

Internet-Policy		Konvention
		intpol 1.0.4
		Entwurf öffentlich
Kurzbeschreibung	<p>Konvention zur Harmonisierung der Kommunikation von Behörde zum Bürger Behörde zu Behörde.</p> <p>Diese Konvention beschreibt in allgemeiner Form die möglichen Wege der Harmonisierung in der Kommunikation von Behörde zum Bürger, Behörde zur Wirtschaft, Behörde zu Behörde (externe Kommunikationspartner) und behördenintern.</p> <p>Bei der technischen Umsetzung kommt es unweigerlich zu Unterschieden in der Behandlung. Durch die Vereinheitlichung des Verhaltens der Kommunikationsschnittstellen soll die Nutzung erleichtert und harmonisiert und unter Einhaltung grundlegender Sicherheitsvorgaben realisiert werden.</p>	
Autor(en)	Bernd Martin Robert Wollendorfer	Projektteam / Arbeitsgruppe Internet-Policy

Stelle	Vorgelegt am	Angenommen am	Abgelehnt am
IKT-Board Länder Gemeindebund Städtebund	03.05.2005	13.05.2005	15.11.2005
	25.10.2005		
	25.10.2005	15.11.2005	
	25.10.2005		

Inhaltsverzeichnis

(1)	Ziel des Dokumentes	3
(2)	Geltungsbereich	3
(3)	Allgemeine Grundsätze	3
(4)	Zielgruppen	4
(4.1)	Behörde	5
(4.2)	Bürger, Bürgerin und Wirtschaft	5
(5)	Formate	5
(5.1)	Unzulässige Formate.....	5
(5.2)	Zugelassene Formate.....	5
(5.3)	Gesendete Formate	5
(5.4)	Ausnahmen von Dateiformaten	6
(6)	Wege der Kommunikation.....	6
(6.1)	Web (Browser)	6
(6.2)	Dateitransfer (Dateiupload/Dateidownload)	6
(6.3)	E-Mail	7
(7)	Bedrohungen	7
(7.1)	Malware.....	7
(7.2)	Spam.....	8
(8)	Logging	8
(9)	Offenlegung der Policies	8
(10)	Referenzen	9
Anhang 1	Glossar.....	12
Anhang 2	- XML/XSLT in Web-Browsern	14

Internetpolicy

(1) Ziel des Dokumentes

Diese Konvention beschreibt in allgemeiner Form die möglichen Wege der Harmonisierung in der Kommunikation von Behörde zum Bürger, Behörde zur Wirtschaft, Behörde zu Behörde (externe Kommunikationspartner) und behördenintern.

Bei der technischen Umsetzung kommt es unweigerlich zu Unterschieden in der Behandlung. Durch eine Vereinheitlichung des Verhaltens der Kommunikationsschnittstellen soll die Nutzung erleichtert und harmonisiert und unter Einhaltung grundlegender Sicherheitsvorgaben realisiert werden.

(2) Geltungsbereich

Dieses Dokument bildet die Basis für die Gestaltung der Internetkommunikation für Bund, Länder und Gemeinden untereinander und mit externen Kommunikationspartnern. Zu diesem Dokument gehören auch die Unterdokumente Transfer-Policy [TRANSPOL], E-Mail-Policy [EMAILPOL] und die Domain-Policy [DOMAINPOL] mit der Internetdomänenverwaltung gv.at: Naming- und Domänenregistrierungs-Policy [DOMAINREG], die speziell auf die einzelnen Kommunikationsarten eingehen. Darauf aufbauend soll jede Behörde die technische Umsetzung vornehmen und die entsprechenden Policies formulieren.

(3) Allgemeine Grundsätze

Der Einsatz moderner Informations- und Kommunikationstechnologien ist aus der öffentlichen Verwaltung heute nicht mehr wegzudenken.

Begründet durch einen Paradigmenwechsel in der Öffentlichkeit und in der Verwaltung in den letzten Jahren stellt die Verwaltung neue Qualitätsansprüche an sich selbst. Effizienz, Schnelligkeit, Serviceorientiertheit, Flexibilität und Sicherheit zählen zu den neuen Merkmalen, die angestrebt werden.

