Inhaltsverzeichnis

1. Ziel und Festlegung der Schnittstellendefinition

1.1 Einleitung

Die rasche technische Weiterentwicklung der Systeme und stetig neue Anforderungen erfordern eine Festlegung für die Übermittlung von Dateien mittels File-Transfer-Protokoll im Gesundheits- und Sozialwesen.

Die folgende Definition einer Schnittstelle ist als festgeschriebene, jedoch offengelegte Schnittstelle für das Gesundheits- und Sozialwesen ausgelegt.

Ziel dieser Definitionen ist es, im Gesundheits- und Sozialwesen eine gesicherte digitale Kommunikation unabhängig von der Art der jeweiligen Systeme zu gewährleisten.

1.2 Festlegungen

Die Definition der Schnittstelle beschreibt die zulässigen Protokolle und das grundlegende Verfahrensmanagement für die automatisierten Verarbeitungsprozesse, um eine einheitliche Abwicklung der zu übermittelnden Dateien im Gesundheits- und Sozialwesen zu gewährleisten.

2. Kurzbeschreibung FTP / SFTP / FTPS

2.1 File Transfer Protocol

Das File Transfer Protocol ist ein im RFC 959 von 1985 spezifiziertes Netzwerkprotokoll zur Übertragung von Dateien über TCP/IP-Netzwerke. FTP ist in der Anwendungsschicht (Schicht 7) des OSI-Schichtenmodells angesiedelt. Es wird benutzt, um Dateien vom Server zum Client (Herunterladen), vom Client zum Server (Hochladen) oder clientgesteuert zwischen zwei Endgeräten zu übertragen. Außerdem können mit FTP Verzeichnisse angelegt und ausgelesen, sowie Verzeichnisse und Dateien umbenannt oder gelöscht werden.

2.1.1 Anwendung von FTP

Das FTP verwendet für die Steuerung und Datenübertragung jeweils separate Verbindungen: Eine FTP-Sitzung beginnt, indem vom Client zum Control Port des Servers (der Standard-Port dafür ist Port 21) eine TCP-Verbindung aufgebaut wird. Über diese Verbindung werden Befehle zum Server gesendet. Der Server antwortet auf jeden Befehl mit einem Statuscode, oft mit einem angehängten, erklärenden Text. Die meisten Befehle sind allerdings erst nach einer erfolgreichen Authentifizierung zulässig. Zum Senden und Empfangen von Dateien sowie zur Übertragung von Verzeichnislisten (der Standard-Port dafür ist Port 20) wird pro Vorgang jeweils eine separate TCP-Verbindung verwendet.

Beim aktiven FTP (auch „Active Mode“) öffnet der Client einen zufälligen Port und teilt dem Server diesen sowie die eigene IP-Adresse mittels des PORT-Kommandos mit. Dies ist typischerweise ein Port des Clients, der jenseits von 1023 liegt, kann aber auch ein anderer Server sein, der seinerseits in den Passive Mode geschaltet wurde, also auf eine Verbindung wartet (so genanntes FXP). Die Datenübertragung auf der Server-Seite erfolgt dabei über Port 20. Die Kommunikation mit Befehlen erfolgt ausschließlich auf dem Control Port. Man spricht auch von der Steuerung „Out of Band“. Somit bleibt es möglich, dass während der Datenübertragung die Partner noch immer miteinander kommunizieren können.

2.2 SSH File Transfer Protocol

Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht (siehe hierzu RFC 4250ff).

Im Unterschied zum FTP über TLS (FTPS) begnügt sich SFTP mit einer einzigen Verbindung zwischen Client und Server. Diese Auslegung ermöglicht, dass SFTP freistellt, statt SSH auch andere Verfahren zur Authentifizierung und Verschlüsselung einzusetzen

Entworfen wurde SFTP für die Verwendung mit SSH ab Version 2, in der SSH Version 1 wurde stattdessen Secure Copy (SCP) verwendet.

SFTP erweitert SCP und bietet zusätzliche Dateioperationen. Das Secure Copy Protokoll (SCP) basiert auf SSH und gewährleistet so die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten. Das Protokoll selbst implementiert nur die Dateiübertragung, für die Anmeldung und Verbindung wird SSH genutzt und auf dem entfernten Rechner ein SCP-Server aufgerufen; dieser ist normalerweise gleichzeitig auch das Client-Programm. Für das darunterliegende SSH wird ein SSH-Server benötigt.

