
| Transfer-Policy | Konvention<br>transpol 1.0.2<br>Entwurf öffentlich |
|---|---|
| Kurzbeschreibung | Policy für Datei-Transfer-Dienste<br>Diese Konvention legt einzelne technisch-organisatorische Aspekte des Verhaltens der öffentlichen Verwaltung bei der elektronischen Datenübermittlung mittels Dateitransfer fest. |

| Autor(en) | Robert Wollendorfer<br>Bernd Martin | Projektteam/Arbeitsgruppe<br>Internetpolicy |
|---|---|---|

| Stelle | Vorgelegt am | Angenommen am | Abgelehnt am |
|---|---|---|---|
| **IKT-Board<br>Länder<br>Gemeindebund<br>Städtebund** | 29.06.2004 | 29.06.2004 | |

| *Dokumentklasse:* | **Konvention**<br>Erläuterung<br>Information | *Doku-Stadium:* | Entwurf intern<br>Entwurf öffentlich<br>**Empfehlung** |
|---|---|---|---|

# Transfer-Policy

## Inhaltsverzeichnis

# (1) Ziel des Dokumentes

Diese Konvention legt einzelne technisch-organisatorische Aspekte des Verhaltens der öffentlichen Verwaltung bei der elektronischen Datenübermittlung mittels Dateitransfermethoden fest.

Ziel dieses Dokumentes ist es, eine Mindestanforderung für den Umgang der öffentlichen Verwaltung mit dem Kommunikationsmedium Dateitransfer zu definieren.

Das gegenständliche Dokument gilt als Grundlage für die Behörden, einerseits für die entsprechende technische Umsetzung und andererseits für die Erstellung der zu veröffentlichenden Policies, an der sich die Zielgruppen (Bürger, Wirtschaft, Behörden - siehe Zielgruppen im Dokument [INTPOL]) orientieren können.

Das Glossar ist im Dokument Internet-Policy [INTPOL] enthalten.

# (2) Übertragungsprotokolle

## (2.1) FTP/SFTP und SCP

FTP, SFTP und SCP sind Basisdienste im Internet, die besonders dem Transport von Dateien zwischen Rechnern dienen.

Die Vorteile von FTP liegen in den effizienten Verfahren zur Übertragung von Dateien beliebigen Formats, der Tatsache, dass der Zugriff seitens beliebiger Internet-Teilnehmer möglich ist und der weit verbreiteten Unterstützung von FTP.

Nachteile von FTP sind die minimalen Möglichkeiten mit dem Benutzer zu kommunizieren und die Gefahr für Serverbetreiber die durch technische Aspekte des FTP entstehen. Die Datenübertragung bei FTP erfolgt im Klartext, bei SFTP bzw. SCP wird diese verschlüsselt durchgeführt und wirken so gegen die Nachteile von FTP (siehe (2.3)). Unter dem Blickwinkel der Authentifizierung werden zwei Arten von FTP unterschieden:

- Benutzerspezifisches FTP

  Dabei wird eine Benutzerauthentifizierung benötigt. Diese Kommunikation kann z.B. zum Herunterladen von Dateien für einen eingeschränkten Benutzerkreis zum Einsatz kommen.

- Anonymous-FTP

  Diese Kommunikation ist für alle Internetbenutzer offen (anonym).

## (2.2) HTTP/HTTPS und WebDAV

Die Vorteile von HTTP liegen in der benutzerfreundlichen und meist bekannten Nutzung die zur Übertragung von Dateien beliebigen Formats seitens beliebiger Internet-Teilnehmer möglich ist.

HTTP Uploads werden in Webapplikationen gehandhabt. Im Gegensatz zum FTP-Dienst erlauben diese Applikationen eine Benutzerführung. Während HTTP wieder die ungesicherte Variante des Protokolls darstellt, kann SSL/TLS zur Verschlüsselung und ggf. auch zur Authentifizierung verwendet werden (HTTPS).

Ein Datentransfer kann auch via WebDAV (WWW Distributed Authoring and Versioning) erfolgen. Dieses Protokoll erweitert HTTP um einen Satz neuer Methoden und Header und erlaubt damit Dateien über HTTP zu transferieren.

