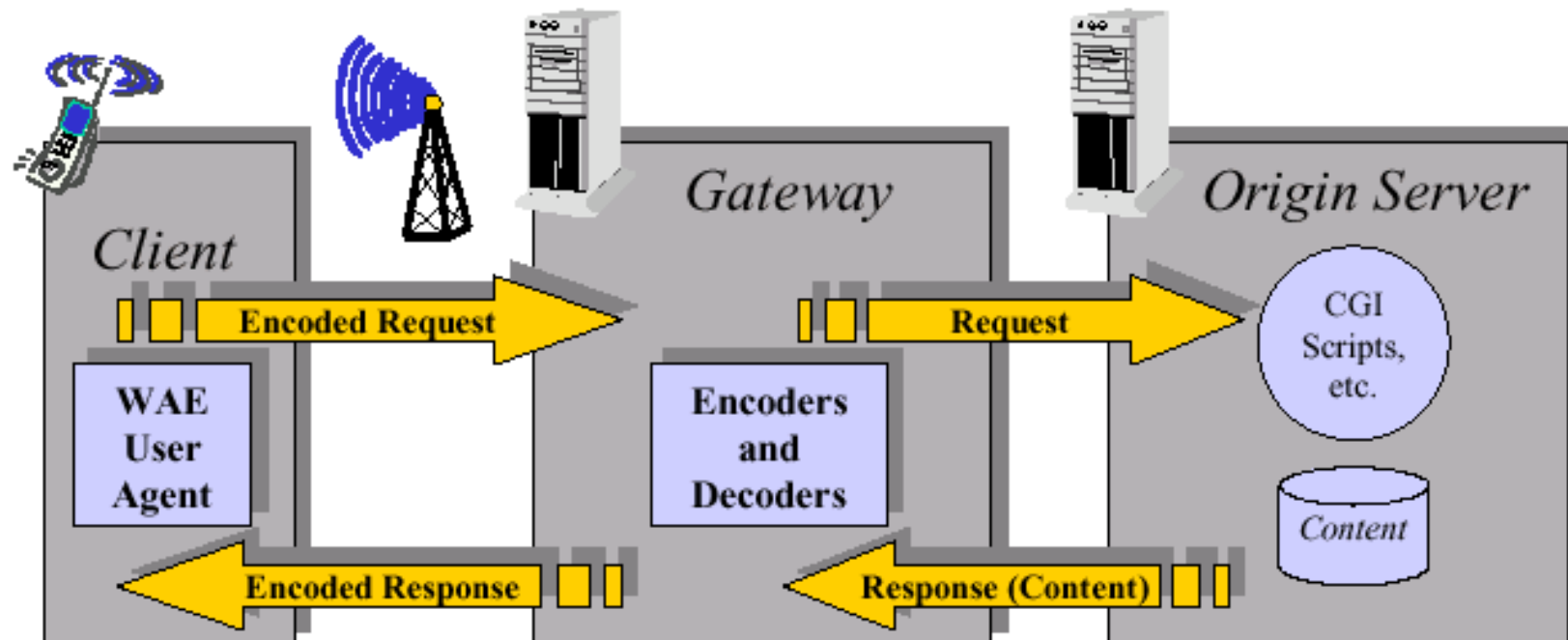
## Warum ein neuer Standard für Wireless-Anwendungen?



- » Immer grössere Verbreitung von Mobile Phones, wachsende Akzeptanz von Data-Anwendungen (SMS)
- » Bisherige Internet-Standards sind schlecht für mobile Anwendungen geeignet
- » Divergierende Entwicklungen von verschiedenen Hersteller
- ➔ Standardisierungsgremium **WAP Forum** unter Beteiligung fast aller wesentlichen Player

# Wireless Application Environment (WAE): Architektur

namics





```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
                "http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>

  <card newcontext="true" id="start">
    <do type="accept">
      <go href="#services"/>
    </do>
    <p>
      Willkommen an der IEX 2000!<br/>
    </p>
  </card>
  ...
```



```
<card id="services">
  <do type="prev">
    <go href="#start"/>
  </do>
  <p>
    <a href="hallo.wml">Applikation 1</a><br/>
    <a href="test.wml">Applikation 2</a><br/>
  </p>
</card>
</wml>
```

- » Handelsüblicher Web-Server, angeschlossen ans Internet
- » Spezialkonfiguration: Spezielle MIME-Typen
- » WML-Seiten bzw. WML-generierende Anwendungen (CGI, Java Servlets, Active Server Pages etc.)  
Generiert mit WAP-Entwicklungsumgebung
- » Zugang für Mobil-User
  - entweder über öffentliches WAP-Gateway
  - ...oder eigenes WAP-Gateway im Intranet