SFTP im TCP/IP-Protokollstapel:

Anwendung	**SFTP**				
	SSH				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Für die Verbindung wird der Port 22 verwendet.

2.3 FTPS, File Transfer Protocol über TLS/SSL

FTPS darf nur nach bilateraler Absprache eingesetzt werden!

FTP über SSL oder FTP over TLS, kurz FTPS, ist eine Methode zur Verschlüsselung des File Transfer Protocol (FTP), die im RFC 4217 beschrieben ist.
Im Unterschied zu SFTP ist FTPS eine Kombination von FTP und dem Transport Layer Security (TLS). Die Verschlüsselungsschicht (TLS/SSL) liegt unterhalb der FTP Anwendungsschicht in der Transportschicht, also zwischen dem TCP und der Anwendung FTP.

FTPS im TCP/IP-Protokollstapel:

Anwendung	FTP				
Transport	SSL/TLS				
	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

FTPS führt vor der Datenübertragung eine Authentifizierung durch.

Siehe dazu auch das Kapitel „Sichere Transportebene mit TLS (SSL)“ in der Security Schnittstelle für den Datenaustausch im Gesundheits- und Sozialwesen.

2.3.1 Explizites und Implizites FTP über TLS

Nicht der FTP Client, sondern der FTP Server definiert, welches FTPS Verfahren genutzt werden darf bzw. genutzt werden muss.

Verschlüsselungsart	Beschreibung
Explizites FTPS	Explizites FTP über TLS ist auch unter der Bezeichnung FTPES bekannt. In diesem Modus muss der Client explizit nach einer sicheren Übertragung beim Server anfragen. Falls ein Client bei diesem Modus keine entsprechende Anfrage an den Server stellt, dann kann der Server entscheiden, ob er diese unsichere Verbindung weiterhin bestehen lässt oder sie aber ablehnt bzw. limitiert.
Implizites FTPS	Das Implizite FTP über TLS ist auch unter der Bezeichnung FTPS bekannt, allerdings nicht in RFC 4217 beschrieben. In diesem Modus wird vom Client erwartet, dass er sich mit einer TLS/SSL „ClientHello“-Nachricht sofort beim Server auf dem dedizierten Port 990/tcp meldet. Tut er dies nicht, trennt der Server die Verbindung.

2.3.2 FTPS im Passiv- und Aktivmodus

Der Passivmodus bietet sich im Gegensatz zum Aktivmodus an, um eventuelle initiale Verbindungsprobleme durch Router- / Firewall-Einstellungen zu reduzieren oder zu vermeiden.

Modus	Beschreibung
Passive Mode	Beim passiven FTP sendet der Client ein PASV-Kommando, der Server öffnet einen Port und übermittelt diesen mitsamt IP-Adresse an den Client. Hier wird auf der Client-Seite ein Port jenseits 1023 verwendet und auf der Server-Seite der vorher an den Client übermittelte Port. Durch den Einsatz des Passive Mode wird erreicht, dass eine Absprache über die zur Kommunikation verwendeten Port-Bereiche zwischen Client- und Servernetz erzwungen wird. Diese Port-Bereiche sind auf beiden Seiten frei zu schalten.
Aktive Mode	Beim aktiven FTP verbindet sich der Client von einem zufälligen Port (N > 1024) mit dem Server Port 21. Dann hört/wartet der Client auf Port N+1 und sendet entsprechend auch an den Server das Kommando "PORT N+1". Der Server verbindet sich mit dem Client-Data-Port N+1 von seinem Dataport 20 aus.

	Aus Sicht des Client erstellt er nicht selbst die Verbindung zum Datenport des Servers. Aus Sicht seiner Firewall initiiert ein außen stehendes System die Verbindung zu einem internen Clientrechner (und das wird normalerweise blockiert). Die Port-Bereiche sind auf beiden Seiten frei zu schalten.

2.3.3 Binärmodus und ASCII Modus

Die richtige Auswahl der Zeichenübertragung ist für eine korrekte Datenübermittlung wichtig.

