Handbuch FDS

File Delivery Services

SFTP Filetransfer

Herausgeber

Post CH AG
Informatik
Webergutstrasse 12
CH-3030 Bern (Zollikofen)

Kontakt

Post CH AG
Informatik
Webergutstrasse 12
CH-3030 Bern (Zollikofen)
IT17.34 FDS Betrieb
E-Mail: fds@post.ch

Version 8.5 / Januar 2023

Download der aktuellen Version: https://www.post.ch/fds

Inhaltsverzeichnis

1. Einleitung

Der File Delivery Services (FDS) ist ein Dienstleistungsangebot des Servicebereichs Informatik der Post CH AG.

FDS spielt die Rolle eines Gateways im IT-Sicherheitssystem zwischen dem Intranet der Schweizerischen Post und den externen Netzwerken und ermöglicht das gegenseitige Austauschen von Dateien zwischen postinternen und externen Partnern sowie Applikationen.

Dieses Handbuch beschreibt, wie Dateien mit dem FDS-Server der Post CH AG ausgetauscht werden können. Der Service steht allen Benutzern zur Verfügung, die auf ihrem Computer einen sftp Filetransfer-Client installiert haben und über den nötigen Account verfügen.

Informatik Post übernimmt für die Richtigkeit der hier gemachten Angaben keine Gewähr. Irrtum und Änderungen bleiben vorbehalten.

2. Das FDS-Modell der Schweizerischen Post

2.1 Überblick

Die Geburtsstunde des FDS liegt im Jahre 1993. Es wurde im Rahmen des DFÜ-C Projekts der damaligen PostFinance Organisation ins Leben gerufen. Die ersten Filetransfers erfolgten mit Kermit, FTP und FTAM. Im Jahr 1995 wurde der Service für den Filetransfer mit CONNECT:Direct™ erweitert. Im Jahr 2002 wurde FDS mit dem FDS-SSH System (FTP über SSH auch Secure FTP genannt) ausgebaut, während inzwischen die Protokolle FTAM und Kermit nicht mehr angeboten wurden.

2007 kam es mit der Einführung von SFTP (SSH File Transfer Protocol) zu einem Technologie- und Generationenwechsel. Mit dieser Einführung wurde der FDS-SSH Service hinfällig und Mitte 2010 eingestellt.

Seit Juni 2015 ist der Einsatz vom Protokoll FTP über Internet aus Sicherheitsgründen (Übermittlung der Daten sowie von Benutzername und Passwort im Klartext) nicht mehr zulässig. Die bestehenden Benutzer wurden bis Ende 2018 auf Protokoll SFTP umgestellt.

2.2 unterstütztes Protokoll

- SFTP (SSH File Transfer Protocol)

2.3 Anschlussarten

Es werden 3 Anschlussarten angeboten:

- Internet
- MPLS/IPSS — Mietleitungen, IPSS Netz der Swisscom
- Intranet — für postinterne Partner/Applikationen

Für neue Mietleitungen und MPLS muss beim gewünschten Termin der Installationstermin des Netzanbieters berücksichtigt werden. Mietleitungen werden dann eingesetzt, wenn ein anderer Anschluss teurer als eine Mietleitung wird, oder wenn spezielle Sicherheitsanforderungen diese notwendig machen. ADSL-Verbindungen sind nur mit einem Provider über das Internet möglich. Mit dem Einsatz von SFTP ist die Nutzung von Mietleitungen und VPN Verbindungen entbehrlich und bringt keine zusätzliche Sicherheit.

3. Die FDS Services

3.1 Die File Delivery Services

Die File Delivery Services basieren auf einem speziellen Mailboxing System, welches den erhöhten Sicherheitsanforderungen im Umfeld Internet, Extranet und Intranet gerecht wird.

3.2 Wo stehen die File Delivery Services?

Die FDS setzen sich aus mehreren Applikationsserver, Datenbankserver und Perimeter-Servern zusammen. Alle Komponenten stehen in verschiedenen Zonen (DMZ) der IX-Plattform. Die IX-Plattform ist die mit Firewalls geschützte Sicherheitszone zwischen dem Postnetz (Intranet) und den externen Netzen (Internet, Mietleitungen). Die Filetransfer- und Datenbankserver stehen in einer hoch geschützten Zone, in die der Zugriff nur sehr beschränkt möglich ist. Die Perimeter-Server stehen in weniger hoch geschützten Zonen, in die der Zugriff mit Clients erlaubt ist. Die Client/Server Verbindungen aus den externen Netzwerken und aus dem internen Postnetz laufen immer über die Perimeter-Server. Der FDS ist georedundant ausgelegt und steht bei einem allfälligen Ausfall eines Rechenzentrums weiter zur Verfügung.