Parallel zum traditionellen Behördenweg können die Bürger und Bürgerinnen heute via Internet z.B. in Form von Web-Formularen, Fax oder E-Mail mit der Behörde in Kontakt treten. Dabei ist anzustreben, dass der einzelne Bürger bzw. die Bürgerin im Bedarfsfall identifiziert werden kann.

Das Universalmedium Internet öffnet der Verwaltung neue Kommunikationsmöglichkeiten sowohl mit den Bürger und Bürgerinnen, als auch im verwaltungsinternen Bereich. Konnten in der Vergangenheit lediglich Teile eines Verwaltungsverfahrens elektronisch ausgeführt werden, sind nun auch komplette vollständige Transaktionen, die vom externen Kommunikationspartner über das Medium Internet ausgelöst werden, möglich.

Eine erste Kontaktaufnahme zwischen den Kommunikationspartnern und der Behörde kann über ein Portal der Behörde mit einem dahinter liegenden Formulareserver erfolgen.

Durch eine Vereinheitlichung der Kommunikation und die Verpflichtung der Einhaltung diverser Mindestanforderungen in den veröffentlichten Policies wird den Kommunikationspartnern die Orientierung und Handhabung unter Einhaltung der Sicherheitsanforderungen für den gesamten Kommunikationsablauf erleichtert.

Um dem Vertrauensvorschuss all jener, die die neuen Technologien nutzen, gerecht zu werden, wurde nunmehr auf der Grundlage eines von Behördenvertretern entwickelten Grundsatzpapiers diese Internet-Policy erstellt.

Die Internet-Policy besteht bzw. wird aus folgenden Teildokumenten bestehen:

- E-Mail-Policy [EMAILPOL]
Dieses Dokument behandelt die Kommunikationsart E-Mail mit Vorschlägen zur Vereinheitlichung der E-Mail-Adressen und gibt Vorschläge im Umgang mit Viren und Spams. Ziel ist es Mindestanforderungen für den Umgang der öffentlichen Verwaltung mit dem Kommunikationsmedium E-Mail zu definieren.
- Transfer-Policy [TRANSPOL]
In dieser Policy werden Protokolle und Regeln für den Dateiaustausch definiert.
- Domain-Policy [DOMAINPOL] und Internetdomänenverwaltung gv.at: Naming- und Domänenregistrierungs-Policy [DOMAINREG]
In diesem Teildokumenten werden jene technischen und organisatorischen Richtlinien ausgearbeitet, die für den Erhalt einer Behördendomäne (*.gv.at) vorausgesetzt und eingehalten werden müssen.
- Dokumentenformate und Behörden [DOKFORMATE]
Dieses Teildokument beinhaltet jene Dokumentenformate, die von der Behörde für den ausgehenden Verkehr zur Verwendung kommen sollten, jene die den Behörden bekannt sind und grundsätzlich kein potentiell Risiko in sich bergen und potentiell gefährliche Formate. Ziel ist es dieses Dokument immer aktuelle zu halten. (vgl. dazu auch Abschnitt (5))

Für alle angesprochenen Protokolle in den oben angeführten Dokumenten gilt, dass die Verwendung von Default-Ports empfohlen wird. Damit soll eine problemlosere Erreichbarkeit sowie eine einfachere Konfiguration von Netzwerken (zB. Firewalls) möglich sein.

Ob und in welchem Ausmaß sich die interne Policy (Intranet) von der externen Policy (Internet) unterscheidet, obliegt der Behörde. Anzustreben ist, dass auch für den internen Verkehr die gleichen Mindestvorgaben in Bezug auf die Funktionalität der Dienste und der Sicherheit gelten.

Jede Organisation muss somit in ihrer eigenen Internet-Policy zumindest auf die Vorgaben der Internet-Policy verweisen bzw. diese ergänzen oder Abweichungen von den Mindestanforderungen explizit anführen.

Bei der Umsetzung kann der Aspekt der wirtschaftlichen Vertretbarkeit sowie der technischen Machbarkeit aufgrund bestehender Infrastrukturen in der jeweiligen Organisation mit einfließen. Neue und längerfristige Planungen sollen jedoch die Inhalte bestmöglich abdecken.

(4) Zielgruppen

Die Zielgruppen für die finalisierten Policies sind grundsätzlich alle Kommunikationspartner jener Organisation, die die Policies veröffentlicht.