Zeichencodierung	Beschreibung
Binär Modus	Der Binär Modus überträgt Zeichen für Zeichen unverändert. Bei der Übermittlung der Daten ist zwingend der Binärmodus zu verwenden, da größtenteils verschlüsselte Daten übertragen werden und hier keine Veränderung erfolgen darf. Auch bei der Übertragung unverschlüsselter ASCII-Daten darf keine Transformation der Nutzdaten erfolgen.
ASCII Modus	Der ASCII Modus ist für die Übertragung von Textdateien gedacht. Hierbei werden Umwandlungen des Zeichensatzes (z.B. von ANSI nach ASCII) durchgeführt oder auch Steuerzeichen von Windows (carriage return / line feed) nach Unix (line feed)gewandelt.

2.3.4 Anwendung von FTPS

- Das implizite FTPS muss verwendet werden.
- Der Passiv Modus sollte nach Möglichkeit verwendet werden.
- Die Daten müssen im Binär Modus übertragen werden.
- **FTPS darf nur nach bilateraler Absprache eingesetzt werden**

3. Angewandte Standards und Normen

Das Verfahren basiert auf den bereits im Gesundheits- und Sozialwesen angewandten Gemeinsamen Grundsätzen Technik und zum anderen auf den Standards des Internets, die einfach umzusetzen sind.

3.1 Sicherheitsstandards

Im Gesundheits- und Sozialwesen werden zur Absicherung des Datenaustauschs mit Arbeitgebern und Leistungserbringern kryptographische Verfahren eingesetzt. Diese sind in der jeweils aktuellen Security Schnittstelle für den Datenaustausch im Gesundheits- und Sozialwesen definiert.

Die dort definierten Standards sind im Gesundheits- und Sozialwesen etabliert. Es sind Trust Center-Strukturen vorhanden und die Annahmestellen sind mit der entsprechenden Software ausgestattet. Eine Vielzahl von Arbeitgebern bzw. Leistungserbringern arbeiten bereits mit diesen Lösungen.

Die Annahmestellen sind berechtigt, zum Schutz des eigenen Netzes gegen Missbrauch nur bestimmte IP-Adressen/-Adressbereiche (z.B. statische IP-Adressen) zum FTP-Verfahren zuzulassen. Die obligatorische Benutzeranmeldung kann von den Annahmestellen in eigenem Ermessen fakultativ mit einem Passwort gesichert werden.

3.2 Kommunikationsstandards

Folgende Protokollvarianten der FTP-Protokollfamilie zur Übermittlung von Dateien werden im Gesundheits- und Sozialwesen generell mit den Standardports unterstützt:

- FTP (File Transfer Protocol) gemäß RFC 959 über die Ports 20 und 21
- FTPS (FTP über SSL) gemäß RFC 4217 über Port 990
- SFTP (SSH File Transfer Protocol) gemäß IETF über Port 22

Die Datenannahme erfolgt ausschließlich per File-Upload über das FTP-Protokoll. Hierfür stellt der Server der Annahmestelle eine entsprechende FTP-Schnittstelle zur Verfügung.

Bei FTPS ist ein digitales Server-Zertifikat für SSL notwendig. Bei erfolgreichem Sitzungsaufbau erfolgt die Übermittlung der Dateien in einem symmetrischen SSL-Tunnel.

Die Anforderungen an diese Zertifikate sind in der Security Schnittstelle für das Gesundheits- und Sozialwesen festgelegt.

Auf der Client-Seite ist für die Nutzung des Systems neben einem Internet- oder Direktwahlzugang als Mindestanforderung auch ein RFC 959-kompatibles FTP-Uploadwerkzeug erforderlich, welches zumeist auch durch das Betriebssystem vorgegeben ist.

Die Verwendung weiterer Protokollvarianten der FTP-Protokollfamilie bedarf einer bilateralen Absprache zwischen den Partnern.

4. Verfahrensbeschreibung

4.1 Voraussetzungen

Es wird ein Verfahren zur Kommunikation über das Internet sowie über Direktwahlleitung vorgeschlagen. Das dabei eingesetzte Kommunikationsprotokoll ist in RFC 765 (IEN 149) sowie 959 beschrieben und wird im Allgemeinen als FTP-Upload auf TCP/IP-Basis bezeichnet. Die FTP-Sicherheitserweiterungen („FTP Security Extensions"), beschrieben in RFC 2228, können optional Anwendung finden.

