

10 Internet-Standards für die Zukunft

IEX 2002 | Seminar w-10

Donnerstag, 7. Februar 2002

Andreas Göldi, Partner, namics ag
Jürg Stuker, Partner, namics ag

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



Die Top 10 Internet-Standards 2001

- » UML
- » .NET/C#
- » SOAP
- » P2P
- » DivX ;-)
- » UMTS
- » RDF
- » Micropayments
- » XForms
- » Spracherkennung/VoiceXML



Die Top 10 Internet-Standards 2002

- » MMS
- » WAP 2.0
- » J2ME / Embedded Java
- » XML Security
- » Web Services
- » Neue DNS Features
- » JXTA
- » Device Independence
- » Universal Usability
- » Flash-Erweiterungen



MMS



Wir alle kennen SMS

- » „Short Message Service“:
Push-Mechanismus im GSM-Standard, nutzt
Signalisierungskanal.
- » Heute extrem populär geworden:
Weltweit werden jeden Monat 30 Milliarden SMS verschickt!
- » Limit auf 160 Zeichen
- » Proprietäre Erweiterungen verschiedener Hersteller für
Übermittlung von Klingeltönen, Logos usw.
Offizieller erweiterter Standard: EMS
- » Anwendungen
 - Persönliche Kommunikation
 - Infodienste
 - Entertainment (z.B. Klingeltöne)
 - Werbung
 - Over-the-Air-Konfiguration (z.B. WAP)

Zwischenstufe: EMS (Enhanced Messaging Service)

- » Gemeinsam akzeptierter Standard für erweiterte SMS-Funktionalitäten
 - Entwickelt von Ericsson
 - Von allen Herstellern unterstützt, nur Nokia ist skeptisch.
 - Kompatibel mit vorhandener SMS-Infrastruktur in den Netzen und den meisten Telefonen

- » Zusätzliche Funktionalitäten
 - Textformatierung
 - Kleine S/W-Bilder und Animationen
 - Sounds und Melodien





MMS (Multimedia Messaging Service)

- » Kompletter neuer Standard, nicht kompatibel mit SMS/EMS
 - Neue Netzinfrastruktur
 - Neue Endgeräte

- » Funktionen
 - Übermittlung von Text, Bildern, Videos, Audio
 - Offen für weitere Formen

- » Benötigt mindestens ein 2.5G-Netz (GPRS), ist aber auch kompatibel mit 3G (UMTS) und weiteren Trägernetzen.



- » Grundtechnologie orientiert sich stark am Internet
- » Unterstützt Standardformate
 - GIF, JPEG
 - MPEG4
 - MP3, MIDI
- » Basisprotokolle
 - Codierung: MIME und SMTP
 - Übertragung/Ausführung: WAP oder MExE (Mobile Station Application Execution Environment, Java-basiert)
- » Übermittlung nicht über Signalisierungs-, sondern Datenkanal



Ericsson T68: EMS-fähig, Farbdisplay,
vorbereitet für MMS (Software-Update nötig)



Nokia 7650 (angekündigt):
Eingebaute Kamera, Farbdisplay,
Symbian-OS, MMS

- » Vielversprechende Technologie, aufbauend auf existierenden (Internet-)Standards
→ Interessanter Trend im Telecom-Umfeld
- » Erfolg dürfte beträchtlich sein, wenn Marktreife erreicht wird.
- » Aber:
 - Zeit der Marktreife von Endgeräten ungewiss
 - Massive Investitionen von Netzbetreibern nötig
 - Abhängig von breiter Verfügbarkeit von 2.5G und 3G-Mobilnetzen

Weitere Informationen

- » <http://www.mobilemms.com/>
- » <http://www.ericsson.com/mms/>
- » <http://www.nokia.com/mms/>
- » <http://www.3gpp.org/>
- » <http://www.wapforum.org/>



WAP 2.0



WAP: Bisher keine Erfolgsgeschichte

- » Wireless Application Protocol (WAP) ist ein Standard für mobile, interaktive Datendienste
 - Informationsabruf, z.B. Wetter, Börsen, Nachrichten
 - Entertainment
 - Location-based Services, z.B. Restaurantsuche
 - M-Commerce

- » Auf den Markt gekommen Anfang 2000, begleitet von sehr viel Hype
 - Massive Werbung
 - Aber: Kaum brauchbare Geräte erhältlich

WAP, ein totaler Flop?

- » WAP 1.0/1.1 muss wohl als Flop angesehen werden
 - Geräteverfügbarkeit inzwischen gut, aber Nutzung enttäuschend
 - Nur wenig brauchbare Inhalte

- » Bisherige Probleme:
 - Zuverlässigkeit und Geschwindigkeit
 - Umständliche Bedienung
 - Fehlende Benutzerfreundlichkeit der Anwendungen
 - Hohe Kosten für Benutzer
 - Investitionsbedarf für Content Provider wg. Anpassung der Inhalte an WAP-Standards

- » Aber: Mobile Datendienste können durchaus erfolgreich sein
 - i-Mode in Japan
 - Erfolg von SMS

Überblick: Was ist neu in WAP 2.0?



- » Zusammenfassend:
WAP mutiert vom „exotischen“ eigenen Mobil-Standard zu einem vereinfachten Subset des normalen Web

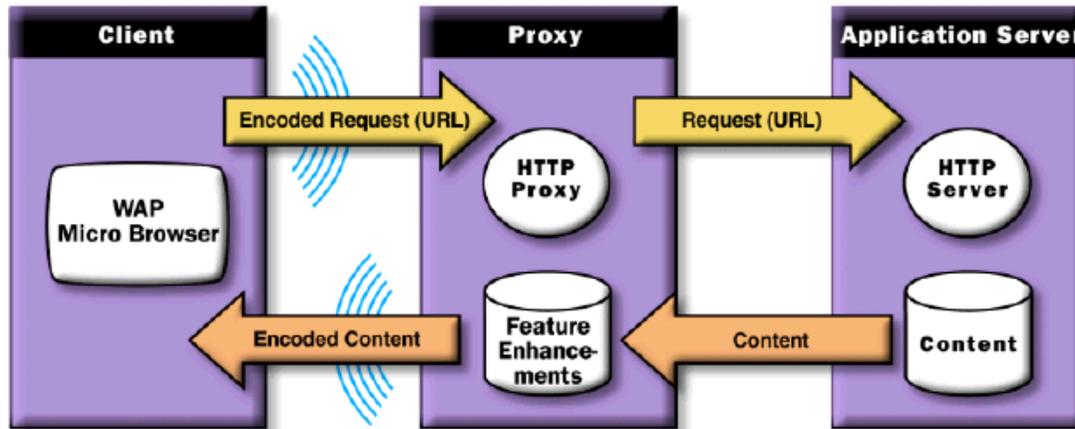
- » Netzwerkebene: Stärkere Orientierung an gängigen Internet-Protokollen
 - TCP
 - TLS (Transport Layer Security)
 - HTTP
 - → Das heisst: Kein WAP-Gateway mehr nötig!

- » Seiten-Codierung in WML2, basierend auf XHTML

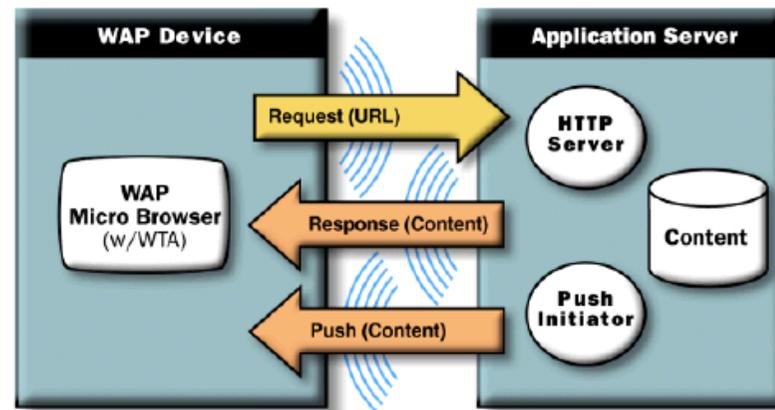


- » Basis: XHTML Basic Profile
Kern der XHTML-Spezifikation von W3C
- » Cascading Style Sheets Mobile Profile:
Subset von CSS2
- » Composite Capabilities/Preference Profiles
(CC/PP) für Beschreibung der User-
Präferenzen und Device-Fähigkeiten

Neues Kommunikationsmodell



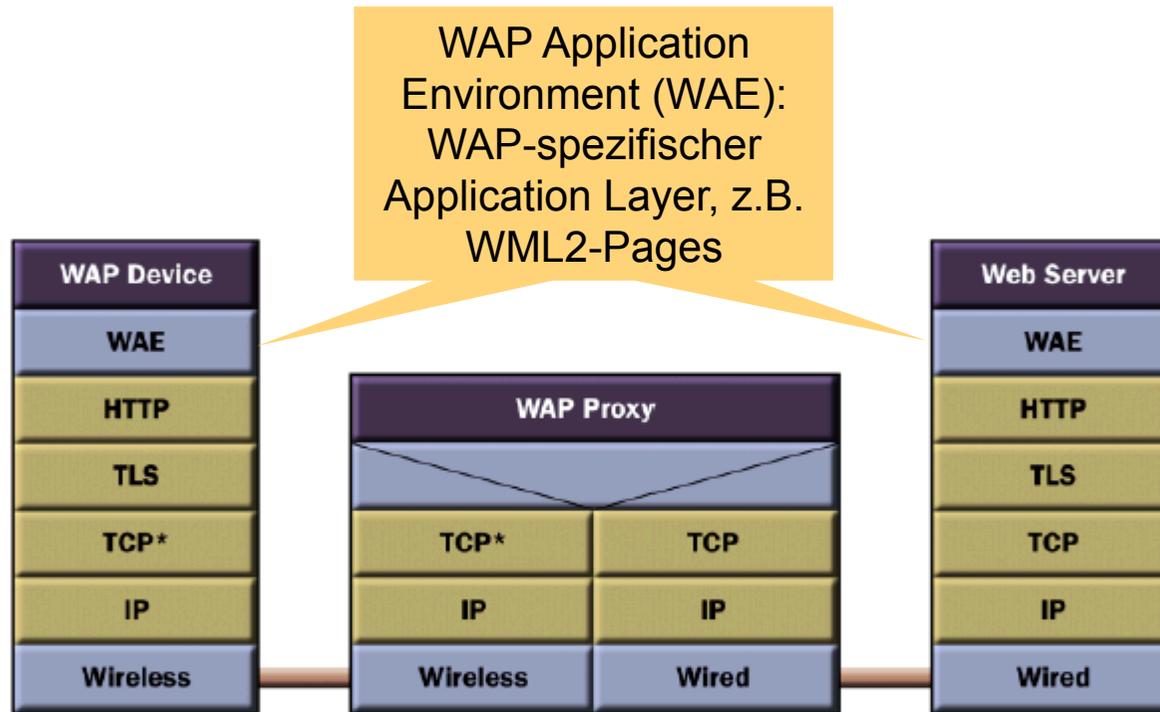
Ursprüngliches WAP-Modell:
Zwingend Proxy (WAP-Gateway) nötig.