## WAP-Links

namics

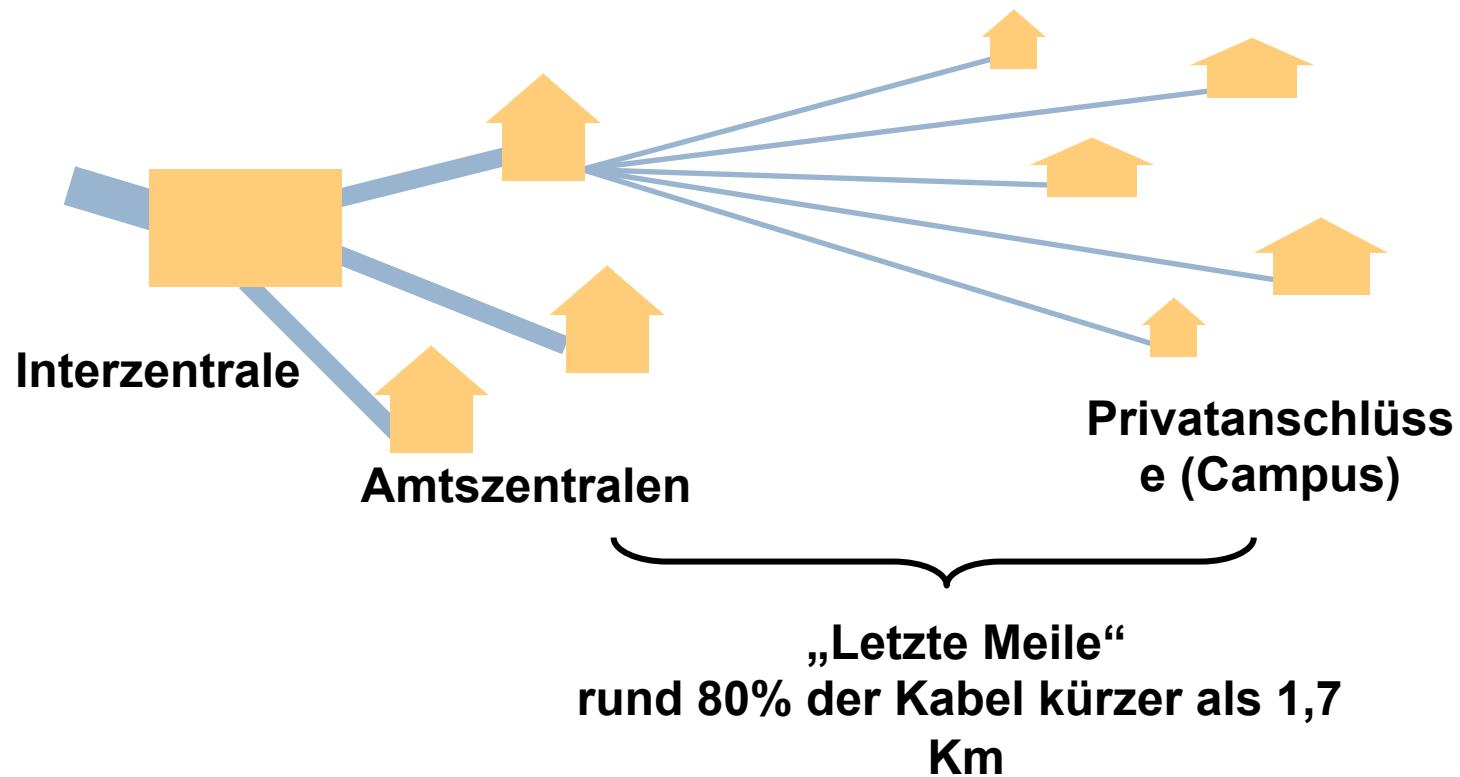


- » [www.wapforum.org](http://www.wapforum.org)
- » [www.ericsson.com/wap](http://www.ericsson.com/wap)
- » [www.wap-magazin.de](http://www.wap-magazin.de)
- » [www.wapnow.ch](http://www.wapnow.ch)
- » [www.wapguide.com](http://www.wapguide.com)