Die bisherige elektronische Kommunikation zwischen Arbeitgebern, Leistungserbringern und Annahmestellen ist dateiorientiert. Es werden eine Nutzdaten-Datei mit den eigentlichen Nachrichten und ein Auftragssatz mit Routinginformationen gebildet. Dieses Verfahren wird beibehalten. Es ist in den Gemeinsamen Grundsätzen Technik definiert und wird als KKS (Krankenkassen-Kommunikations-System) bezeichnet.

Um zu verhindern, dass Nutzdaten verfälscht oder von Unberechtigten gelesen werden, werden sie verschlüsselt. Hier werden im Gesundheits- und Sozialwesen etablierte Verfahren verwendet, die jeweils gültige Security Schnittstelle ist bindend. Die Kommunikation setzt voraus, dass der Absender bereits über ein gültiges Zertifikat verfügt und somit die Möglichkeit der Verschlüsselung nutzen kann.

4.2 Das Übermittlungsverfahren

Gemäß der Security Schnittstelle verschlüsselt der Sender die Datei für den Empfänger, erstellt den dazugehörigen Auftragssatz und überträgt die Dateien mittels FTP-Upload zu einem Server des Empfängers im Internet oder per Direktwahlleitung.

Der Absender identifiziert sich auf dem FTP-Server durch Anmeldung mit Username und Kennwort (z.B. seiner Betriebsnummer bzw. seinem Institutionskennzeichen). Die Anmeldung erfolgt case-sensitive, d. h. es ist die Groß-/Kleinschreibung zu beachten (z.B.: „BN12345678" bzw. „IK123456789").

In einer Session sollten die Dateien immer paarweise (eine Nutzdaten- und eine Auftragssatzdatei) übertragen werden. Vor Versand muss die Eindeutigkeit des verwendeten Transfernamens durch den Absender durch Verwendung der 3-stelligen TRANSFER_NUMMER (Stelle 25-27) sichergestellt werden.

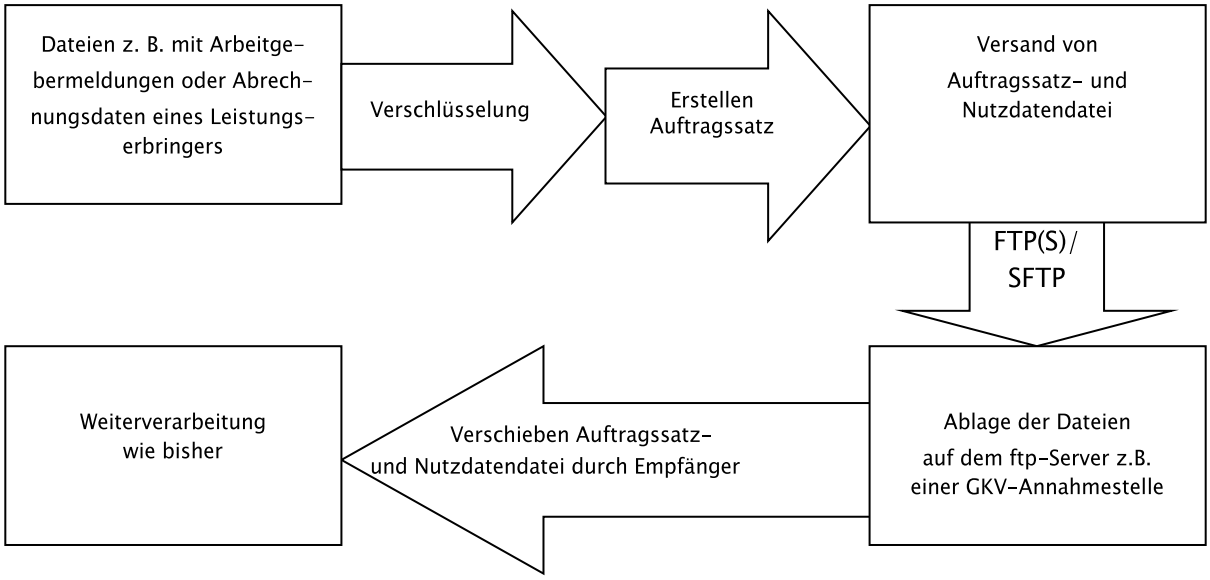
Die Übertragung der Dateien muss im Binary Mode durchgeführt werden, damit die verschlüsselten Dateien fehlerfrei für die weitere Verarbeitung übertragen werden. Die Nutzdaten-Datei wird als erste Datei versendet, nach erfolgreicher Übertragung der Nutzdaten-Datei wird die Auftragssatzdatei versendet. Falls es bei der Übertragung der Nutzdatendatei zu einem Verbindungsab-

bruch kommt, ist diese mit der gleichen TRANSFER_NUMMER erneut zu übertragen. Falls es bei der Übertragung der Auftragssatzdatei zu einem Verbindungsabbruch kommt, ist diese ebenfalls neu zu übertragen.