(4.1) Behörde

In der Zielgruppe Behörde sind alle Organe der öffentlichen Verwaltung der Bundes-, Landes- und Gemeindeverwaltung.

(4.2) Bürger, Bürgerin und Wirtschaft

Diese Zielgruppe umfasst alle Kommunikationspartner, die nicht in der Zielgruppe Behörde definiert sind und die mit Behörden auf elektronischem Wege Daten und/oder Nachrichten austauschen (natürliche und juristische Personen).

(5) Formate

Je nach Kommunikationsform kann die öffentliche Verwaltung eine Mindestanforderung festlegen, welche Dateiformate bzw. Dateiendungen, welche Größe von Dateien und deren Formatierung angenommen werden bzw. welche prinzipiell immer abgelehnt werden.

Weitere Einschränkungen der Formate aus Sicherheitsgründen aber auch die Erweiterung der zulässigen Formate sind dann möglich, wenn diese gemäß Punkt (9) offen gelegt werden.

Welche Formate von der Behörde angenommen werden, ist im Dokument [DOKFORMATE] aufgelistet. Dateien, die mit höheren Versionen von Programmen erstellt wurden, müssen nicht angenommen werden.

Zur Verringerung der Dateigrößen können die zulässigen Formate auch in eines der im [DOKFORMATE] unter „Komprimierung“ angeführten Formate, komprimiert werden.

(5.1) Unzulässige Formate

Dokumente, die ausführbare Programme sind bzw. solche enthalten (z.B. *.EXE, *.BAT, *.VBS, Makros, ...), sind im Regelfall abzuweisen und z.B. durch technische Maßnahmen wie Filter nicht anzunehmen.

Eine Liste der abzuweisenden Dateiendungen und Dateitypen ist in der Policy über die Dokumentenformat angeführt.

Gefährlicher Inhalt sollte geblockt werden, damit bereits präventiv und dem Virens Scanner eventuell noch unbekannte Angriffe abgehalten werden. Dazu zählen z.B.

- Ausführbarer Inhalt
- Inhalt mit Formatverletzungen (z.B. Dateien bei denen eine Prüfung ergibt, dass sie nicht dem erwarteten Format genügen oder unerwarteten/unerwünschten Inhalt haben wie etwa Archive mit falschen Inhaltsangaben)

(5.2) Zugelassene Formate

Die Behörde gibt in der gemäß Punkt (9) offen gelegten Policy jene Dokumentformate bekannt, die von ihr angenommen werden und bei denen die Lesbarkeit und Weiterverarbeitbarkeit zuverlässig gegeben ist.

(5.3) Gesendete Formate

Die Behörde soll keine Dokumente versenden, für deren Lesen und weiteres Verarbeiten ein kommerzielles Softwareprodukt eingesetzt werden muss. Beim

Versenden von Dateien sind grundsätzlich nur jene Formate zu wählen, die vom Hersteller spezifiziert und offen gelegt sind.

Eine Liste der Formate, die in der Kommunikation zwischen Bürger, Bürgerinnen, Wirtschaft und Behörde (Amtsformat) bzw. zwischen Behörden angewendet werden sollte, ist dem Dokument [DOKFORMATE] zu entnehmen.

Auch bei der elektronischen Signatur von Dokumenten ist darauf Rücksicht zu nehmen; Es sind nur solche Signaturverfahren anzuwenden, deren Spezifikation offen gelegt ist und wo es dem Empfänger möglich sein muss, die Signaturen auch verifizieren zu können. Es sind elektronische Signaturen von solchen Dokumenttypen zu bevorzugen, für die es eine Standardisierung gibt (z.B. XMLDSig).

Derzeit sind noch Web-Browser in Verwendung, die XML-Dateien mit entsprechenden Stylesheets nicht anzeigen können. Im Anhang 2 sind beispielhaft jene Web-Browser angeführt, die dies bereits ermöglichen.

Bei der Kommunikation zwischen Behörden sollte der gleiche Standard wie bei der Kommunikation zwischen Bürger mit der Behörde (anzunehmende Formate) angewendet werden.

(5.4) Ausnahmen von Dateiformaten

Im Zuge von bilateralen Vereinbarungen (z.B. mit der Berufsgruppe der Notare) oder wenn es das Verfahren erfordert (z.B. CAD-Formate in Bauverfahren) können auch der Versand und die Annahme anderer Dateiformate als zulässig definiert werden.