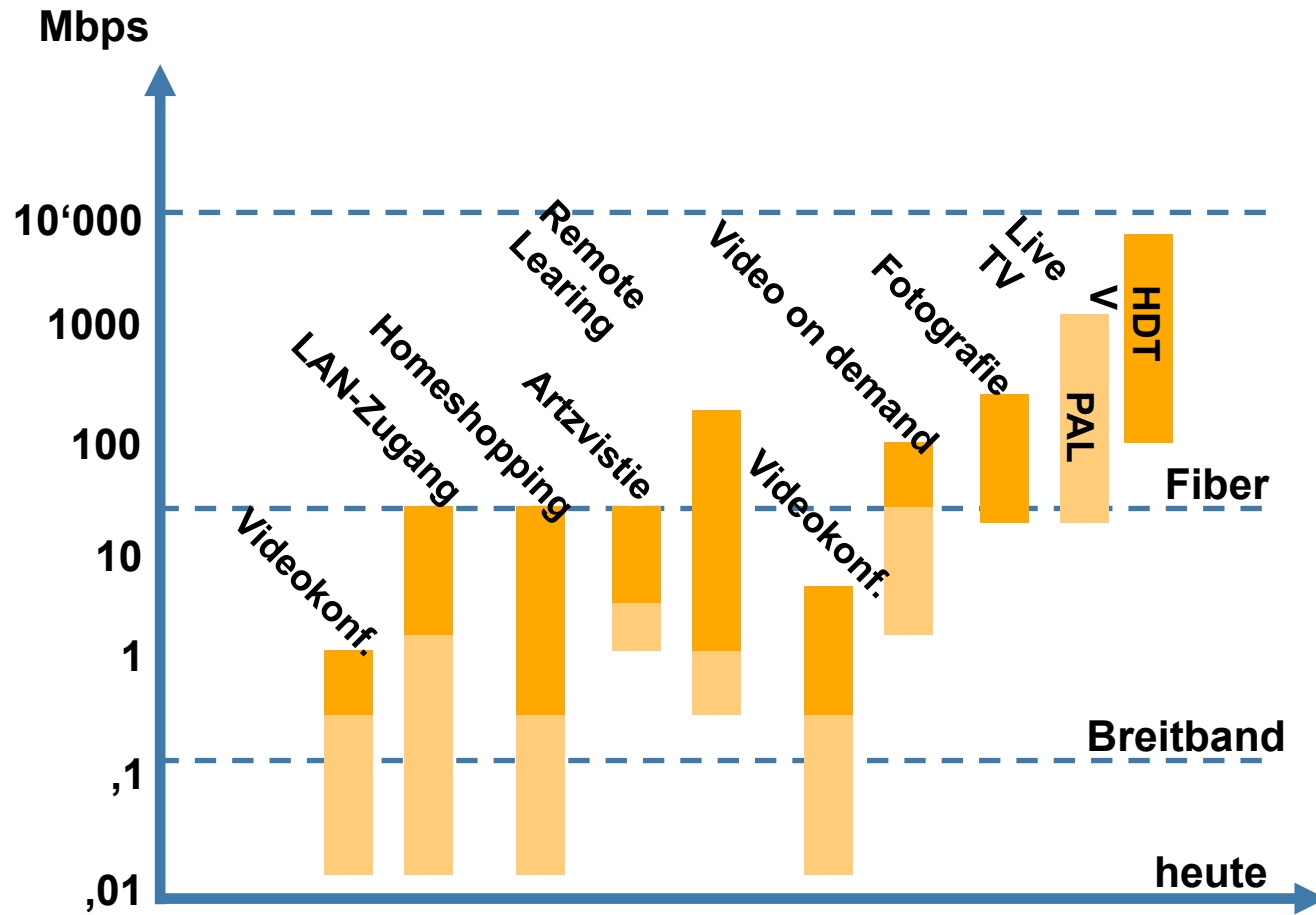


# xDSL (Digital Subscriber Line)

- » „Der Kampf um die letzte Meile“ oder „Aus Kupfer wird Gold“



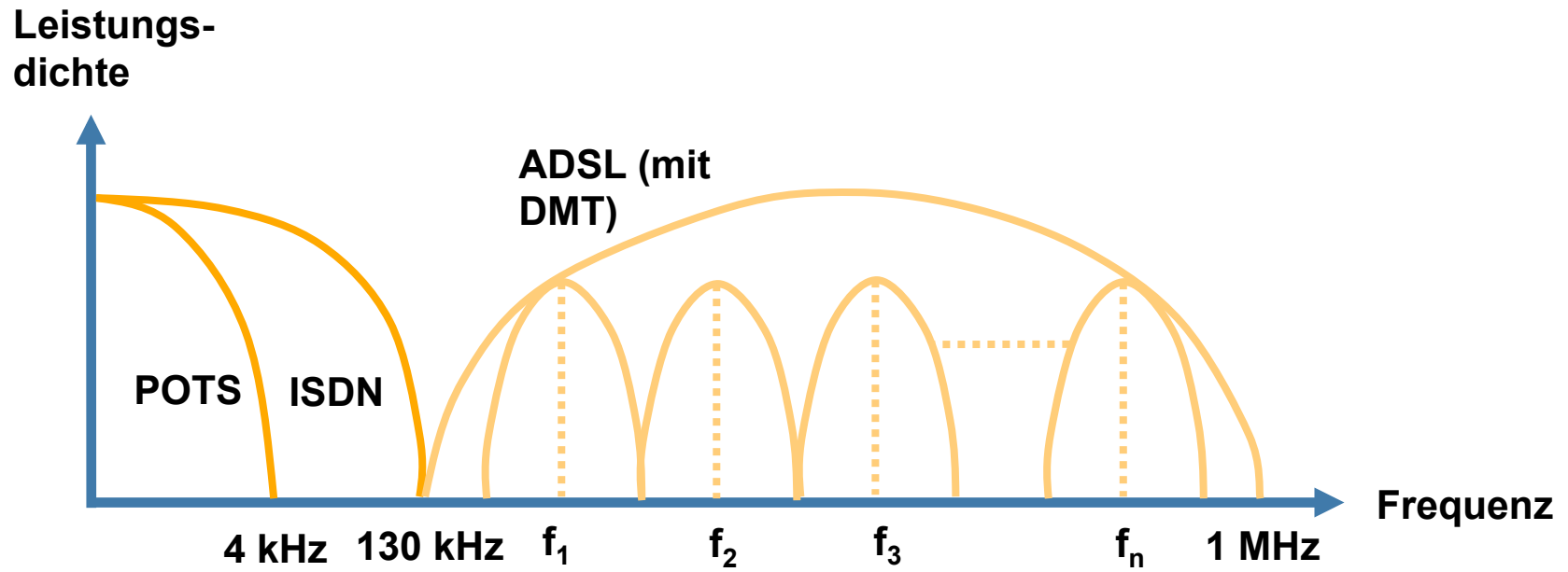




Residential Broadband. Kim Maxwell. Wiley, 1999



- » DSL = Digital Subscriber Line
- » Punkt zu Punkt Verbindungen über bestehende Kupfer-Leitungen (1 bis 4 Adern), „always on“
- » Erste DSL-Anwendung: ISDN
- » HDSL (high bitrate DSL) ab 1992 Technologie für T1/E1 auf fast allen Kabeln bis ca. 3 km