Daraus resultiert, dass der ftp-Client Überschreibrechte auf dem Zielverzeichnis haben muss.

Nach dem Ende des Upload-Prozesses ist der jeweilige Return-Code pro Datei vom Absender (Uploader) auszuwerten. Eine erfolgreiche Beendigung des Transfers wird durch den Return-Code 226 vom empfangenden System bestätigt.

Das Übermittlungsverfahren erfolgt gemäß nachfolgender Abbildung:



4.3 Prüfungen

Die Daten-Annahmestelle führt bei Vorliegen eines Dateipaares zeitnah folgende Prüfungen durch:

Nr.	Prüfung
1.	zwei Anlagen pro Übertragung (Nutzdaten-/Auftragsdatei)
2.	gleicher Name Nutzdaten- und Auftragsdatei (Extension der Nutzdaten-Datei wird ignoriert)
3.	Länge Auftragsdatei 348 Byte
4.	Namenskonventionen gemäß den Richtlinien zum Datenaustausch
5.	Korrekter Eintrag der Zieladresse im Auftragssatz

In Abhängigkeit von dem Ergebnis der Prüfungen wird das Dateipaar zur Verarbeitung weitergeleitet. Das Dateipaar ist für die Annahmestelle zur Weiterverarbeitung markiert und wird dort nach Eingangsprüfung und Verschiebevorgang automatisch weiterverarbeitet.

4.4 Rückmeldungen der Eingangsquittung

Es ist zu beachten, dass der Annahmeserver jedoch bei diesem Transferverfahren, entgegen anderer Übermittlungsspezifikationen, keine direkte Quittung erstellen kann, die das Eintreffen der Daten bestätigt bzw. fehlerhafte Datenlieferungen ausweist. Daher ist es erforderlich, durch einen Medienwechsel die Möglichkeit einer Quittierung darzubieten.

Zu diesem Zweck bieten sich zwei Alternativen an, die jeweils optional und nur nach bilateraler Absprache anzuwenden sind:

Alternative 1:

Die E-Mail-Adresse in Feld E-MAIL-ADRESSE EIGNER der Auftragsdatei (Stellen 275-318) kann als Antwortadresse für eine Quittung und/oder Fehlermeldung benutzt werden. Der Aufbau der zu generierenden E-Mail orientiert sich an der jeweils gültigen E-Mail-Spezifikation.

Alternative 2:

Der Annahmeserver kann nach Eingangsprüfung des Dateipaares eine gleichnamige ASCII-Datei mit der Extension „.QUIT“ in das Anmeldeverzeichnis des Users einstellen. Diese Eingangsquittung bestätigt dem Sender die Übernahme in das Verarbeitungssystem.

Falls bei Eingangsprüfung ein Fehler festgestellt wird, kann eine gleichnamige ASCII-Datei mit der Extension „.FEHL“ in das Anmeldeverzeichnis des Users eingestellt werden. Die Fehl-Datei enthält die Gründe für die Abweisung der Datenlieferung zur Übernahme in das Verarbeitungssystem. Der Aufbau der zu generierenden Datei als Eingangsquittung bzw. Fehlerdatei orientiert sich an der jeweils gültigen E-Mail-Spezifikation.

Die Rückantwort bezieht sich auf die durchgeführten formellen Prüfungen bei der Datenannahme, bevor die Dateien in die Fachverarbeitung übernommen wurden. Die Struktur der Antwort ist durch die jeweils aktuelle Fassung der „Spezifikation für die Übermittlung von Nachrichten mittels E-Mail (Anlage 7)“ vorgegeben.

4.5 Weiterverarbeitung der übermittelten Dateien

Die Verschlüsselung muss den Vorgaben aus der jeweils aktuellen Security Schnittstelle für das Gesundheits- und Sozialwesen entsprechen.