(6) Wege der Kommunikation

Bei der Übertragung von vertrauenswürdigen Daten, jedenfalls bei der von personenbezogenen Daten ist u. a. aus Datenschutzgründen (siehe auch [DSG2000]) die jeweils verschlüsselte Variante des jeweiligen Protokolls wie z.B. TLS/SSL (HTTPS) oder SFTP zu verwenden (vgl. (6.2)).

(6.1) Web (Browser)

Die Übertragung von Daten im WWW erfolgt über das HTTP-Protokoll.

Der Aufruf einer Webseite im Internet erfolgt durch die Angabe ihrer gültigen HTTP-Adresse (URL bzw. URI) z.B. <http://www.help.gv.at>. Das Naming und der Registrierungsprozess für gv.at Adressen werden im Dokument [DOMAINREG] geregelt.

Im WWW angezeigte Webseiten bestehen aus Programmcode, der auf den lokalen Rechner geladen und dort interpretiert und dargestellt wird. Die Anzeige von Webseiten erfolgt mittels einer Browser-Software (z.B. Internet-Explorer, Netscape, Opera, Mozilla, etc.). Die Vorgaben, die für Behördenseiten zu beachten sind, werden in der Domain-Policy [DOMAINPOL] geregelt.

(6.2) Dateitransfer (Dateiupload/Dateidownload)

Es müssen die Übertragungsmöglichkeiten, wie z.B. FTP, SFTP, WebDAV, HTTP, SCP, etc. definiert und Richtlinien erstellt werden. Die einzelnen Richtlinien zu den Übertragungsarten werden in der Transfer-Policy [TRANSPOL] beschrieben.

Der Benutzer/die Benutzerin erhält beim Aufruf von Diensten zumindest folgende Hinweise:

- Eigentümer – wer ist Eigentümer des Servers, für den Inhalt verantwortlich
- Betreiber – wer ist Betreiber des Servers
- genaue postalische Adresse
- den für diesen Dienst vorgesehenen Benutzerkreis (Einschränkungen, allgemeine Angaben wie z.B. geschlossener Benutzerkreis, Public/Alle, etc.)
- Kommunikationsdaten für Anfragen – z.B. Telefon, Fax, E-Mailadresse des Webmasters, Link zu einem Formular, etc.
- Hinweis (Link) auf die Policy gemäß Punkt (9)
- Hinweis auf das Logging gemäß Punkt (8)

(6.3) E-Mail

Alle Richtlinien, die bei der E-Mail-Kommunikation zwischen Behörden bzw. zwischen Wirtschaft und Bürger/-innen und Behörden zu beachten sind, werden in einer eigenen E-Mail-Policy angeführt. Darin werden neben den Minimalanforderungen auch jene Anforderungen angeführt, die von den Behörden für deren eigenen Policies definiert werden müssen. Des Weiteren werden Regelungen und Vorgehensweisen im Umgang mit Spams und Viren angegeben. Es werden auch Angaben darüber gemacht, was bei signierten und verschlüsselten E-Mails zu beachten ist, und wie der Zugang und Übertragung zum E-Mailserver gesichert werden kann.

(7) Bedrohungen

In diesem Dokument werden jene Bedrohungen berücksichtigt, die bei der Kommunikation zwischen Bürger und Behörde bzw. zwischen Behörde und Behörde (externe Kommunikationspartner) existieren, nicht jedoch gezielte Angriffe (Hack-Attacken).

(7.1) Malware

Viren, Würmer und andere Schadenssoftware sind eine Begleiterscheinung des Computereinsatzes. Durch die Vernetzung der Rechner ist daraus eine permanente Bedrohung der Produktivität entstanden.

Das Dokument sowie die Folgedokumente beschäftigen sich weder mit der Notwendigkeit der Virenabwehr noch im Detail mit der Abwehr oder Maßnahmen zum Schutz der Infrastruktur selbst. Es schlägt eine Grundstruktur und Konventionen für die Behandlung der, durch die Virenabwehr hervorgerufenen und nach außen und innen sichtbaren Aktionen vor.

Was ist Malware?