DSL – Die schnelle Leitung. c't  
19/1999

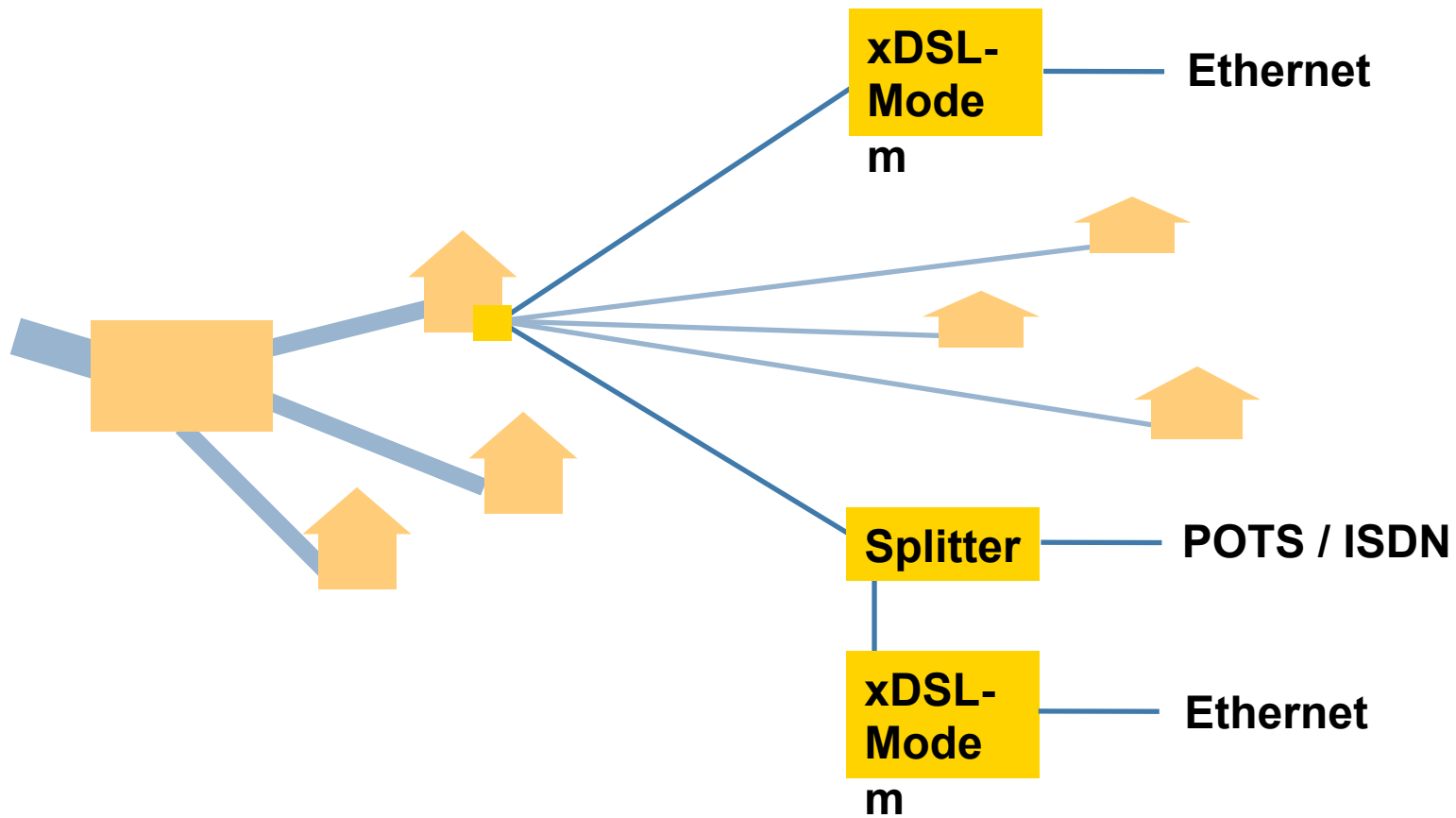
# Die wichtigsten xDSL Technologien

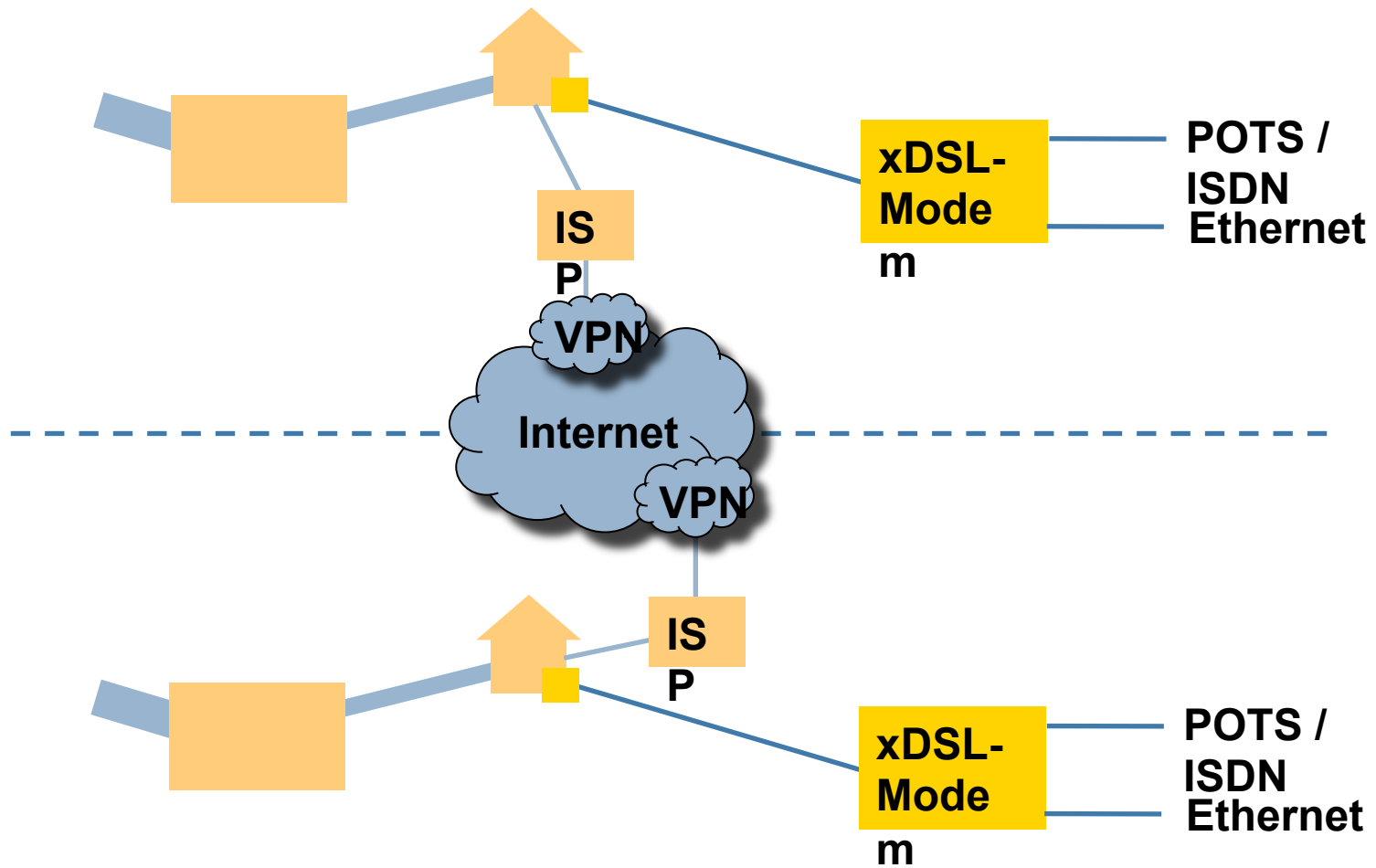


<b>ADSL</b>	<b>asynchron</b>	<b>1,5 - 8 Mbps down 64 Kbps – 640 Kbps up</b>	<b>2-Draht, bis 6 Km</b>
<b>ADSL Lite</b>	<b>universal, G-Lite</b>	<b>1 Mbps down 512 Kbps up</b>	<b>Microsplitter, 2-Draht, bis 6 Km</b>
<b>HDSL</b>	<b>high data rate</b>	<b>1,544 Mbps duplex (T1) 2,048 Mbps duplex (E1)</b>	<b>robust, 3 Km, 2 bis 6-Draht, bis 8 Km, repeater</b>
<b>SDSL</b>	<b>single line</b>	<b>200 Kbps - 2,048 Mbps</b>	<b>1-Draht, variable Bandbreite, bis 2,4 Km, 5,5 Km = 200 ...</b>
<b>VDSL</b>	<b>very high data rate</b>	<b>13- 52 Mbps down 1,5 – 2,3 Mbps up (oder 34 Mbps symmetrisch)</b>	<b>bis 1,5 Km, 2-Draht</b>

# Verbindung in der gleichen Stadt: 2 Mbps

namics







- » Schlecht standardisiert
  - ANSI, ETSI
  - Hersteller
  
- » Datenrate hängt vor allem ab von
  - Dämpfung (Kabellänge)
  - Übersprechung (Beschaltungsgrad, Anzahl Kabel, Dienste)
  - Reflexion an Kabelübergängen
  - Kabelqualität



- » Sehr billig
  - Aufschaltung und Miete Leitung
  - Veränderungen zu Hause
  - Endgeräte
  
- » Bsp. St. Gallen
  - Aufschalten Fr. 800.—
  - 1 km Fr. 45.—
  - jede weiter 100 Meter Fr. 3.— (Luftlinie)
  - Endgeräte...