Neues Modell:
Direkte Kommunikation mit Server über HTTP.

Quelle: WAP Forum

→ Konsequenz: Potentiell weniger Kontrolle für Netzbetreiber, aber grössere Ansprüche an Endgeräte.



WAP 2.0 Kommunikation zu Web-Server unter Verwendung eines WAP-Proxys.

Weitere Features (Auswahl)

- » WAP Push (über Push Proxy):
Effizientes Senden von Inhalten zu einem WAP-Device
- » User Agent Profile: Standardisiertes Übermitteln der Fähigkeiten eines Endgerätes an den Server
- » External Functionality Interface: Zugriff auf nicht-standardisierte Device-Fähigkeiten, z.B. GPS-Empfänger
- » Daten-Synchronisation: Kalender-Abgleich basierend auf SyncML
- » Pictograms: Standardisierte Icons, z.B. 😊

- » Das WAP-Forum hat seine Lektion gelernt und orientiert sich stärker an Enduser-Bedürfnissen und gängigen Internet-Standards.
- » Viele Ideen wurden von i-Mode aus Japan übernommen.
- » Erfolg ist daher deutlich wahrscheinlicher als bei WAP 1.1.
- » Verbleibende Hauptprobleme:
 - Schon wieder ein neuer Standard, den Endgerätehersteller und Informationsanbieter implementieren müssen
 - Grosse installierte Basis von WAP1.1-Geräten: Informationsanbieter müssen sich in der Praxis immer noch am alten Standard orientieren.

Weitere Informationen

- » <http://www.wapforum.org/>
- » <http://www.yes2wap.com/>
- » <http://www.w3c.org/>
- » <http://www.syncml.org/>



J2ME / Embedded Java

- » Java hat sich in den letzten Jahren als Sprache und Softwareumgebung breit durchgesetzt.
- » Laufende Weiterentwicklung durch Sun und den Java Community Process.
- » Java 2 ist in drei “Editions” aufgeteilt:
 - Java 2 Standard Edition (J2SE):
Applets und clientseitige Applikationen
 - Java 2 Enterprise Edition (J2EE):
Serverseitige Applikationen
 - Java 2 Micro Edition (J2ME):
Mobile Geräte und Consumer-Elektronik

Mögliche Endgeräte

Endgeräte in verschiedenen Bereichen werden immer intelligenter:

- » TV-Set-Top-Boxen
 - » Spielkonsolen
 - » PDAs (Palm, Pocket PC)
 - » Mobiltelefone und Pager
 - » GPS-Empfänger
 - » Navigationssysteme, Bord-Computer
 - » Videorecorder, Kühlschränke, ...
 - » Smart Cards, z.B. SIM Cards
- } 32-Bit-CPU
2 MB RAM oder mehr

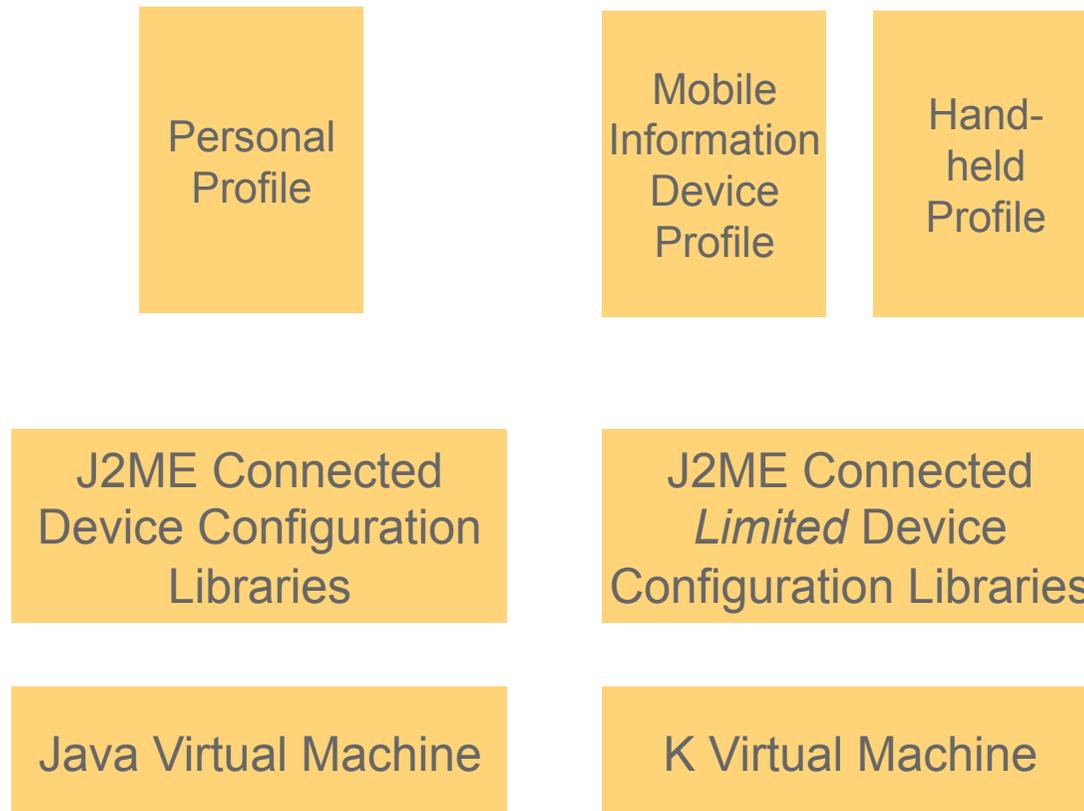
} 16- oder 32-Bit-CPU
<512 KB RAM

} 8-Bit-CPU
<16 KB RAM

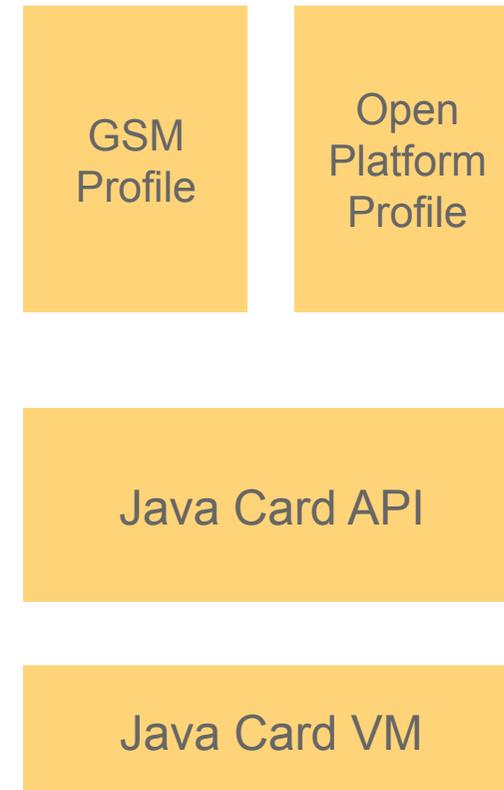
Überblick: Aufbau der J2ME-Umgebung und Ausprägungen für verschiedene Geräte



J2ME



Java Card



→ Für jede Geräteart bestehen geeignete Profile, Libraries/APIs und Virtual Machines

Stand heute: Kommerziell erhältliche Endgeräte mit Java-Support



PDA's: Auf allen gängigen Plattformen (Palm, PocketPC, Symbian) sind brauchbare Java-Implementationen verfügbar.

→ Personal Profile oder Handheld Profile



Mobiltelefone: Verfügbar auf einigen High-End-Geräten. Implementierte Standards und VMs aber noch sehr unterschiedlich.

→ Mobile Information Device Profile

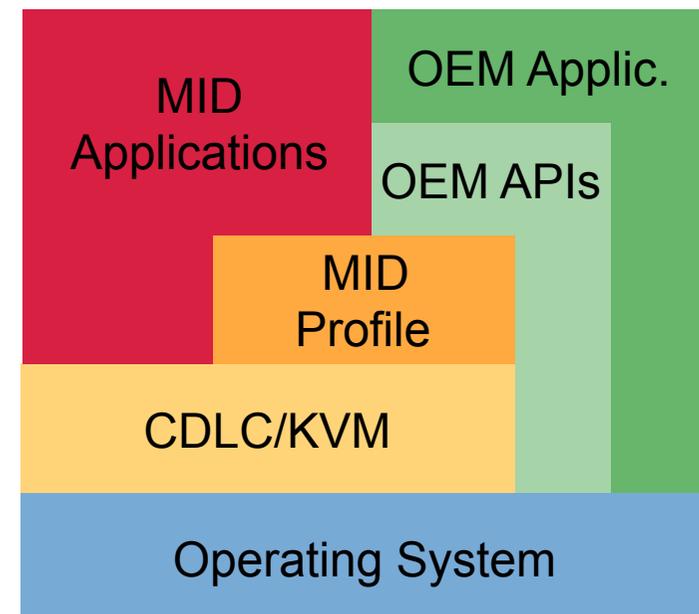
Mobile Information Device Profile (MIDP)

- » API für „kleine“ mobile Geräte
 - Kleines Display
 - Prozessor ca. 16 Bit/16 MHz, ca. 32 KB RAM
 - “Langsame” Netzwerkverbindung, z.B. GPRS

- » Basis: CLDC und K Virtual Machine
 - ca. 50-80 KB Objektcode
 - Anwendungen: “MIDlets”

- » Limitationen gegenüber J2SE: u.a.
 - Kein Java Native Interface (JNI)
 - Keine Custom Class Loaders
 - Einfachere Sandbox-Security

- » Zusätzliche Klassen:
 - Network Connectivity via Subset von HTTP
 - Anzeigefunktionalitäten
 - Einfache Datenbank
 - MIDlet-Verwaltung



Ergänzende Produkte und Initiativen

- » **Personal Java:** Heutige Version für grössere Geräte, wird abgelöst durch CDC/Personal Profile.
- » **Java Embedded Server**
 - Komplette kleine Serverumgebung für Devices
 - Inklusive HTTP- und Servlet-Service
 - Ziel: Ausstatten aller möglichen Geräte mit Netzwerk-Connectivity, Verwaltung per Web-Browser
- » **Java TV**
 - API mit Funktionalitäten für Digital-TV
- » ...plus diverse spezialisierte Profiles für J2ME



Stärken

- » Java als Sprache: flexibel und vielseitig
- » Breite Akzeptanz, viele Tools und Klassen-Libraries
- » Plattformunabhängigkeit
- » Eingebaute Kommunikationsfunktionalitäten

Schwächen

- » Nicht zu unterschätzende Komplexität für Entwickler
- » Ressourcenanforderungen an Devices immer noch relativ hoch
- » Performance-Einschränkungen. Klarer Nachholbedarf im Realtime-Bereich.
- » Implementierungen noch frisch, Reifegrade noch nicht perfekt. Grosse Vielfalt an Varianten

→ Der Hauptkonkurrent, Microsoft Windows CE, verfügt über eine schon viel grössere installierte Basis, hat aber dafür andere Schwächen (Grösse, Komplexität, Offenheit).