3.3 Filetransferprotokoll

Mehr detaillierte Informationen sind in unserem „File Transfer Clients Handbuch“ auf https://www.post.ch/fds zu finden.

3.3.1 SFTP

SFTP (SSH Secure File Transfer Protocol) ist ein sicheres Filetransferprotokoll. Zwischen Client und Server wird eine ununterbrochene verschlüsselte Verbindung hergestellt, welche die Daten und Benutzernamen für einen Angreifer unlesbar machen. Zudem ermöglicht die Key-Authentifizierung, dass sich Clients ohne Benutzerinteraktion auf dem Server einloggen können. SSH garantiert das vollständige und unveränderte Übertragen der Daten vom Absender zum Empfänger. Unterstützt wird nur SSH-2 (Version 2) und ausschliesslich Key-Authentifizierung.

Mit einem **SFTP** Client kann mit dem FDS SFTP-Server eine Verbindung aufgenommen und die nötigen Kommandos ausgeführt werden.

Achtung: SFTP ist nicht mit FTPS (FTP über SSL) oder mit FTP über SSH (manchmal Secure FTP genannt) zu verwechseln.

3.4 Auslieferung und Abholung von externen Servern

Wenn gewünscht wird, dass der FDS-Service die Dateien zustellt oder beim Kunden abholt, müssen einige Voraussetzungen erfüllt sein. Diese Voraussetzungen sind im Kapitel 6 aufgeführt.

Die Auslieferung und Verteilung einer Datei erfolgt ereignisorientiert. Nach dem Eingang einer Datei wird diese vom FDS-Server an die vorbestimmten Destinationen weitergeleitet. Die Festlegung eines bestimmten Zeitpunktes für die Ausführung einer Aktion ist nicht möglich.

3.5 Benutzung des File Delivery Service

Die administrative Anmeldung für die Nutzung des FDS Services erfolgt über den Kundendienst des Service- oder Geschäftsbereichs der Schweizerischen Post.

Dringende Probleme nach der Inbetriebnahme können an unsere Hotline (+41 (0)848 800 030) eskaliert werden.
Für Anfragen betreffend File Delivery Services steht die folgende Email-Adresse zu Verfügung: fds@post.ch

4. Sicherheit

4.1 Benutzernamen (Login)

Externe Teilnehmer erhalten je Service- und Geschäftsbereich eigene Benutzernamen. Setzt ein Kunde für mehrere Geschäftsbereiche seiner Firma ein und denselben Benutzernamen ein, übernimmt die Post CH AG keine Haftung für entstandene Schäden, welche durch den möglichen übergreifenden Zugriff auf Daten des Filetransfer-Servers der Post entstehen können.

4.2 Link-Verschlüsselung

Die Link-Verschlüsselung ist keine Standarddienstleistung der FDS-Services. Sie kann aber als Netzwerk-Option genutzt werden. Mit der Nutzung von SFTP ist die zusätzliche Link-Verschlüsselung entbehrlich und die Verbindung kann auch ohne Verlust an Sicherheit über das Internet aufgebaut werden.

4.2.1 Für alle Verbindungsarten

Für eine Client-to-Server Verschlüsselung steht das Protokoll SFTP für alle Verbindungsarten zur Verfügung.

4.2.2 MPLS/IPSS

Mit MPLS/IPSS kann eine Link-Verschlüsselung gemacht werden.

4.2.3 LAN-LAN

Bei LAN-LAN Verbindungen kann mit den beiden Routern eine Linkverschlüsselung aufgebaut werden.

5. Konfigurationen

5.1 FDS Client-Server Konfiguration

5.1.1 Filetransfer Server

Zone	Hostname
Internet und Mietleitungen	fdsbc.post.ch
Postnetz/DMZ	fdsbc.pnet.ch

Die Verteilung der Kommunikation über zwei Standorte wird mittels DNS Loadbalancing (Round-Robin) erreicht. Dies bedeutet, dass abwechselnd die IP-Adressen der beiden Standorte zurückgegeben werden.