- » Telephonleitungen sind flächendeckend vorhanden, sicher und rückwärtstauglich
- » Eignet sich zum Transport verschiedenster Netzwerkprotokolle
- » „Always on“, Robust
- » Rasche Amortisation, kleiner Installationsaufwand
- » Nicht nur zum surfen... (symmetrisch)

## Links

namics



- » [www.etsi.org](http://www.etsi.org)
- » [www.xdsl.com](http://www.xdsl.com)
- » [www.dslreports.com](http://www.dslreports.com)
- » Residential Broadband. Kim Maxwell. Wiley, 1999

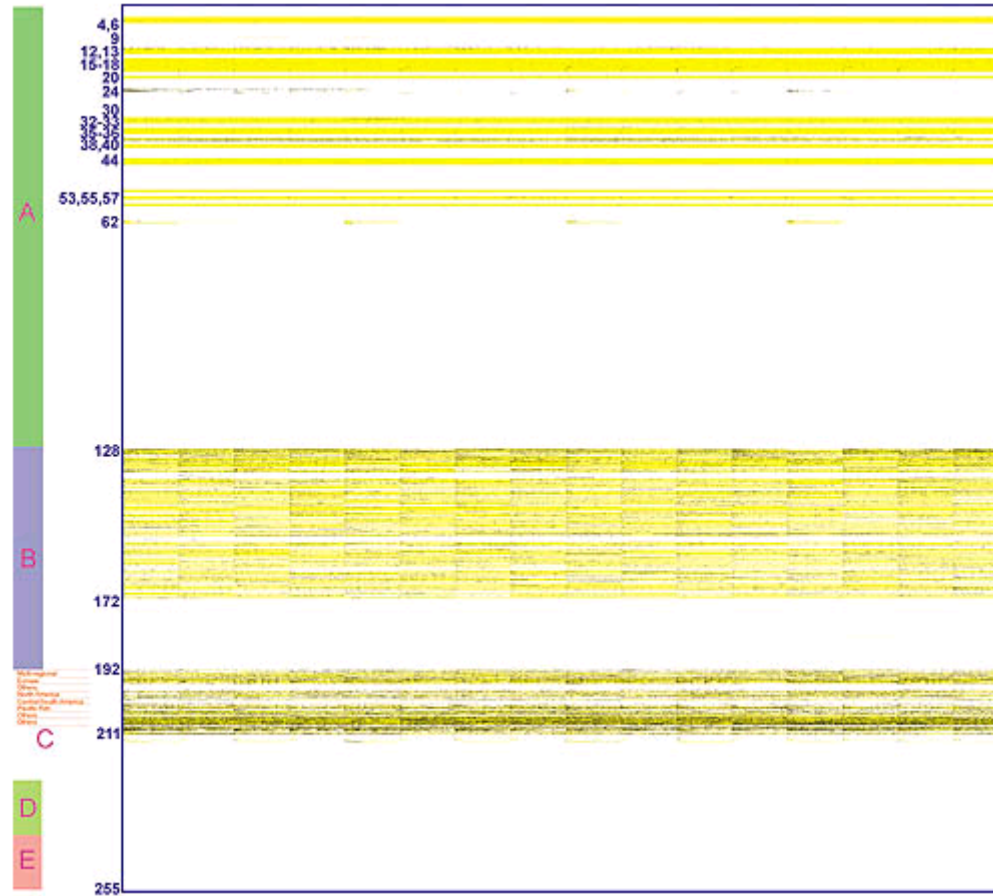


# IPv6

## Weshalb ein neuer Standard?

- » Knappheit von IP-Adressen
  - Wachstum Internet
  - NAT (network address translation, RFC 1631)
  - CIDR (classless interdomain routing, RFC 1817)
  - Intranet Adressen (RFC 1918)
  - Subnettierung (RFC 950 und RFC 1219)
  - xDSL, CATV sind „always on-line“

# Adressraum IPv4




Nummernspiele. c't 9/1999

- » grösserer Adressraum
- » einfacher, schnell auswertbare Pakete
- » Bessere Routen im Internet durch Gruppierung
- » Sicherheit im Protokoll verankert
- » bessere Multicast, Anycast statt Broadcast
- » QoS (quality of service)
- » Unterstützung von Switching

# IPv4 Paket

← 32 Bit →

<b>V</b>	<b>HL</b>	<b>SVC</b>	<b>Lenght</b>	
<b>ID</b>		<b>F</b>	<b>Offset</b>	
<b>TTL</b>	<b>Prot</b>	<b>Checksum</b>		
<b>Source Address (32 Bit)</b>				
<b>Destination Address (32 Bit)</b>				
<b>Options</b>			<b>Padding</b>	
<b>Data Field (bis 65'516 Bytes, typisch 500 resp. 1500)</b>				