## (2.3) Telnet, SSH

Telnet wird als Dienst sehr eingeschränkt verwendet. Telnetdienste erlauben direkten Zugriff auf Systeme, bzw. Anwendungen. Die Anwenderschnittstelle ist hier von der Anwendung selbst abhängig.

Da bei Telnet alles im Klartext übertragen wird, sollte dies nur für Daten, die auch sonst frei zugänglich sind, verwendet werden.

Secure-Shell erlaubt die Absicherung der Klartextübertragung von Telnet vor Mithören und bietet zusätzliche Authentifizierungsmöglichkeiten. SFTP (SSH FTP) und SCP sind Protokolle, die auf SSH aufbauen und über eine Public Key Infrastruktur Authentifizierung und Verschlüsselung zur sicheren Datenübertragung nutzen.

Den in diesem Dokument gelisteten Anforderungen zur Kennzeichnung von Diensten sollte auch hier entsprochen werden.

# (3) Datentransfer mit FTP, SFTP und SCP

## (3.1) Datenschutz und sichere Übertragung

Bei [FTP] wird das Passwort im Klartext zwischen Client und Server übertragen. Aus diesem Grund sollte die verschlüsselte Variante [SFTP] eingesetzt werden.

Bei der Übertragung von wichtigen Daten, jedenfalls bei der von personenbezogenen Daten ist eine verschlüsselte Verbindung herzustellen.

Auf eine entsprechende Rechteverwaltung ist zu achten um das Überschreiben von bereits vorhandenen gleichnamigen Dateien zu verhindern.

## (3.2) Informationsdatei

Wie derzeit auf FTP-Servern üblich, sollten die Informationsdateien wie README bzw. und/oder LIESMICH vorhanden sein. Im Wurzelverzeichnis (Root) soll in diesen Dateien in jedem Fall auf Deutsch das Verhalten des Dateiservers erklärt sein; weitere Sprachen können vorgesehen werden.

Insbesondere soll auf Virenscanner und dessen Verhalten beim Auffinden von Malware hingewiesen werden.

## (3.3) Sonderfälle beim Scannen nach Malware

Bei Dateitransferdiensten können Dateien entweder während des Transfers oder durch automatisierte Abläufe auf Malware geprüft werden.

Während des Transfers kann ein Virenscanner auf dem Server das Speichern der mit einem Virus infizierten Datei blockieren. Dabei ergibt sich jedoch, dass der FTP Server nur einen Schreibfehler als Fehler-Code zurückbekommt. Die tatsächliche Fehlermeldung und deren Ausprägung ist produktabhängig.

Derzeit unterstützen die meisten End-User Clients für FTP keine Auswertung von zusätzlichen Fehlermeldungen bzw. sind die Fehlermeldungen für den Endanwender nicht aussagekräftig genug.

### (3.3.1) FTP-Upload bei Online-Scannern im Dateisystem

Online-Scanner unterbrechen bei einer erkannten malwarebehafteten Datei bereits den Upload und liefern einen Schreibfehler des Dateisystems. Dieses Verhalten verhindert zwar den Upload von Malware, ist aber für Endanwender nicht sofort

klar und durchschaubar. Deshalb sollte in den Informationsdateien und in der Policy deutlich darauf hingewiesen werden.

### (3.3.2) FTP-Upload bei Servern ohne Online-Scanner

Hier wird die Datei ohne Prüfung entgegengenommen. Die Datei wird erst nach erfolgreicher Fertigstellung des Uploads auf Malware gescannt, und nach diesem Scannen weiter verarbeitet. Dateien, die nicht gesäubert werden können, sind in ein Quarantäneverzeichnis zu verschieben. Zur Zeit des Scannens kann keine Meldung mehr an den Anwender gegeben werden.

## (3.4) Anonymer Upload

Ein anonymer Upload soll von Servern der öffentlichen Verwaltung nur in Ausnahmefällen, und da nur zeitlich begrenzt, möglich sein. In jedem Fall ist jedoch durch geeignete Maßnahmen zu verhindern, dass aus Uploadverzeichnissen Downloads durchgeführt werden können.