- » <http://java.sun.com/j2me/>
- » <http://www.javamobiles.com/>
- » <http://www.borland.com/jbuilder/mobileset/>
- » <http://forum.nokia.com/>
- » <http://www.ericsson.com/mobilityworld/>



XML Security



XML (Extensible Markup Language)

- » Methode, strukturierte Daten in Text-Datei zu speichern, zu transportieren, zu...
- » Gute lesbar, sprechend, keine vordefinierten Tags
- » Automatisierbare Validitätsprüfung und Transformation (DTD, MSL-Schema, XSLT...)
- » Lizenzfrei, technologieneutral
- » Basis für eine Familie von Technologien

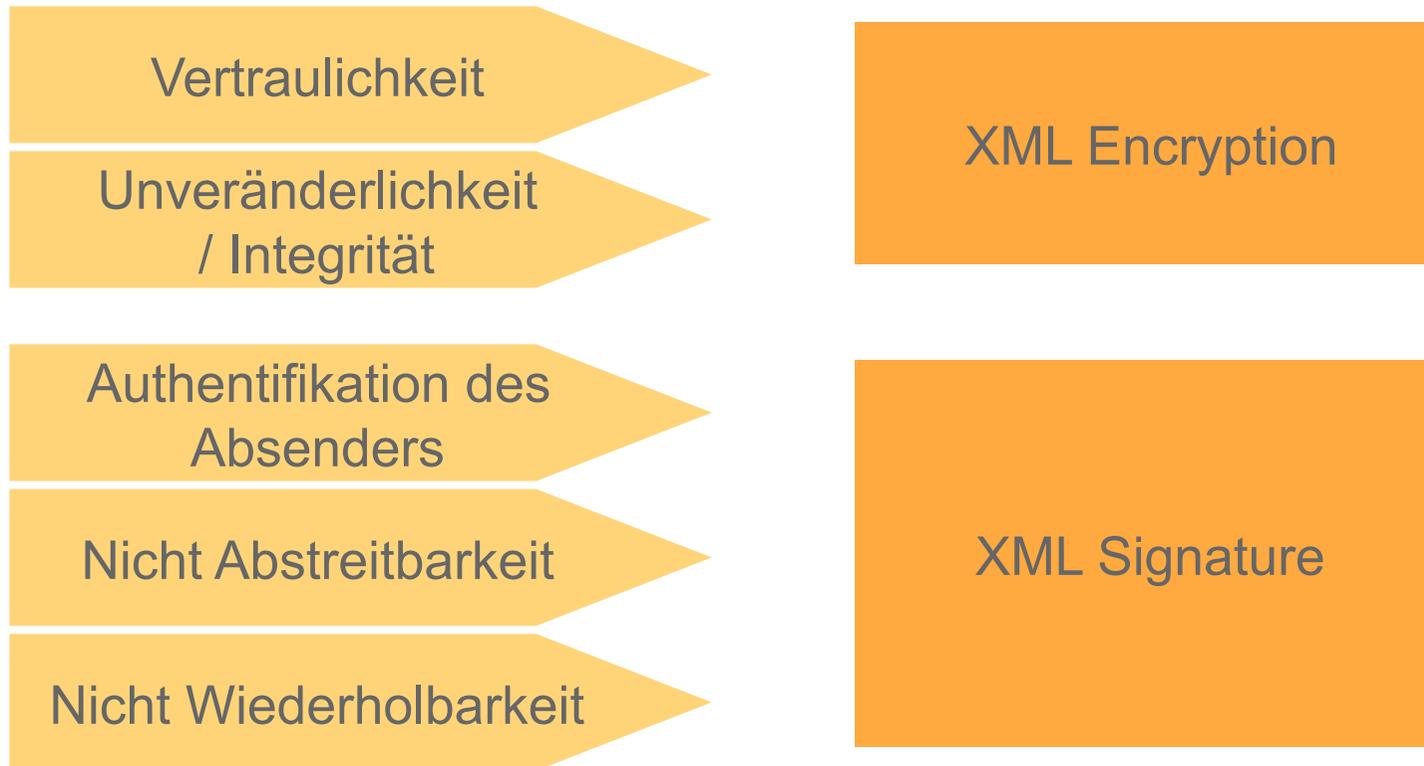


Bedeutung von XML

- » XML ist aus der eBusiness-Welt (und der IT) nicht mehr wegzudenken
- » Teil oder Grundlage für fast alle neueren Standards
- » Häufigste Verwendungen:
 - Content Management: Medienneutrale Datenhaltung
 - Systemintegration: Kommunikation zwischen Software-Komponenten, auch über System- und Netzwerkgrenzen hinweg (Bsp: SOAP)
 - eCommerce: Codierung von Geschäftsdokumenten, z.B. Bestellungen, Rechnungen, usw.

Grosser
Bedarf nach
Sicherheit!

Sicherheitsanforderungen an eine XML-Message



- » W3C entwickelt mit XML Encryption und XML Signature die nötigen Standards für sichere Kommunikation per XML.

- » Verschlüsselung von XML-Kommunikation könnte auch auf Netzwerk- oder File-Ebene gelöst werden.
 - Kommunikation mit SSL/TSL
 - XML-File direkt verschlüsseln

- » Zielsetzung von XML Encryption
 - End-zu-end Ansatz
 - Vorteile einer XML-Nachricht im Klartext erhalten (Effizienz, standardisierte Verarbeitbarkeit usw.)
 - Verschlüsselung nur einzelner Teile der Nachricht ermöglichen

XML Encryption: Code-Beispiel

Klartext:

```
<?xml version='1.0'?>
  <PaymentInfo xmlns='http://example.org/paymentv2'>
    <Name>John Smith</Name/>
    <CreditCard Limit='5,000' Currency='USD'>
      <Number>4019 2445 0277 5567</Number>
      <Issuer>Bank of the Internet</Issuer>
      <Expiration>04/02</Expiration>
    </CreditCard>
  </PaymentInfo>
```

Verschlüsselt:

```
<?xml version='1.0'?>
  <PaymentInfo xmlns='http://example.org/paymentv2'>
    <Name>John Smith</Name/>
    <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
      xmlns='http://www.w3.org/2001/04/xmlenc#'>
      <CipherData>
        <CipherValue>A23B45C56E8984BC3A83F32</CipherValue>
      </CipherData>
    </EncryptedData>
  </PaymentInfo>
```

- » Standard für digitales Signieren von XML-Dokumenten.
- » Berücksichtigt, dass zwei XML-Dokumente textlich unterschiedlich, aber logisch identisch sein können.
 - Verwandlung in Canonical XML
- » Kann Kontrollsummen über einzelne Teile des Dokuments rechnen, Signatur (mit Private Key) über Sammlung der Kontrollsummen.
- » Verwendet etablierter Kryptographiestandards



Einfache Bestellung

```
<order Id="order">
  <item>
    <title>XML and Java</title>
    <price>100.0</price>
    <quantity>1</quantity>
  </item>
  <cardinfo>
    <name>Your Name</name>
    <expiration>04/2002</expiration>
    <number>5283 8304 6232 0010</number>
  </cardinfo>
</order>
```



XML Signature: Code-Beispiel

Bestellung mit Signatur

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="#order">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/..." />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>345x3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
    <Object>
      <order Id="order">
        <item>
          <title>XML and Java</title>
          ...
        </item>
      </order>
    </Object>
  </Signature>
```

verwendeter Algorithmus

Hash über Objekt „Order“

Message Authenticator (signierter Hash) über gesamtes Dokument

- » Private Keys können mit verschiedenen Algorithmen und PKIs erstellt und verwaltet werden: X.509, PGP, SPKI, ...
- » XML Signature verwendet das Element KeyInfo zum Transport.
Beispiel:

```
<KeyInfo>
  <X509Data> <!-- certificate chain -->
    <!--Signer cert, issuer CN=arbolCA,OU=FVT,O=IBM,C=US, serial 4-->
    <X509Certificate>MIICXTCCA..</X509Certificate>
    <!-- Intermediate cert subject CN=arbolCA,OU=FVT,O=IBM,C=US
      issuer CN=tootiseCA,OU=FVT,O=Bridgepoint,C=US -->
    <X509Certificate>MIICPzCCA...</X509Certificate>
    <!-- Root cert subject CN=tootiseCA,OU=FVT,O=Bridgepoint,C=US -->
    <X509Certificate>MIICSTCCA...</X509Certificate>
  </X509Data>
</KeyInfo>
```

- » XML Encryption: Working Draft 18.10.01
- » XML Signature: Proposed Recommendation 20.8.01
- » Bereits mehrheitlich akzeptiert und zunehmend adaptiert von meisten Herstellern
 - Aufgenommen im Java Community Process
 - Basis für Microsoft Web Services Security
 - XML Security Suite von IBM
 - usw.

- » <http://www.w3.org/Encryption/2001/>
- » <http://www.w3.org/Signature/>
- » http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html
- » <http://www-106.ibm.com/developerworks/xml/library/s-xmlsec.html/index.html>
- » <http://msdn.microsoft.com/ws/2001/10/Security/>



Web Services



„Web Services“: Buzzword des Jahres

Defining Web Services

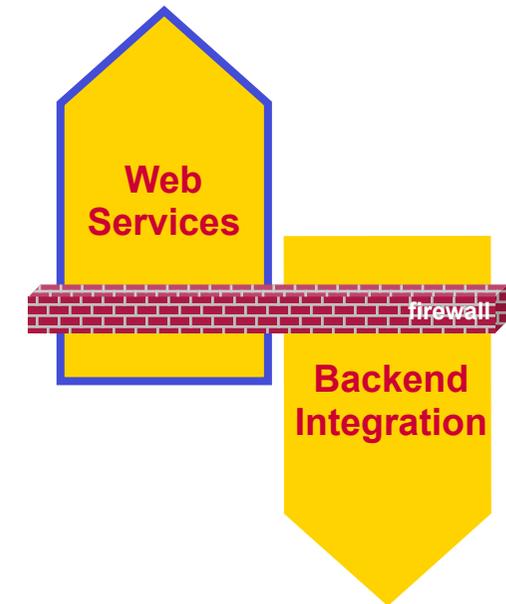
(June 2001) The label "web services" is incredibly generic. Like any promising and loosely defined technology trend, the concepts it describes will be subject to a great deal of speculation and bandwagoning in the months to come.

By Brent Sleeper and Bill Robins.

- » Web Services sind eine Sammlung von neuen Standards, die eine service-orientierte, komponentenbasierte Applikationsarchitektur beschreiben.
- » Konzeptionell helfen Web Services dabei, komplexe e-Business-Prozesse über mehrere Systeme und mehrere Partner zu verteilen.

Web Services

- » sind Schnittstellen von wiederverwertbare und lose gekoppelte Softwarekomponenten
- » offerieren eine semantisch gekapselte, diskrete Funktionalität
- » werden von Programmen, nicht direkt von Usern benutzt
- » werden über das Internet mit etablierten Protokollen wie http(s) oder auch E-Mail (smtp) verteilt



Der bekannteste Web Service: Microsoft Passport



- » Zentrale Userverwaltungs-Infrastruktur für dezentrale Anwendungen.
- » Stark gestützt von Microsoft mit Hotmail, Windows XP und anderen Produkten.
- » Erster Baustein der .NET My Services (Hailstorm)-Strategie.
- » Microsoft begegnet Kritik mit Versuch einer Dezentralisierung.



Geplante Microsoft .NET My Services



Abdeckung unterschiedlichster Anwendungsbereiche:

- » myAddress: Elektronische und geografische Adresse
- » myProfile: Name, Daten, Bild etc.
- » myContacts: Adressbuch
- » myNotifications: Abonnieren von Benachrichtigungen aller Art
- » myInbox: Inbox für e-Mail und Voice-Mail
- » myCalendar: Kalender- und Tasklistenverwaltung
- » myDocuments: Dokumentenspeicherung online
- » myApplicationSettings: application settings
- » myWallet: Zahlungsmittel, z.B. Kreditkartennummern

Technische Kernstandards für Web Services

- » HTTP(S): Grundlegendes synchrones Kommunikationsprotokoll
- » XML: Meta-Standard für Informationscodierung (Daten und Funktionen)
- » SOAP (Simple Object Access Protocol): Zugriff auf verteilte Programmobjekte
- » WSDL (Web Service Definition Language): Beschreibung der Eigenschaften und Schnittstellen eines Web Service
- » UDDI (Universal Description, Discovery and Integration): Verzeichnisdienst für Web Services

SOAP (Bsp. einer Request Nachricht)



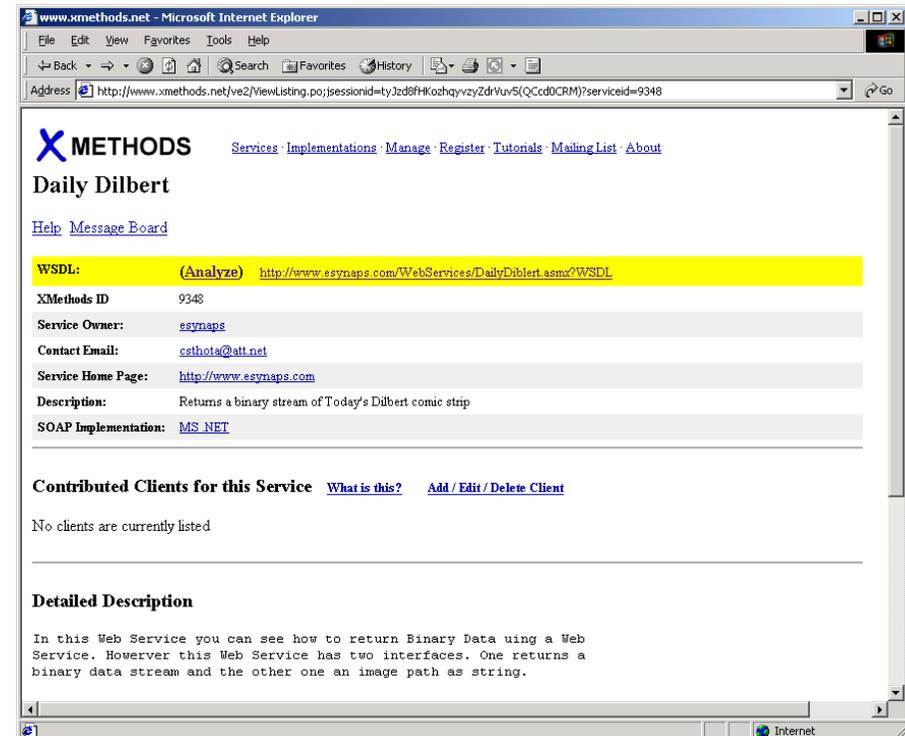
```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV=
    "http://www.w3.org/2001/06/soap-envelope"
  SOAP-ENV:encodingStyle=
    "http://www.w3.org/2001/06/soap-encoding">

  <SOAP-ENV:Body>
    <m:GetLastTradePrice xmlns:m="Some-URI">
      <symbol>DIS</symbol>
    </m:GetLastTradePrice>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

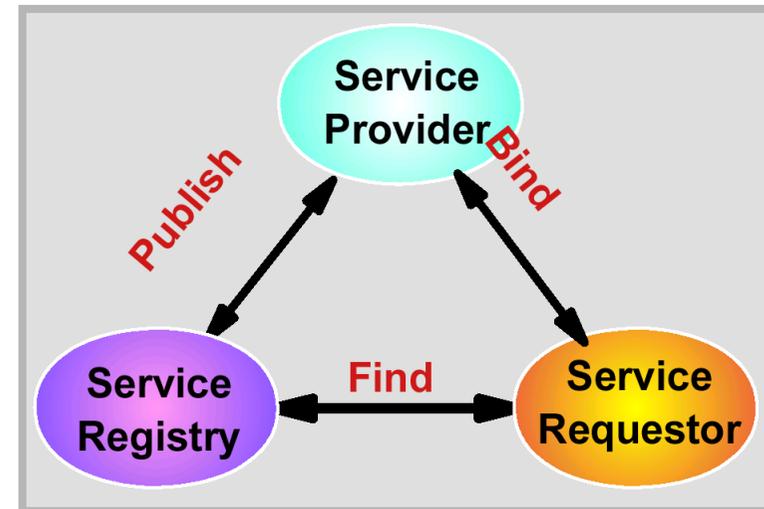
message

SOAP envelope

- » Beschreibt einen Web-Service
- » Elemente:
 - Verwendete (komplexe) Datentypen
 - Verwendete Nachrichtentypen
 - Ports: mögliche Nachrichten-Kombinationen
 - Kommunikationsoperationen (Request-Response, One-Way usw.)
 - Serveradressen, Details von Message-Formaten und Protokollen (z.B. HTTP, SMTP usw.)



- » „Telefonbuch für Web Services“:
Spezifikation für verteilte, web-
basierte Verzeichnisse von Web
Services.
- » Suchbar durch User oder
zugreifbar für Programme (als Web
Service über SOAP natürlich)
- » Konkrete Verzeichnisse können
von mehreren Anbietern betrieben
werden.
Beispiele:
 - <https://www-3.ibm.com/services/uddi/protect/home.jsp>
 - <http://uddi.microsoft.com/>



Bewertung von Web Services

Vorteile:

- » Sprach- und plattformunabhängig: Interface abstrahiert von der Implementationsprache und der Runtime-Umgebung
- » Netzwerkoptimiert: Ausgelegt auf Betrieb über das Internet
- » Starke Unterstützung fast aller Hersteller

Nachteile:

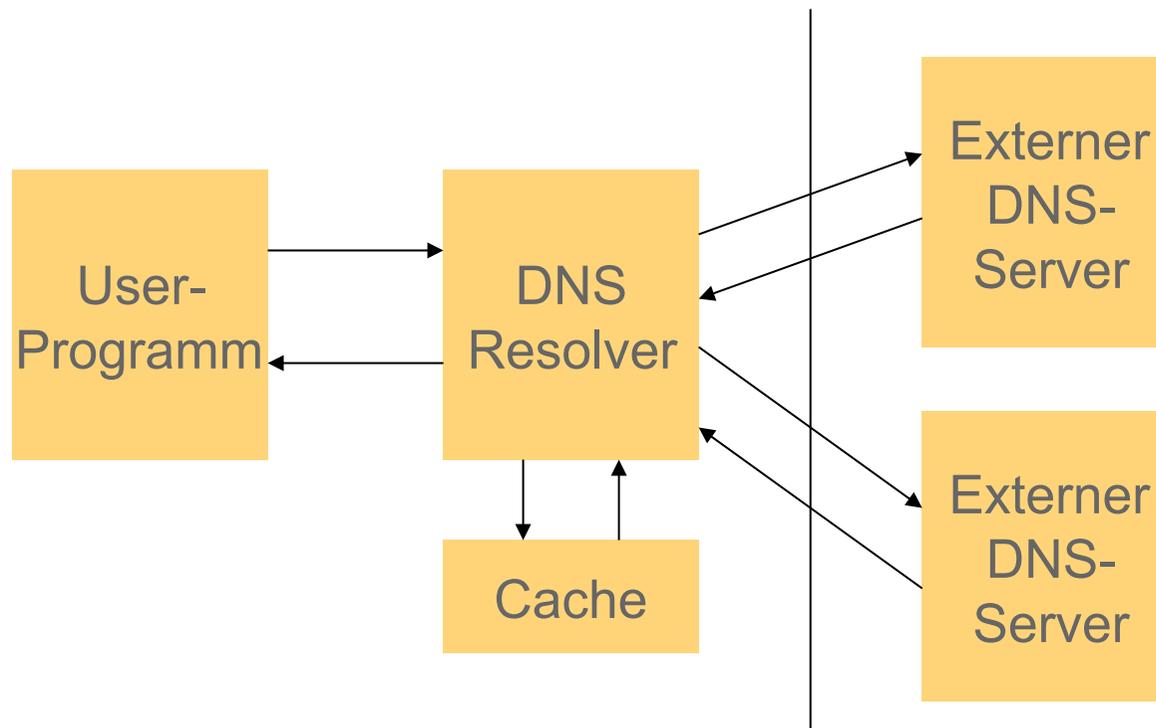
- » Noch sehr junge Technologie, stark überhyped.
- » Noch keine wirklich stabilen Implementationen.

- » <http://www.w3.org/TR/SOAP/>
- » <http://www.w3.org/TR/wsdl/>
- » <http://www.uddi.org/>
- » <http://www.xmethods.net/>
- » <http://www.microsoft.com/webservices/>
- » <http://java.sun.com/webservices/>
- » <http://www-106.ibm.com/developerworks/webservices/>



Neue DNS-Features

- » Grundfunktion:
Umwandlung von Klartextadressen (z.B. <http://www.iex.ch/>)
in numerische IP-Adressen (z.B. 193.247.126.215)



- » Ungenügende Sicherheit: Schutz gegen Manipulationen nur unzureichend.
- » Direkte Zuweisung Name → physische IP-Adresse macht Netzstrukturänderungen schwierig.
- » Ursprünglich keine Unterstützung von IPv6-Adressen
- » Keine Unterstützung internationaler Zeichensätze

- » Verhindern von Manipulationen wie DNS Spoofing.
- » Sicherstellen von Echtheit und Integrität von DNS-Daten.
- » Nicht zu verwechseln mit Zugriffsschutz. Grundprinzip: DNS-Daten sind öffentlich, alle Anfrager bekommen gleiche Antwort.
- » Methode: Signaturen mit Private-Public-Key-Verschlüsselung
 - Digitale Signatur für jeden DNS-Eintrag.
 - Resolver prüft die Signatur, bevor ein Eintrag akzeptiert wird.