Malware kann in Viren, Würmer, Spyware und Trojanische Pferde unterteilt werden. Viren im Sinne dieses Dokuments sind Dateninhalte, die von einem Virenschanner erkannt werden sollten und eine Funktion enthalten, die entweder die Weiterverbreitung der Software selbst, ein Ausspähen von Daten oder einen anderen Schaden zum Ziel haben.

Autoren der Malware verbessern ständig ihre Implementierungen, was zur Folge hat, dass das Erkennen einer Malware sehr erschwert wird. Daher müssen Anti-Malware-Software ständig gewartet und aktuell gehalten werden.

Aufgrund der verstärkten Problematik bei E-Mails wird dieser Thematik in der E-Mail-Policy [EMAILPOL] besonderes Augenmerk geschenkt.

(7.2) Spam

Während Malware bei jeglicher Art von elektronischer Kommunikation von Bedeutung ist, spielt Spam nur bei der E-Mail-Kommunikation eine Bedeutung. Spam beeinträchtigt zunehmend die Kommunikation über E-Mail. Aus diesem Grund wird diesem Thema in der E-Mail-Policy [EMAILPOL] spezielle Aufmerksamkeit geschenkt.

(8) Logging

Das Logging sollte in einem, für den Betrieb, eine eventuell notwendige Nachvollziehbarkeit von Aktionen und einem für die statistische Auswertung sinnvollen Umfang erfolgen. Dieser Umfang wird im Detail durch die Behörde selbst definiert.

Die Speicherung von personenbezogenen Daten darf nur in dem, vom Datenschutz genehmigten Umfangs erfolgen.

Den dafür relevanten Vorgaben des jeweilig geltenden Sicherheitshandbuchs soll dabei entsprochen werden.

Best Practice

Als allgemeine Referenz kann das Österreichische Sicherheitshandbuch [SIHB] angeführt werden, wo folgende Themen im Teil 2 im Abschnitt 5.10 (Protokollierung) eingehend behandelt werden:

- Erstellung von Protokolldateien
- Datenschutzrechtliche Aspekte bei der Erstellung von Protokolldateien
- Kontrolle von Protokolldateien
- Rechtliche Aspekte bei der Erstellung und Auswertung von Protokolldateien zur E-Mail- und Internetnutzung
- Audit und Protokollierung der Aktivitäten im Netz
- Intrusion Detection Systeme

Inhalte vergleichbarer Art sollten jedenfalls von der Behörde in einer vergleichbaren Art definiert werden.

Im Abschnitt 6.2 (Security Compliance Checking und Monitoring) wird auf die Maßnahmen bei der Auswertung von Protokolldateien hingewiesen.

(9) Offenlegung der Policies

Um die Bürger/Bürgerinnen über die in Verwendung stehenden Policies zu informieren, müssen diese auf der Homepage der Behörde/Dienststelle an sehr prominenter, leicht ersichtlicher bzw. auffindbarer Stelle zur Verfügung stehen. Diese Vorgabe und weitere Richtlinien werden in der Domain-Policy behandelt.

Die Policies sind zumindest in Deutsch anzubieten und zu veröffentlichen, weitere Sprachen sind möglich (Englisch ist empfehlenswert);

Der Mindestumfang der Offenlegung wird in den jeweiligen Policies geregelt. Es wird darauf hingewiesen, dass sowohl das Mediengesetz [MEDG] als auch das E-Commerce-Gesetz [ECG] im Bedarfsfall berücksichtigt werden müssen.

(10) Referenzen

[DOKFORMATE]

Michael Liehmann, Bernd Martin, Robert Wollendorfer: Dokumentenformate. Konvention / Empfehlung, Version 1.0.2. Abgerufen aus dem World Wide Web am 31.05.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

[DOMAINPOL]

Michael Liehmann, Bernd Martin: Domain-Policy. Konvention / Empfehlung, Version 1.0.0. Abgerufen aus dem World Wide Web am 30.09.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

[DOMAINREG]

Helmut Hummer, Bernd Martin, Gerhard Schwarz: Internetdomänenverwaltung gv.at Naming- und Domänenregistrierungs-Policy. Konvention / Empfehlung, Version 1.0.0. Abgerufen aus dem World Wide Web am 30.09.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

[DSG2000]