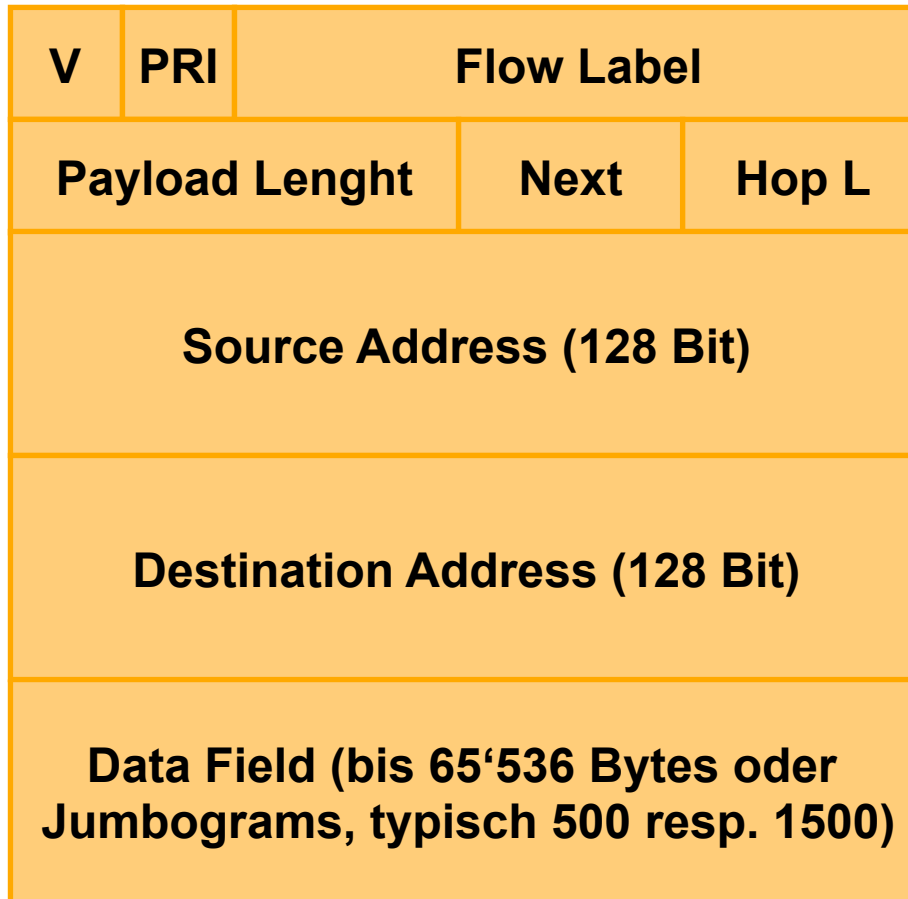


# IPv6 Paket

namics

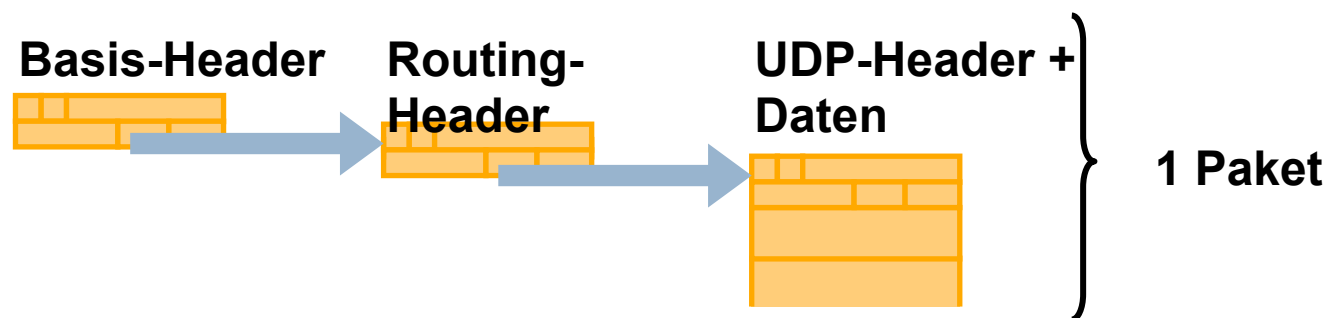


← 32 Bit →



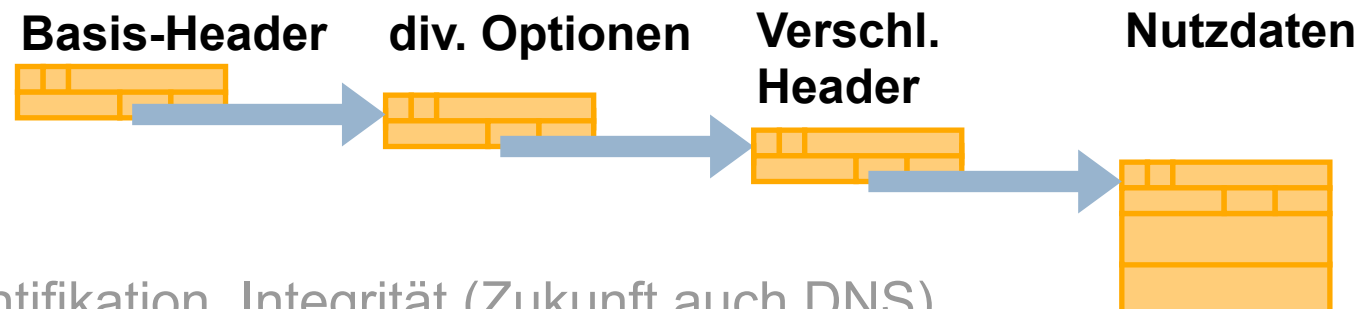


- » Header auf Minimum gekürzt und fixe Länge
- » Fragmentierung durch Router verboten, keine Checksumme
- » Optionen durch verkettete Header