» Traditionell:

- Resolver muss „wissen“, wie der Server für einen bestimmten Dienst in einer Domain heisst.
- Port-Nummern sind per Konvention festgelegt oder müssen explizit angegeben werden.
- Beispiel: Mail-Server muss explizit konfiguriert sein.

» Neu:

- Allgemeine Anfrage nach Dienst
- DNS der Domain kann verschiedenen Servern Prioritäten zuweisen → Load Balancing, flexibles Umkonfigurieren

» Beispiel:

- Anfrage nach `_ldap._tcp.example.com` liefert einen LDAP-Server, der TCP unterstützt.

- » IPv6: Der neue IP-Standard mit erweitertem Adressraum
- » Derzeit zwei vorgeschlagene Standards:
- » AAAA (RFC 1886): äquivalent zu traditioneller Methode mit A-Record
N AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
- » A6 (RFC 2874): Erweiterte Version
 - Fragmentierte Adressspeicherung für einfachere Verwaltung komplexer Netzwerkstrukturen
- » AAAA ist bereits breit verfügbar, A6 stösst eher auf Zurückhaltung wegen grosser Komplexität.

Internationalized Domain Names

» DNS unterstützt bisher nur ASCII-7Bit

» Starker Wunsch nach Zulässigkeit internationaler Zeichen:
<http://www.zürich.ch/> statt
<http://www.zuerich.ch/>

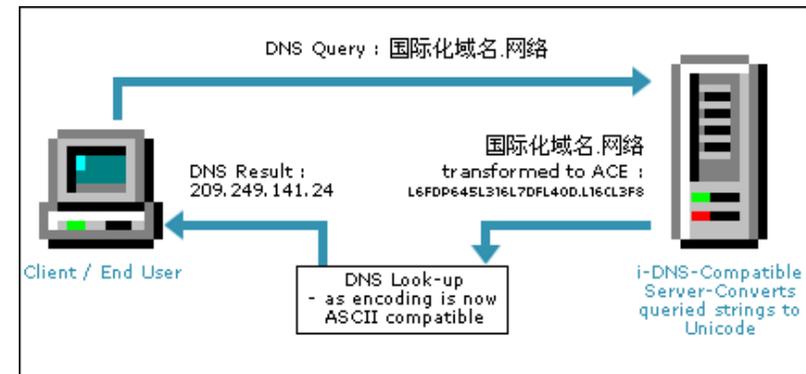
» Schwierigkeiten:

- Koexistenz mit älterer DNS-Software
- Verschiedene Codierungen sind möglich (insb. ACE)
- Viele Sicherheitsmechanismen basieren auf DNS-Namen → potentielle Sicherheitslöcher
- Ohne stabilem DNS läuft das Internet nicht

» Working Group der IETF arbeitet an Standards

» Testbed von Verisign

- Phase 1: Vorbereitung der Domain-Registatoren
- Phase 2: Registration von nicht-englischen Domains
- Phase 3: Auflösung von nicht-englischen Namen

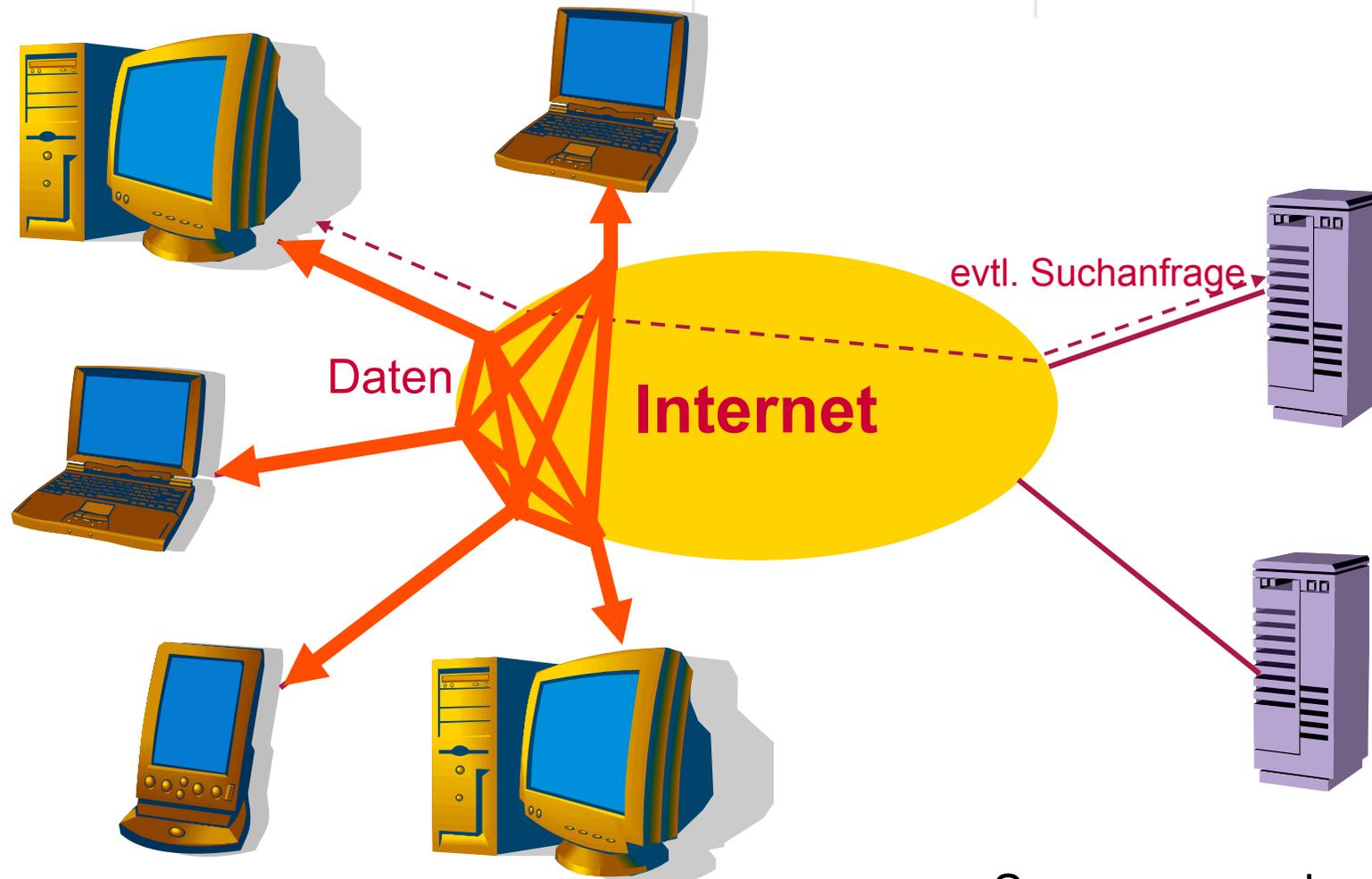


- » <http://www.ietf.org/html.charters/dnsex-charter.html>
- » <http://www.ietf.org/rfc.html>
- » <http://www.i-d-n.net/>
- » <http://www.dnsii.org/>
- » <http://www.verisign-grs.com/idn/index.html>
- » <http://www.w3.org/2000/Talks/0717-mldns/Overview.html>



JXTA (Juxtapose) und P2P-Standards

Das Prinzip von Peer-to-Peer (P2P): Gleichwertige Netzteilnehmer



Intelligente Clients („Peers“), die direkt kommunizieren

Server nur noch als Vermittlungsstelle, evtl. gar nicht mehr benötigt

Haupttypen von P2P



Datenzentriert:
Content
Sharing

Austausch von
Multimedia-Files,
Dokumenten etc.

Beispiel:
Napster,
Morpheus,
Gnutella

Computerzentriert:
Resource
Sharing

Gemeinsame Nutzung
brachliegender
Rechnerkapazität

Beispiel:
SETI@Home

Userzentriert:
Collaborative
Computing

Online-Zusammenarbeit
über Instant Messaging
und Shared
Workspaces

Beispiele:
ICQ, MS Messenger,
Groove

Send/receive:
Austausch der Nutzdaten

Lookup:
Inhalte/Resourcen/User finden

Discover:
Peers finden

Authenticate:
Login, Identität und Adresse etablieren

Offene Protokolle und P2P-Plattformen

- » Bisher: Fast alle P2P-Systeme verwenden eigene, proprietäre Protokolle → Ineffizient für Entwickler!
- » Darum: Trend zu gemeinsamen Protokollen und offenen Standards
- » Vorteile:
 - Flexible und ausbaufähige Architekturen
 - Interoperabilität
 - Massive Zeitersparnis für Entwickler von P2P-Applikationen
 - Breite Auswahl an Tools und Modulen
- » Problem:
 - Wer definiert die Standards?
 - Standard-Organisationen (W3C, IETF) sind nicht sehr aktiv
 - Industriekonsortien, z.B. Peer-to-Peer Working Group, stehen noch am Anfang



Wichtige Player bei P2P-Standards

- » Intel: PtPTL (Peer-to-peer Trusted Library)
 - Geht Sicherheitsproblematik und Infrastrukturdienste an
 - Derzeit in Alpha-Version