Bundesgesetz über den Schutz personenbezogener Daten. (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999. Ausgegeben am 17. August 1999. Abgerufen aus dem World Wide Web am 03.01.2005 unter <http://www.ris.bka.gv.at/taweb/cgi/taweb?x=d&o=r&v=bgbldf&d=BGBLPDF&i=593&p=1>

[ECG]

152. Bundesgesetz - Jahrgang 2001: E-Commerce-Gesetz. Regelung bestimmter rechtlicher Aspekte des elektronischen Geschäfts- und Rechtsverkehrs (E-Commerce-Gesetz - ECG) und Änderung des Signaturgesetzes sowie der Zivilprozessordnung

(NR: GP XXI RV 817 AB 853 S. 83. BR: AB 6499 S. 682.) [CELEX-Nr.: 300L0031]

[EMAILPOL]

Micheal Liehmann, Bernd Martin: E-Mail-Policy. Konvention / Empfehlung, Version 2.0.2, von 31.05.2005. Abgerufen aus dem World Wide Web am 29.06.2004 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

[FTP] – RFC 0959

Postel J., Reynolds J.: File Transfer Protocol (FTP). Request for Comments. Oktober 1985. Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc0959.txt>

[HTTP1.1] - RFC 0913

J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: Hypertext Transfer Protocol – HTTP/1.1. Standards Track. Juni 1999. Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc2616.txt>

[IMAP4]

Crispin M.: Internet Message Access Protocol - Version 4 (IMAP4). Standards Track Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc1730.txt>

[MEDG]

Bundesgesetz vom 12. Juni 1981 über die Presse und andere Publizistische Medien (Mediengesetz) StF: BGBl. Nr. 314/1981 (in der Fassung BGBl I Nr. 136/2001)

[POP3]

Myers J., Carnegie Mellon, Rose M.: Post Office Protocol - Version 3 (POP3). Standards. Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc2821.txt>

[SFTP] - SSH File Transfer Protocol (secure shell)

Secure Shell (secsh) IETF working group. Abgerufen aus dem World Wide Web am 19.1.2004 unter <http://www.ietf.org/html.charters/secsh-charter.html>

[SIHB]

Chief Information Office, IKT-Stabsstelle, Österreichisches IT-Sicherheitshandbuch Teil 1: IT-Sicherheitsmanagement Version 2.2 November 2004 und Teil 2: IT-Sicherheitsmaßnahmen Version 2. 2 November 2004. Abgerufen aus dem World Wide Web am 15.12.04 unter <http://www.cio.gv.at/securenetworks/sihb/>

[SMTP]

Klensin J.: Simple Mail Transfer Protocol (SMTP). April 2001. Standards Track Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc2821.txt>

[TELNET]

Postel J., Reynolds J.: Telnet Protocol Specification (Telnet). Request for Comments. Mai 1983. Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.ietf.org/rfc/rfc0854.txt>

[TRANSPOL]

Bernd Martin, Robert Wollendorfer, Transfer-Policy. Konvention / Empfehlung, Version 1.0.2. Abgerufen aus dem World Wide Web am 31.05.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

[WAI]

Wendy Chisholm, Gregg Vanderheiden, Ian Jacobs: Web Content Accessibility Guidelines 1.0. W3C Recommendation, Mai 1999. Abgerufen

aus dem World Wide Web am 15.12.03 unter
<http://www.w3.org/TR/WCAG10/>

[WebDAV]

Y. Goland, A. Faizi , S. Carter, E. Whitehead, D. Jensen: HTTP Extensions for Distributed Authoring – WEBDAV. Standards Track. Februar 1999. Abgerufen aus dem World Wide Web am 20.05.04 unter
<http://www.ietf.org/rfc/rfc2518.txt>

[XMLDSIG]

Eastlake, Donald, Reagle, Joseph und Solo, David: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. Abgerufen aus dem World Wide Web am 14.05.2004 unter <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>.