Es muss sichergestellt werden, dass die Kommunikation zu - oder ab FDS in Ihrem Netzwerk erlaubt ist. In vielen Fällen muss das Netzwerk-Team die Verbindungen mit entsprechenden Firewall-Regeln erlauben.
Es werden zwei IP-Adressen verwendet. Die IP-Adressen dürfen nur für die Konfiguration von Firewall-Regeln verwendet werden. Für den Verbindungsaufbau ist zwingend der DNS-Name zu benutzen.

Die beiden IP-Adressen können mittels DNS-Auflösung (*nslookup fdsbc.post.ch*) durch mehrere Versuche ermittelt werden.

FDS unterstützt IPv4 und IPv6. Die Verwendung von IPv6 erfordert durchgehende IPv6-Unterstützung in Ihrer Infrastruktur.

5.1.2 DNS Caching
Die Plattform wird mit einer Active / Active Konfiguration über zwei Standorte betrieben. Der Failover-Mechanismus wird mit einer „Global Server Load Balancing (GSLB)" Infrastruktur sichergestellt. Damit Sie von einem raschen Failover der Verbindung zu FDS profitieren können, müssen Sie in Ihrer Umgebung sicherstellen, dass kein zusätzliches DNS-Caching gemacht wird. Die Time to live (TTL) Angabe vom Post-DNS muss zwingend respektiert werden.

5.1.3 Ports
Das FDS Protokoll läuft auf Standard-Port 22.

5.1.4 Benutzernamen (Login)
Der Benutzername wird im Rahmen der Service Bestellung kommuniziert.

5.1.5 Verzeichnisse
Die Namen der Verzeichnisse auf dem FDS Server sind in Kleinbuchstaben und enthalten die folgenden Einschränkungen

- Zeichen: [a-z], [0-9], [. -] (Punkt, Bindestrich)
- Beginn: das erste Zeichen muss [a-z], [0-9] sein

Die Benutzer können die Verzeichnisse weder kreieren noch löschen.

5.1.6 Dateinamen
Für die Namen der Dateien in den Verzeichnissen der FDS-Server sind die folgenden Richtlinien einzuhalten:

- Zeichen: [A-Z], [a-z], [0-9], [. - _] (Punkt, Bindestrich, Unterstrich)

5.2 SFTP

5.2.1 Allgemeines
Detaillierte Informationen sind in unserem „File Transfer Clients Handbuch" auf https://www.post.ch/fds zu finden.

5.2.2 Public-Key an Informatik Post senden

Eine Kopie des Public-Keys muss der Post per E-Mail (fds@post.ch) zugestellt werden. Damit der erhaltene Key auf Seiten der Post mit dem Absender verifiziert werden kann, muss der Key durch die Kontaktperson geschickt werden (oder diese muss im E-Mail-Austausch vorkommen).

Falls erwünscht, besteht die Möglichkeit, mehrere Public-Keys für den gleichen Benutzernamen zu konfigurieren. Ebenso können mehrere Benutzer den gleichen Key benutzen.

Der SSH Key muss mindestens 4096 bit lang sein.

5.2.3 Umgang mit Keys

Behandeln Sie Ihren Private-Key wie ihre persönliche Kreditkarte! Schützen Sie ihn vor unberechtigten Zugriffen.

6. Anhang A. Informationen zur Anwendung FDS

Die vorliegende Kurzinformation beschreibt den Datenaustausch und die Funktionen von FDS und stellt allgemein gültige Regeln und Vorgaben für die Übertragung von Dateien mit den FDS Filetransfer-Servern auf. Es richtet sich an die FDS-Benutzer der Geschäftsbereiche und Konzerngesellschaften der Schweizerischen Post und deren externen Kunden.