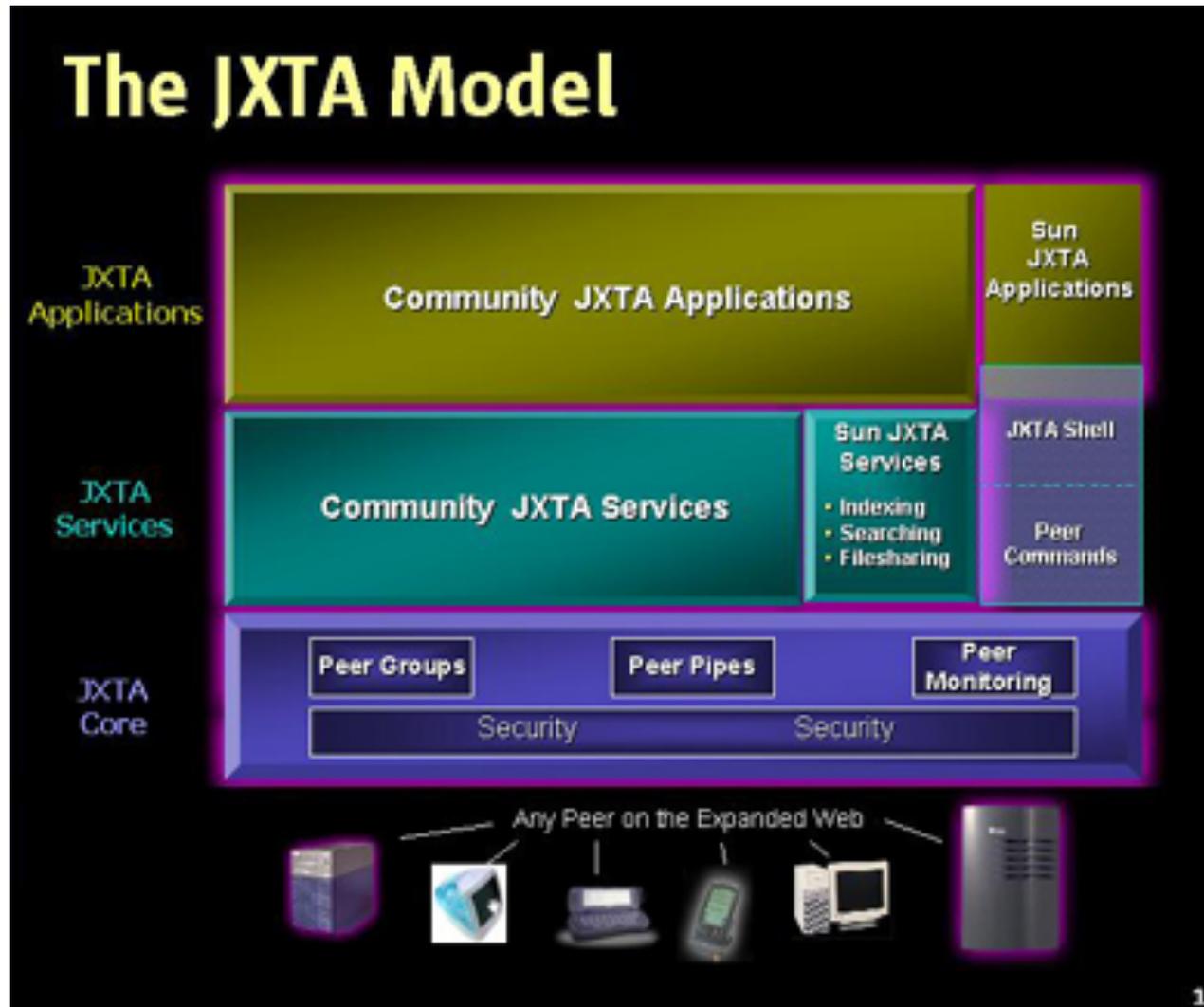
- » Microsoft .NET
 - P2P-Services sind auch Teil des .NET-Frameworks
 - Module: Passport (Authentisierung), .NET My Services, Messenger, .NET Framework, Visual Studio.NET
 - Problem: Geringe Akzeptanz

- » Sun: JXTA (Juxtapose)



JXTA (Juxtapose)

- » Forschungsprojekt von Sun Microsystems
- » Ziel: Satz von gemeinsamen Protokollen für P2P.
Abstraktes Schichtenmodell für P2P-
Applikationsentwicklung
- » Verfügbar in erster Java-Implementation
 - `net.jxta` und `net.jxta.impl`



Quelle: SUN



JXTA-Schichtenmodell

- » Hardware: PCs, PDAs, Handies etc.
- » Runtime-Umgebung oder Virtual Machine
 - Vorerst Java, später weitere Technologien
- » JXTA-Technologielayer
 - Peer Groups: Zugehörigkeit der User zu Gruppen
 - Peer Pipes: Kommunikationskanäle zwischen Peers
 - Peer Monitoring: Überwachung, Benutzungsstatistik etc.
- » Peer Services Layer
 - Raum für verschiedene Dienste, z.B. Suche, Filesharing, Indexierung etc.
 - Referenzimplementation: Suns JXTA Shell
- » Peer Applications
 - Eigentliche Anwendungen mit Benutzerschnittstelle, z.B. File-Sharing à la Napster

- » Alles natürlich XML-basiert

- » Grundprotokolle:
 - Peer discovery: Existenz von Peers und Services entdecken
 - Peer resolver: Adresse anderer Peers finden
 - Peer information: Angaben über Peers
 - Peer membership: Mitgliedschaft in Gruppen managen
 - Pipe binding: Kontaktaufnahme für Datenaustausch
 - Peer endpoint routing: Weiterleitung über Zwischenstationen

Bedeutung von JXTA

- » Zukunft von P2P dürfte in der Integration in andere Applikationen liegen
- » Darum: Offene Standards und Entwicklungsplattformen sind wichtig
- » JXTA ist der bisher konsistenteste Ansatz in diesem Bereich
 - Umfassend
 - Offen bzgl. Grundtechnologien
 - Schwäche: Authentisierung und Security nur am Rand behandelt
 - Befindet sich noch in einer sehr frühen Phase



Weitergehende Informationen

- » Projekt JXTA: <http://www.jxta.org/>
- » P2P allgemein:
 - <http://www.openp2p.com/> (O 'Reilly)
 - <http://www.peer-to-peerwg.org/> (P2P Working Group)
- » Die Konkurrenz: <http://www.microsoft.com/hailstorm/>
- » Bücher:
 - Oram, Andy (ed.): Peer-to-Peer: Harnessing the Power of Disruptive Technologies. O 'Reilly, 2001.
 - Barkai, David: Peer-to-Peer Computing. Intel Press, 2001



Device Independence

Immer mehr Gerätetypen werden Internet-fähig



Spielkonsolen



PDA's, Handies und andere mobile Geräte



Einfache und billige, PC-ähnliche Geräte

Neue PC-Formate, z.B. Tablet PC



Internet-Kühlschrank (Pilotversuch in Dänemark)





Unterschiede zwischen Geräten

- » Standard-PC: Nur kleine Unterschiede
 - *Relativ* eingeschränkte Vielfalt an Varianten
 - Meistens keine ernsthaften Speicher- und Geschwindigkeitslimitationen für Web-Darstellung

- » Neue Internet-Devices: Grosse Unterschiede
 - Display: zwischen 32x96 Pixel schwarzweiss und normaler PC-Auflösung
 - Prozessor: zwischen 8 MHz/8 Bit und Pentium III
 - RAM: zwischen wenigen KByte und einigen MB
 - Netzgeschwindigkeit: Zwischen 9.6kbit/s und Breitband
 - Stark unterschiedliche Browser, Betriebssysteme, unterstützte Programmiersprachen usw.

Aktivitäten des W3C (World Wide Web Consortium)

- » „Universal Access“ mit beliebigen Geräten ist eins der sieben Hauptziele des W3C
- » Die „Device Independence Working Group“ kümmert sich um die Erarbeitung entsprechender Standards.
- » Untergruppen:
 - TV & the Web
 - Mobile Access
 - CC/PP (Composite Capability/Preference Profiles)
- » Benachbarte Themen:
 - Web Accessibility Initiative (Zugriff für Behinderte)
 - Internationalization Activity

Grundprinzipien (Zusammenfassung)

- » Device independent access:
Zugriff über jedes beliebige Gerät soll möglich sein.
- » Device independent web page identifiers:
Adressen (URLs/URIs) sollen für gleichen Inhalt identisch sein, unabhängig vom Zugriffsmechanismus
- » Fehlermeldungen:
Falls der Zugriff auf einen Inhalt über ein bestimmtes Gerät nicht sinnvoll möglich ist, muss eine konsistente Fehlermeldung geliefert werden.
- » Customization:
Falls vom Autor gewünscht, soll der User die Art der Anzeige eines Inhalts beeinflussen können.
- » Delivery Context/Preferences:
Die Art der Lieferung von Inhalten soll abhängig von den Umständen (z.B. Netzbandbreite) beeinflusst werden können. Der User soll das auch selbst einstellen können.



Definition des Delivery Context

- » Zentraler Standard:
CC/PP (Composite Capability/Preference Profiles)
- » Basiert auf RDF / XML (Resource Description Format)
- » Angaben:
 - Client Hardware / Software / Softwareversionen
 - Unterstützte HTML-Versionen
 - Proxy-Details (z.B. verbotene Dateitypen)



CC/PP Profil-Beispiel (gekürzt)

```
<?xml version="1.0"?>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
        xmlns:ccpp="http://www.w3.org/2000/07/04-ccpp#">
  <rdf:Description rdf:about="MyProfile">

    <ccpp:component>
      <rdf:Description rdf:about="TerminalHardware">
        <rdf:type rdf:resource="HardwarePlatform" />
        <display>320x200</display>
        <memory>16Mb</memory>
      </rdf:Description>
    </ccpp:component>

    <ccpp:component>
      <rdf:Description rdf:about="TerminalSoftware">
        <rdf:type rdf:resource="SoftwarePlatform" />
        <name>EPOC</name>
        <version>2.0</version>
        <vendor>Symbian</vendor>
      </rdf:Description>
    </ccpp:component>

    [...]
  </rdf:Description>
</rdf:RDF>
```

- » Mehrere HTML-Source-Files, je eines pro Ausgabeformat, Zuweisung durch den Server
- » Style Sheets (z.B. CSS, XSL):
Umwandlung auf dem Client
- » Transformation (XSLT):
Umwandlung auf dem Server
- » Dynamisch programmierte Seiten (z.B. JSP)

- » Das Problem wird zunehmend akuter, je mehr Geräte Internet-fähig werden.
 - Die Erfahrungen bei WAP haben gezeigt, dass schlechte Implementationen bei Browsern und Geräte die Content-Erstellung massiv hindern können.

- » Technologie-Situation sieht nicht vielversprechend aus
 - Die technischen Standards (inkl. CC/PP) stecken noch in den Kinderschuhen.
 - Tools für eine wirklich effiziente Implementierung gibt es kaum.