Anhang 1 Glossar

BROWSER	"to browse = grasen, schmökern"; Software die es gestattet, von Servern im Internet Informationen abzurufen.
CAD	Computer Aided Design
CLIENT	Arbeitsplatzrechner
CRL	Certificate Revocation Lists
DOC	Dokumentenformat von Microsoft Word
FRAME	engl. Rahmen; rechteckiger Bildschirmbereich
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL/TLS
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MTA	Message Transport Agent
IMAP4	Internet Message Access Protocol
NDR	None Delivery Record
PC	Personal Computer, Arbeitsplatzrechner
PDF	Portable Documentation Format) ; Adobes Format für digitales Layout
POP3	Post Office Protocol
RTF	Rich Text Format
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
Spam	Als „Spam“ (sprich: späm) werden Massensendungen bezeichnet, die zu Werbezwecken z.B. per E-Mail versendet werden. Eine andere Bezeichnung hierfür ist UCE (Unsolicited Commercial E-Mail).
SPYWARE	Programm (-teil) das ohne Wissen des Anwenders dessen Surfgewohnheiten protokollieren und diese unbemerkt auf einen Server im Internet überträgt.

SSH	Secure Shell
SSL	Secure Socket Layer
TELNET	Remote Terminal Emulation; Protokoll der Internet Protokollsuite
TLS	Transport Layer Security
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
WAI	Web Accessibility Initiative
WebDAV	WWW Distributed Authoring and Versioning
WWW	World Wide Web
XMLDsig	XML Digital Signature

Anhang 2 - XML/XSLT in Web-Browsern

Folgende Web-Browser-Versionen unterstützen die Anzeige von XML und XSLT-Dateien.

Browser-Hersteller	Version
Internet Explorer	ab Version 5.5 ¹
Konqueror	NICHT
Mozilla	ab Version 1.2
Netscape	ab Version 6 ²
Opera	Eingeschränkt ab Version 4.0 ³
Safari	ab Version 1.0 ⁴

¹ Internet Explorer 5.0 und 5.5 kann aufgrund der späteren Fertigstellung des XSLT-Standards als nicht vollständig kompatibel zur offiziellen W3C XSL Empfehlung angesehen werden. Bei IE 5 und IE 5.5 werden XML-Formatierungen auf CSS-Basis werden nur unzulänglich unterstützt. Auch auf MAC kann es beim IE im Umgang mit XML zu Problemen kommen.

² Netscape 6 unterstützt ebenfalls nicht die volle W3C XSLT-Empfehlung, diese ist erst in Version 7 implementiert.

³ Opera kann wohl XML mit CSS anzeigen, XSL bzw. XSLT wird jedoch nicht unterstützt. Mehr zur aktuellen Version 7.5 unter <http://www.opera.com/docs/specs/index.dml> bzw. <http://people.opera.com/howcome/1999/foch.html>

⁴ Siehe <http://www.apple.com/safari/>

Historie

Version	Datum	Kommentar
1.0.0	15.01.2004	
Ersteller		
Robert Wollendorfer		
Version	Datum	Kommentar
1.0.1	01.03.2004	
Ersteller		
Robert Wollendorfer		
Version	Datum	Kommentar
1.0.2	20.05.2004	
Ersteller		
Bernd Martin		
Version	Datum	Kommentar
1.0.3	26.01.2005	
Ersteller		
Bernd Martin		

		<ul style="list-style-type: none"> • Aufnahme des Dokuments für die Domänenregistrierung und das Naming als Referenz und im Literaturverzeichnis • Anpassung auf die aktuelle Version des im Literaturverzeichnis referenzierten Sicherheitshandbuchs sowie der Dokumente der AG Internetpolicy • Entfernen des Hinweises auf das Mediengesetz §24, da dies für Webauftritte nicht gilt. Dies ist kein Medienstück lt. Mediengesetz.
Version	Datum	Kommentar
1.0.4	25.08.2005	
Ersteller		
Bernd Martin		
		<ul style="list-style-type: none"> • Punkt (3): Explizite Aufnahme, dass wirtschaftliche Vertretbarkeit bei der Umsetzung mit bestehenden Infrastrukturen berücksichtigt werden kann. • Punkt (6): sensible Daten wurde durch vertrauenswürdige Daten ersetzt, um keine Missinterpretation mit dem Begriff lt. [DSG2000] zu erhalten. Verweis auf [DSG2000] wurde aufgenommen. • Punkt (8): Klarstellung, dass nur das jeweils geltende Sicherheitshandbuch anzuwenden sei. • Punkt (9): Entfernen des vorgeschlagenen Links und Ersatz mit prominenter Stelle.