- » Verlängerung von 4 auf 16 Bytes
  - $2^{128}$  IP-Adressen =  $3,4 * 10^{38}$
  - 340'282'366'920'938'463'463'374'607'431'768'211'456
  - pro  $\text{mm}^2$  der Erdoberfläche 667 Billionen Adressen
  
- » Andere Darstellung wegen Lesbarkeit
  - Gruppen von 2 Bytes in HEX
  - 4711:0:0:0:0:5:EEC1:6008 ist gleich 4711::5:EEC1:6008
  - 0000:0000:0000:0000:0000:0065:78C1:009A:6008  
ist gleich ::65:78C1:9A:6008
  
- » Gemischte Schreibweise: ::FFFF:128.1.35.201

- » Basiert vollständig auf Verfahren von IPSec
- » Vertraulichkeit



- » Authentifikation, Integrität (Zukunft auch DNS)
  - Eigener Header, min. MD5 oder SHA, Verschlüsselung nicht festgelegt

- » Zusätzlich zu DHCP statusfreie Adressengenerierung
- » ICMP-Erweiterungen
  - Router-Bekanntmachung, Anfrage an Router
  - Bekanntmachung von Nachbarn, Anfrage am Nachbarn
  - ARP-Ablösung
- » Mobile-IPv6: Zusätzliche Adresse und Agent im Heimnetz

## » PRI-Feld im Basis-Header

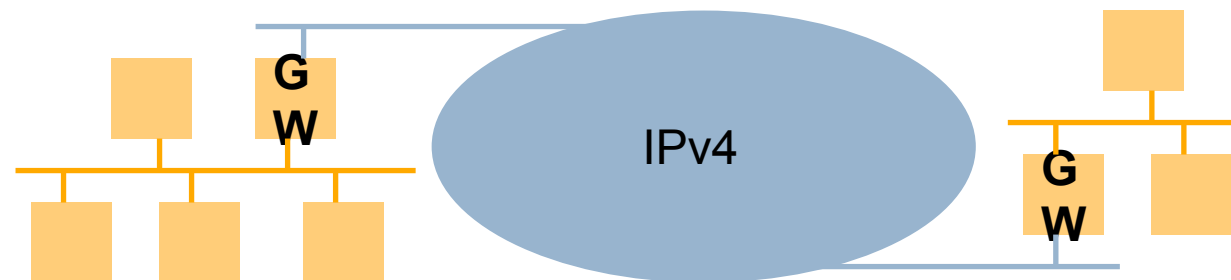
## » Flusskontrollen in höheren Schichten

<b>0000</b>	<b>unklassifiziert</b>
<b>0001</b>	<b>zeitunkritisch (NEWS) / geringste Kosten</b>
<b>1000</b>	<b>interaktiv (TELNET) / geringe Verzögerung</b>
<b>1001</b>	<b>realtime / geringe Verzögerung +</b>
<b>0010</b>	<b>Steuerungsnachrichten (ROUTING) / Zuverlässigkeit</b>
<b>0100</b>	<b>Massendaten (FTP) / max. Durchsatz</b>

- Unterhalb von IP nicht möglich
- Flow Label erlaubt Unterscheidung von Datenströmen

- » IETF working group NGTRANS
- » Auswirkungen auf Protokolle in Abklärung
  - UDP, TCP: Jumbograms
  - FTP: IP in Datenkapsel, PORT-Befehl
- » DNS: Neuer Bezeichner AAAA
- » DHCPv6, RIPng

- » IPv6 kompatible Produkte, Adressen und RFCs: [www.6bone.net](http://www.6bone.net)
- » Aufbau von IPv6-Inseln mit neuen Komponenten
  - Router, Nameserver, evt. DHCP, Clients
- » IPv6 durch IPv4 tunneln (später umgekehrt)



# 6Bone in Europa

namics



[www.nas.nasa.gov/Groups/LAN/IPv6/viz/static-maps.html](http://www.nas.nasa.gov/Groups/LAN/IPv6/viz/static-maps.html)



- » Adressraum ist nicht das Thema
- » Viele interessante und gute Neuerungen
- » Rückwärtskompatibel aber Infrastruktur muss angepasst werden
- » Beide Standards werden während Jahren nebeneinander existieren
- » 6Bone: 1996 – 100 Standorte; Aktuell 503 über IPv4 Tunnel verbunden



- » [www.ip-sec.com](http://www.ip-sec.com)
- » [www.ietf.org/html.charters/ipngwg-charter.html](http://www.ietf.org/html.charters/ipngwg-charter.html)
- » [www.ietf.org/html.charters/ipsec-charter.html](http://www.ietf.org/html.charters/ipsec-charter.html)
- » [www.cisco.com](http://www.cisco.com)
- » [www.6bone.net](http://www.6bone.net)
- » IPv6 – das neue Internet Protokoll. Hans Peter Dittler. dpunkt-Verlag, 1998

**Danke für Ihre Aufmerksamkeit!**

Frankfurt, Genf, Konstanz, Lausanne, St.Gallen, Zug, Zürich