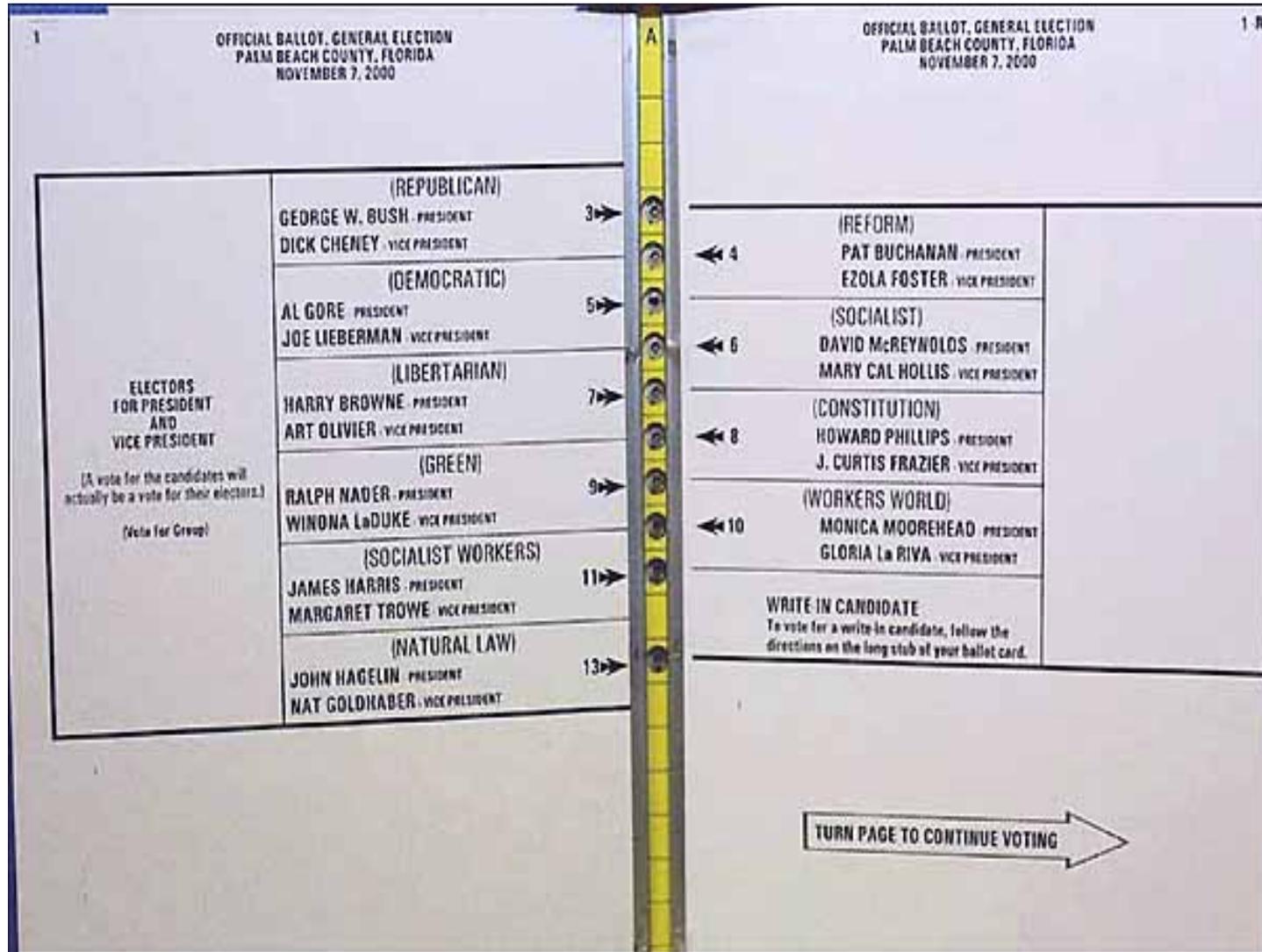
- » Wichtigste Empfehlung für Web-Developer:
Content und Layout strikt getrennt halten (z.B. über XML oder ein CMS)

- » <http://www.ccpp.org/>
- » <http://www.w3.org/2001/di/>
- » <http://www.w3.org/TR/CCPP-struct-vocab/>



Universal Usability

Usability ist nicht nur im Web ein Thema...



Nächstesmal lieber so?

namics



Universal Usability: Das Problem

- » Das Web wird immer wichtiger als Medium...
 - Information und Kommunikation in der Geschäftswelt und privat
 - Bald auch für Bürgerrechte und -pflichten: eGovernment, Schulen ans Netz, ...

- » ...aber ist für viele immer noch viel zu schwierig zu bedienen
 - Relativ hoher Lernaufwand für PC-Bedienung
 - Zurechtfinden im Internet ist schwierig
 - Rein praktische Bedienungsprobleme für ältere Leute und Behinderte (Maus, Schriftgröße usw.)
 - Viele Sites sind ausgelegt für High-End-PCs und -Zugriffsmechanismen

Forderung nach Universal Usability

- » Forderung: Internet sollte **für alle** zur Verfügung stehen, unabhängig von Alter, Behinderungen, Einkommen, kulturellem Hintergrund oder anderen Rahmenbedingungen.
- » Web-Designer als Informationsanbieter tragen hierbei eine wesentliche Verantwortung!
- » Für Bereiche wie eGovernment ist Universal Usability unbedingte Voraussetzung...
- » ... aber auch wichtig im kommerziellen Bereich.

Herausforderungen für universelle Benutzbarkeit einer Website

namics



Computer-Skills
des Users

Wissen über jeweiliges
Thema

Sprachkenntnisse

Alphabetismus

Einkommen

Technische Ausstattung

Behinderungen:
Visuell, auditiv,
motorisch, kognitiv

Behindernde Umstände:
Mobilität, Verletzungen,
Lärm, ...

Persönlichkeits-
eigenschaften

Kultureller
Hintergrund

Benutzbar für jeden?



» In verschiedenen Ländern gibt es bereits Vorschriften oder Empfehlungen für die Gestaltung öffentlicher Websites.

» Beispiel: US Rehabilitation Act, Section 508

» Schweizer Seiten: www.admin.ch weitgehend OK, www.parlament.ch nicht.

- » Web Accessibility Initiative (WAI) des W3C:
„WAI, in coordination with organizations around the world, pursues accessibility of the Web through five primary areas of work: technology, guidelines, tools, education and outreach, and research and development.”

- » Aktivitäten:
 - Review aller neuen W3C-Standards
 - Guidelines für Content, Authoring Tools und User Agents/Browser:
z.B. Web Content Accessibility Guidelines 1.0
 - Ausbildungsmaterial und Veranstaltungen

WAI Web Content Accessibility Guidelines: Einige Grundregeln



1. Immer Alternativen zu visuellem und auditivem Content anbieten (z.B. ALT-Tags)
2. Text und Grafik müssen auch ohne Farbe funktionieren
3. Trennung zwischen Struktur und Layout: Style Sheets richtig verwenden
4. Richtige Sprachcodierung für Output mit Sprachsynthesizern oder Braille
5. Vernünftiger Einsatz von Tables (für tabellarische Daten, nicht für Layout)
6. Alternativen für Seiten mit neuen Technologien anbieten
7. Animationen, Blinken und Auto-Updates abschaltbar machen.
8. Design für Geräteunabhängigkeit (Device Independence) ausrichten.
9. Klare und verständliche Struktur für Seiten und Navigation.

Überprüfungstool: Bobby

namics



» Prüft auf WAI- oder US 508-Compliance

» Gibt konkrete Verbesserungsvorschläge

<http://www.cast.org/bobby/>

- » <http://www.w3.org/WAI/>
- » <http://www.access-board.gov>
- » <http://www.cast.org/bobby/>
- » Shneiderman, Ben: “Universal Usability”, Communications of the ACM, May 2000.



Flash-Erweiterungen

Verbreitung von Flash

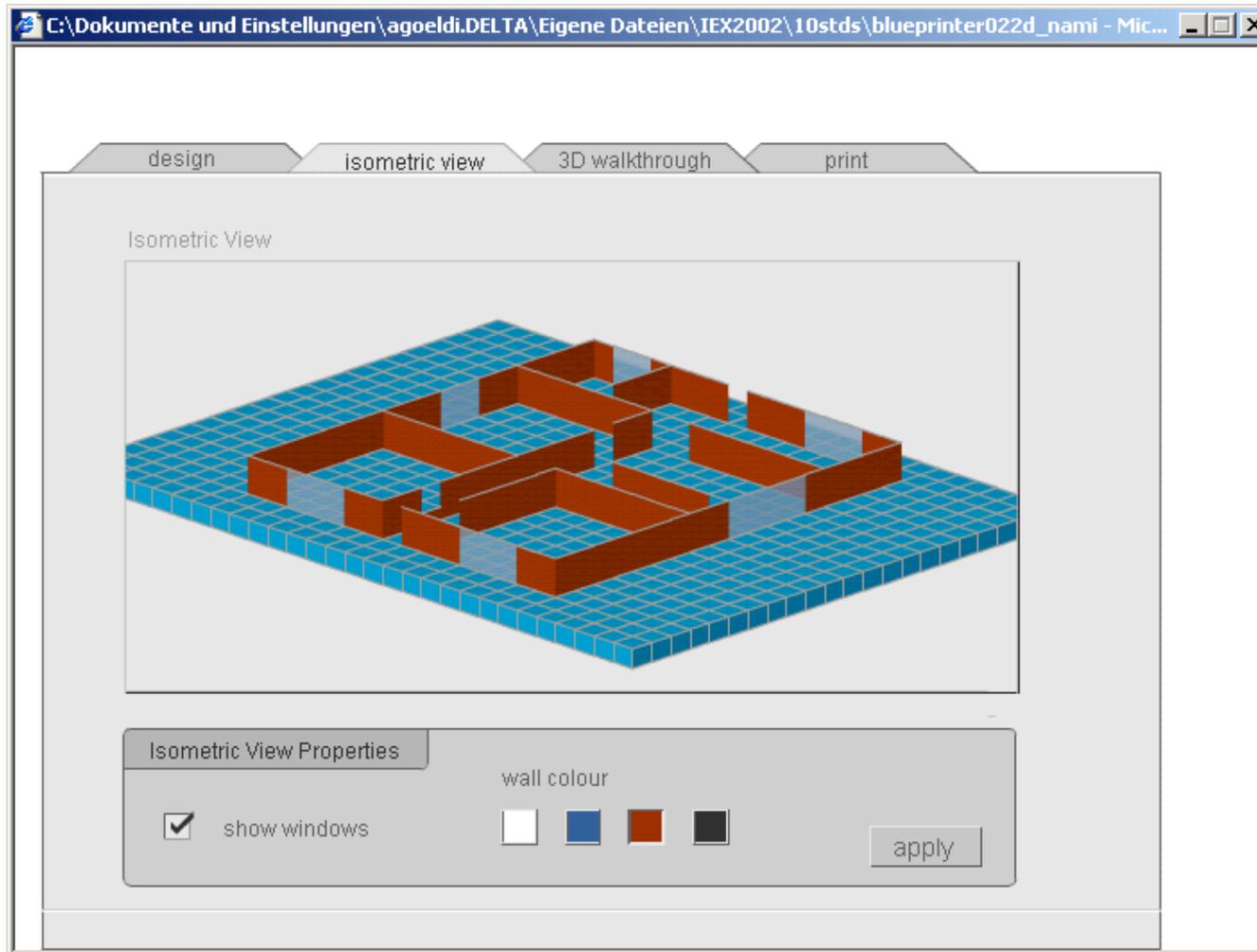
- » Macromedia Flash hat sich als Plattform für Web-Animation breit durchgesetzt. Aktuelle Version: 5.0
- » Flash ist (laut Hersteller) auf 96% aller Web-PCs verfügbar.
- » „Klassische“ Einsatzgebiete:
 - Animierte Intros
 - Consumer-orientierte Werbe-Sites
 - Animierte Werbebanner
 - Online-Spiele
- » Flash bietet aber viel weitergehende Features, die für fortgeschrittene Web-Developer interessant sind.

Flash-Animationen: Nicht nur für hippe Intros auf Consumer-Sites...