Bei einem anonymen Upload besteht keine zuverlässige Möglichkeit dem Endanwender zu verständigen, dass seine Daten Malware enthalten.

## (3.5) Upload durch registrierten Benutzer

Registrierte Benutzer können entweder durch E-Mail oder durch spezielle Einträge in Benutzerverzeichnissen auf Malware hingewiesen werden.

# (4) Datentransfer mit HTTP und WebDAV

## (4.1) Datenschutz

Bei der Übertragung von wichtigen Daten, jedenfalls bei der von personenbezogenen Daten ist u. a. aus Datenschutzgründen die jeweils verschlüsselte Variante wie z.B. HTTPS des Protokolls zu verwenden.

## (4.2) Benachrichtigung des Benutzers

Wenn möglich soll der Benutzer, der den Upload durchführt im Upload-Formular oder im Clientprogramm eine E-Mail-Adresse als Benutzername angeben damit diese für Benachrichtigungen des Benutzers zur Verfügung steht.

## (4.3) Malwareprüfung während des Upload-Vorganges

Wird die Malwareprüfung durchgeführt, bevor für den Benutzer der Vorgang beendet ist, so soll der Benutzer eine entsprechende aussagekräftige Fehlermeldung erhalten.

## (4.4) Malwareprüfung nach dem Upload

Wird die Datei erst nach dem Upload als infizierte Datei identifiziert, erhält der Benutzer eine Nachricht.

# (5) Offenlegung der Policy

Die veröffentlichte Policy für Transfer-Dienst enthält zumindest folgende Angaben (vgl. E-Commerce-Gesetz [ECG]):

- Eigentümer – wer ist Eigentümer des Servers, für den Inhalt verantwortlich (Impressum)

- Betreiber – wer ist Betreiber des Servers, genaue postalische Adresse
- Kommunikationsdaten für Anfragen – z.B. Telefon, Fax, E-Mail-Adresse des Webmasters, Link zu einem Formular, etc.
- weitere Informationen – z.B. Link zur Startseite
- Hinweis auf das Logging

# (6) Referenzen


### [INTPOL]

Arbeitsgruppe Internetpolicy: Internet-Policy. Konvention zum E-Government Austria erarbeitet von Chief Information Office, Stabsstelle IKT-Strategie des Bundes. Öffentlicher Entwurf, Version 1.0.2, 29.06.2004. Abgerufen aus dem World Wide Web am 29.06.2004 unter http://www.cio.gv.at/it-infrastructure/intpol/

### [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]

### [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

### [HTTP 1.1] - RFC 2616

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

### [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

### [WEBDAV] - RFC 2518

Y. Goland, E. Whitehead, A. Faizi, S. Carter, D. Jensen: HTTP Extensions for Distributed Authoring – WEBDAV. Februar 1999, Abgerufen aus dem World Wide Web am 9.6.2004 unter http://www.ietf.org/rfc/rfc2518.htm

# Historie

| Version | Datum | Kommentar |
|---|---|---|
| 1.0.0 | 15.01.2004 | Initialversion erstellt. |
| Ersteller: Robert Wollendorfer | | |

| Version | Datum | Kommentar |
|---|---|---|
| 1.0.1 | 01.03.2004 | • Layout geändert<br>• Glossar ergänzt<br>• Tippfehler korrigiert<br>• Anhang 2 durch Beschreibung ergänzt<br>• Tabelle mit den Formatangaben ergänzt bzw. Versionen eingearbeitet |
| Ersteller: Robert Wollendorfer | | |

| Version | Datum | Kommentar |
|---|---|---|
| 1.0.2 | 20.05.2004 | • Layout geändert<br>• Tippfehler korrigiert<br>• Ergänzung um Teil des bisherigen Internet-Policy Teils für die Dateitransferformate (Abschnitt (2) in diesem Dokument).<br>• Ergänzung der Kommunikationsprotokolle um WebDAV und SCP |
| Ersteller: Bernd Martin | | |