Die Dateien werden in das (Anmelde-)Dateisystem des Annahmeservers übertragen und auf Konsistenz geprüft. Die Dateipaare, die eindeutig benannt sind, werden per Filetransfer automatisch auf die Verarbeitungsrechner der Annahmestellen weitergeleitet und wie bisher verarbeitet, d. h. die Dateien werden entschlüsselt und die Nachrichten verarbeitet.

Der Annahmestelle (dem Betreiber des FTP-Servers) obliegt die Pflicht, die Upload-Verzeichnisse unverzüglich nach abgebrochenen und fertig gestellten Transfers zu durchsuchen und zu bereinigen. Hierdurch hat der Server-Betreiber sicherzustellen, dass zu einem Upload stets ausreichend viele, freie (unbenutzte bzw. nicht-vergebene) Transfernummern zur Verfügung stehen.

Evtl. vorhandene Dateien mit den Extensionen „.QUIT“ bzw. „.FEHL“ werden durch den Absender (Uploader) nach Verarbeitung gelöscht. Bei Vernachlässigung dieser Pflicht des Absenders oder Beeinträchtigung des Betriebes ist die Annahmestelle berechtigt, diese Dateien ohne Absprache nach eigenständigem Ermessen zu löschen.

Es steht dem Server-Betreiber frei, userspezifisch andere Upload-Verzeichnisse zu verwenden (und zuzuweisen) als das Wurzelverzeichnis der Absenderkennung (d. h. Home-Verzeichnis ungleich Root-Verzeichnis), um z. B. das Überschreiben von fremden Dateien bei Nutzung eines gemeinsamen Upload-Verzeichnisses zu verhindern. In jedem Fall muss der Upload in dem Verzeichnis stattfinden, das dem Absender nach der Anmeldung am Annahmeserver zugewiesen wird.

5. Anhang

5.1 Numerische Aufstellung RFC-konformer FTP-Returncodes:

110	Restart marker reply. In this case, the text is exact and not left to the particular implementation; it must read: MARK yyyy = mmmm Where yyyy is User-process data stream marker, and mmmm server's equivalent marker (note the spaces between markers and "=").
120	Service ready in nnn minutes.
125	Data connection already open; transfer starting.
150	File status okay; about to open data connection.
200	Command okay.
202	Command not implemented, superfluous at this site.
211	System status, or system help reply.
212	Directory status.
213	File status.
214	Help message. On how to use the server or the meaning of a particular non-standard command. This reply is useful only to the human user.
215	NAME system type. Where NAME is an official system name from the list in the Assigned Numbers document.
220	Service ready for new user.
221	Service closing control connection. Logged out if appropriate.
225	Data connection open; no transfer in progress.
226	Closing data connection. Requested file action successful (for example, file transfer or file abort).
227	Entering Passive Mode (h1,h2,h3,h4,p1,p2).
230	User logged in, proceed.
250	Requested file action okay, completed.
257	"PATHNAME" created.
331	User name okay, need password.
332	Need account for login.
350	Requested file action pending further information.
421	Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
425	Can't open data connection.
426	Connection closed; transfer aborted.
450	Requested file action not taken. File unavailable (e.g., file busy).
451	Requested action aborted: local error in processing.
452	Requested action not taken. Insufficient storage space in system.
500	Syntax error, command unrecognized. This may include errors such as command line too long.

501	Syntax error in parameters or arguments.
502	Command not implemented.
503	Bad sequence of commands.
504	Command not implemented for that parameter.
530	Not logged in.
532	Need account for storing files.
550	Requested action not taken. File unavailable (e.g., file not found, no access).
551	Requested action aborted: page type unknown.
552	Requested file action aborted. Exceeded storage allocation (for current directory or dataset).
553	Requested action not taken. File name not allowed.

5.2 Literaturverweise:

[1] RFC 959 File Transfer Protocol http://tools.ietf.org/html/rfc959

[2] RFC 2228 FTP Security Extensions http://tools.ietf.org/html/rfc2228

[3] SSH File Transfer Protocol http://tools.ietf.org/wg/secsh/draft-ietf-secsh-filexfer

[4] RFC 4217 FTP over TLS http://tools.ietf.org/html/rfc4217

[5] Wikipedia http://de.wikipedia.org/wiki/File_Transfer_Protocol
http://de.wikipedia.org/wiki/SSH_File_Transfer_Protocol