» Beispiel:
Interaktive
Router-
Installations-
anweisung bei
Cisco

Interessante Features: 3D-Unterstützung



» Einsetzbar für
3D-Animationen
oder „ernsthafte“
Anwendungen

Interessante Features: Flash-basierte Formulare



ZS

Vehicle Specs

Technical Specs
Standard Equipment
MSRP

Dealer Options:

- Base Model
- Sports Package
- Deluxe Stereo

Country:

Zip Code:

Starting at \$128,000
Plus \$570 handling and destination, \$128,570



- » Direkte Eingabe von User-Daten in Flash-Anwendung. Anwendung kann sofort reagieren.
- » Weiterleitung der Feldwerte an beliebige Scripts, Servlets usw.

Anwendung: E-Commerce-Applikationen mit Flash



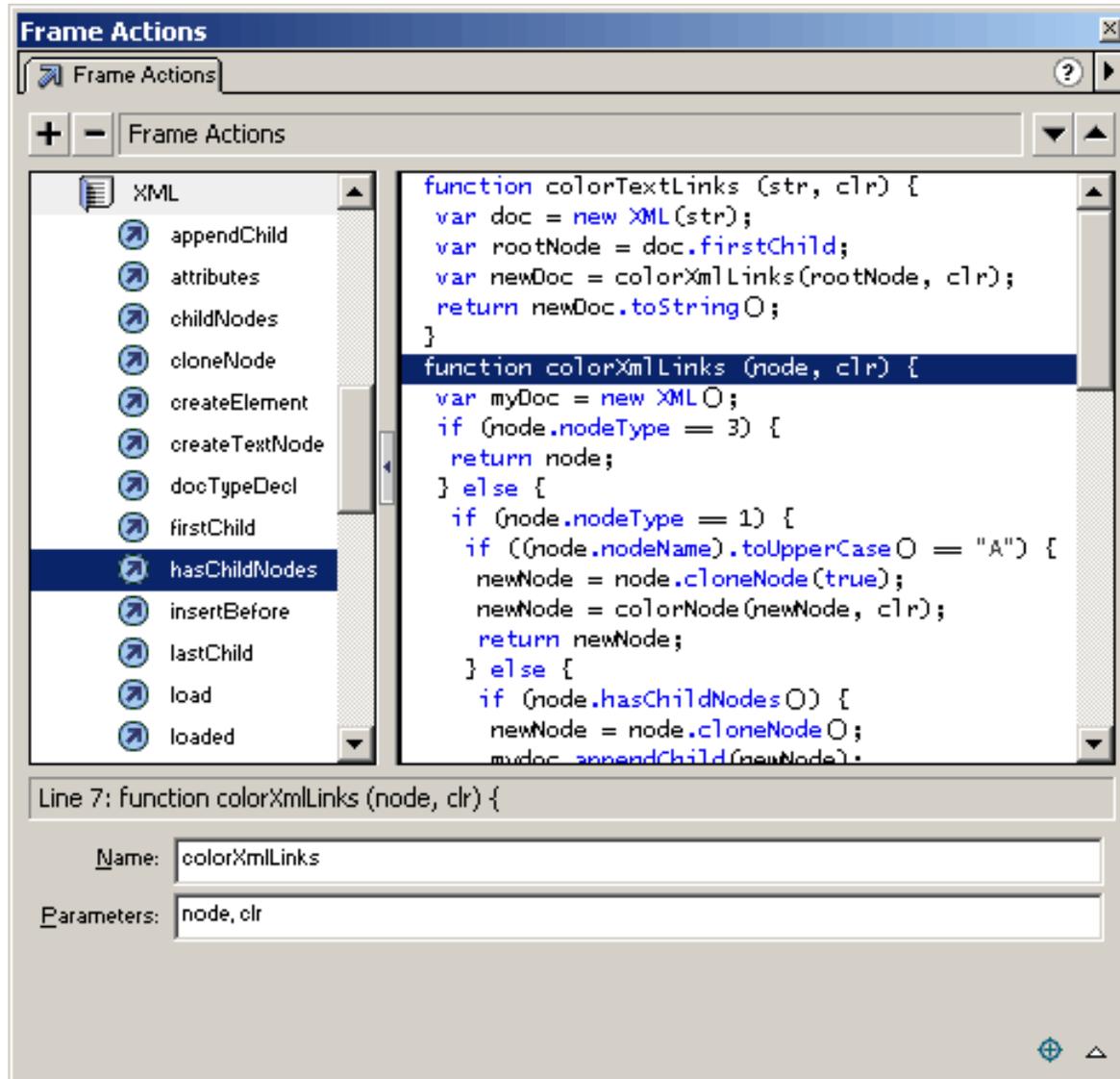
The screenshot shows a Microsoft Internet Explorer browser window displaying the Broadmoor Online Reservations interface. The browser title is "The Broadmoor Online Reservations in oneScreen(TM) - Microsoft Internet Explorer". The address bar shows the URL: <https://www.enteryourinformation.com/broadmoor/onescreen.cfm?CFID=49744&CFTOKEN=3755010>. The page content includes:

- Header:** THE BROADMOOR COLORADO SPRINGS. A message states: "The entire reservation process is contained in this screen. You may start anywhere, and order does not matter."
- Calendar:** A calendar for January and February. The selected dates are January 29 and 31, 2002. A "clear dates" button is visible.
- Room Selection:** A table showing room types and their prices for the selected dates.

Room Type	Price
Classic	\$210
Deluxe	\$350
Eastmoor Suite	not available
Elite	not available
Patio Suite	\$630
Premier	\$450
Superior	\$270
West Tower Suite	\$520
- Room Details:** A section for the "Premier Room" with a 360-degree panorama view. Description: "These large rooms are located in the West Tower, with walk-in closets, marble vanities, and views of the mountains, lake or golf courses."
- Reservation Summary:** check in: January 29, 2002; check out: January 31, 2002; nights: 2; room type: Premier; rooms: 1; people: 1; total: \$450.
- Form:** Fields for First Name, Last Name, Address, City, State, Zip, Country, Email, Phone, Fax, Credit Card (with logos for VISA, MasterCard, DISCOVER, and American Express), Name on Credit Card, Credit Card Number, and Expiration Date. A "Finish Reservation" button is at the bottom.

- » Vorteil: Reichhaltigeres User-Interface als mit HTML möglich.
- » Beispiel: Komplette Hotelreservation auf einem einzelnen Screen. <http://reservations.broadmoor.com>

Interessante Features: XML-Integration in ActionScript



The screenshot shows the 'Frame Actions' panel in an IDE. On the left, a list of XML-related methods is displayed, with 'hasChildNodes' selected. The main area contains the following ActionScript code:

```
function colorTextLinks (str, clr) {  
    var doc = new XML(str);  
    var rootNode = doc.firstChild;  
    var newDoc = colorXMLLinks(rootNode, clr);  
    return newDoc.toString();  
}  
function colorXMLLinks (node, clr) {  
    var myDoc = new XML();  
    if (node.nodeType == 3) {  
        return node;  
    } else {  
        if (node.nodeType == 1) {  
            if ((node.nodeName).toUpperCase() == "A") {  
                newNode = node.cloneNode(true);  
                newNode = colorNode(newNode, clr);  
                return newNode;  
            } else {  
                if (node.hasChildNodes()) {  
                    newNode = node.cloneNode();  
                    myDoc.appendChild(newNode);  
                }  
            }  
        }  
    }  
}
```

Below the code editor, the 'Name' field is set to 'colorXMLLinks' and the 'Parameters' field is set to 'node, clr'.

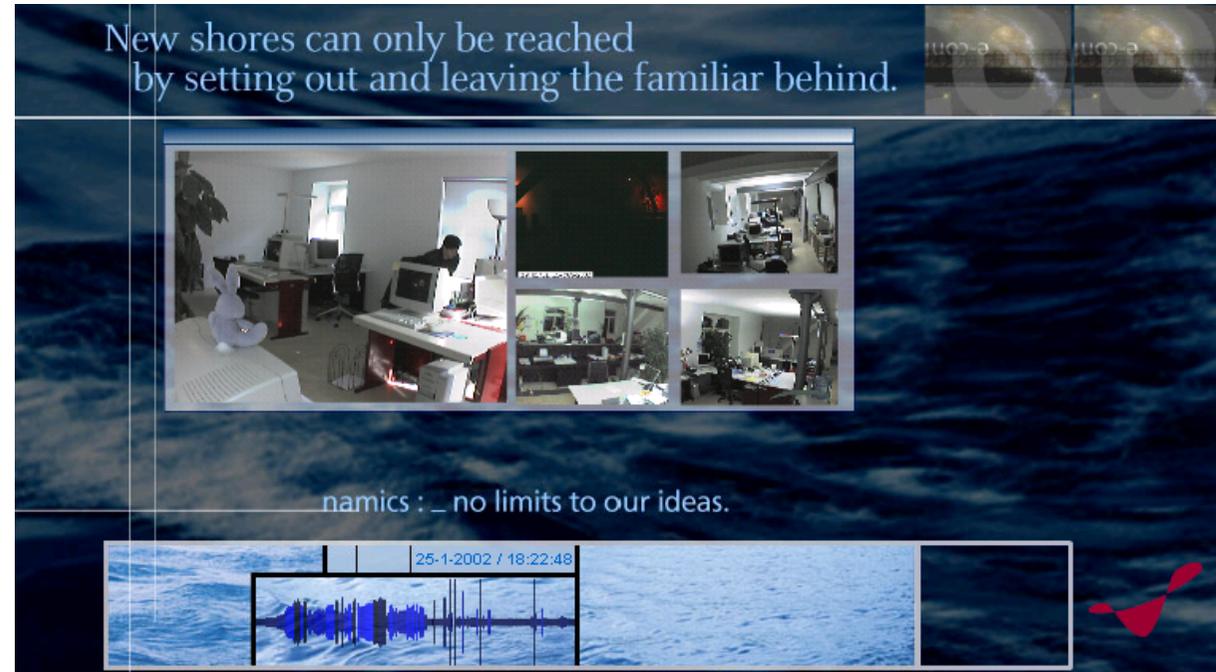
» ActionScript bietet XML-Objekte für direkte Verarbeitung von XML-Streams.

Flash Extensions: Plug-Ins für zusätzliche Fähigkeiten



Beispiele:

- » Generieren von anderen File-Formaten aus Flash-Animationen
- » Steuern anderer Anwendungen
- » Verwenden lokaler Peripherie (z.B. Webcam)
- » Pocket-PC-Unterstützung
- » Vorgefertigte Funktionalitäten



- » <http://www.flash.com/>
- » <http://www.macromedia.com/support/flash/>
- » http://builder.cnet.com/webbuilding/0-7335.html?tag=st.cn.sr1.ssr.bu_flash
- » <http://flashplanet.com/>
- » <http://www.flashkit.com/>

Vielen Dank für Ihre Aufmerksamkeit
Seminarunterlagen: <http://namics.com/knowledge/>

Besuchen Sie uns am Stand 165 in der Halle 5!

andreas.goeldi@namics.com
juerg.stuker@namics.com

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