6.1 Rahmenbedingungen/Einschränkungen

a) FDS ist kein Archivierungssystem. Abzuholende Dateien, die der Kunde noch nicht gelöscht hat, werden in jedem Fall nach 9 Tagen vom Server automatisch entfernt.

b) Jede Datei kann maximal 20-mal abgeholt werden.

c) FDS hat einen Verarbeitungsrhythmus von 1 Minute. Angelieferte Dateien erscheinen 1 Minuten nach Ende des Filetransfers in der Empfänger-Mailbox. Wenn die Konfiguration es verlangt, dass die Dateien an einem Zielrechner weitergeleitet werden, kann es je nach Filegrösse und Fileanzahl länger dauern.

d) Grosse Files sind, wenn möglich, in komprimierter Form zu übermitteln. Sender und Empfänger (End-to-End) einigen sich über die Komprimierungsmethode (z.B. GZIP).

e) Eine grosse Anzahl Files muss mit einer entsprechend grossen Anzahl von Filetransfers (put/get) pro SFTP Login-Session übertragen werden. Beispiel für 1200 Files: 10 Verbindungen/Logins mit je 120 Filetransfers. Wird die Anzahl der Logins während einer bestimmten Zeiteinheit zu gross, sperrt das Intrusion Prevention System der Post CH AG die verursachende Source IP-Adresse automatisch während 15 Minuten.

f) FDS quittiert dem Absender keine Filetransfers. Das Erstellen und Versenden von Quittungen ist Aufgabe der Empfänger und wird nicht von FDS sichergestellt.

g) Beim Filetransfer ist bei Weiterleitungen keine Übertragungs-Reihenfolge garantiert. Files unterschiedlicher Grösse können sich bei einer parallellaufenden Datenübertragung überholen. Das Empfangssystem der End-to-End Beziehung ist für die Wiederherstellung der richtigen Reihenfolge der übertragenen Files zuständig.

h) Die Weiterleitung und Verteilung von Files ist ereignisgesteuert. Eine zeitliche Steuerung ist nicht möglich.

i) Informatik Post muss bei allen Filetransfers, die über die FDS-Server laufen, frühzeitig über Grösse, Häufigkeit und Volumenänderungen der Files informiert werden. Nur so kann gewährleistet werden, dass die erforderliche Kapazität zur gewünschten Zeit verfügbar ist.

j) Informatik Post muss für alle Filetransfers, die über die FDS-Server laufen, über die Prioritäten im Eskalationsfall informiert werden. Für alle anderen Fälle kommt die Standard SLA zum Tragen.

6.2 Einschränkungen bei der Datenanlieferung (Client → FDS Server)

- Bei einer Upload-Funktion (put) eines Filetransfer-Clients in eine FDS Mailbox (Verzeichnis) werden die Files von den Prozessen auf dem FDS-Server unmittelbar nach Abschluss des Filetransfers bearbeitet. Die Einträge der Files in den Upload-Mailboxen bleiben jedoch für den Kunden während zwei Minuten ersichtlich (Anzeige der Files mittels „dir“ und „ls“). **Die Löschung oder die Umbenennung einer gesendeten Datei ist wirkungslos: diese Datei wird mit dem ursprünglichen Filenamen an den Empfänger weitergeleitet.**
- FDS stellt sicher, dass nur vollständig übermittelte Dateien weiterverarbeitet werden. Im Fall eines Verbindungsabbruchs wird die unvollständige Datei verworfen.
- Eine Änderung der File-Attribute nach dem Filetransfer ist auf FDS nicht möglich.

6.3 Anforderungen bei der Datenauslieferung (FDS Server → Zielsystem)

Damit der FDS-Service Dateien ausliefern kann, müssen beim Post-internen und externen Empfänger die folgenden Anforderungen erfüllt sein:

– permanente Netzwerkverbindungen, wie WAN-Access (MPLS) oder Internet
– das System muss 7x24h verfügbar sein
– ein operativer RZ-Betrieb ist sichergestellt
– Ansprechstellen für den Support (Telefonnummern, E-Mail) und die Erreichbarkeit ist sichergestellt.

6.4 Anforderungen und Einschränkungen bei der Datenabholung

FDS kann automatisch Dateien mit SFTP auf Fremdsystemen abholen.
Diese Funktion soll nur in Ausnahmefällen eingesetzt werden.

Voraussetzungen:
- permanente Netzwerkverbindung, wie WAN-Access (MPLS) oder Internet
- das System muss 7x24h verfügbar sein
- ein operativer RZ-Betrieb ist sichergestellt
– Ansprechstellen für den Support (Telefonnummern, E-Mail) und die Erreichbarkeit ist sichergestellt.

Einschränkungen:
- Dieser Service wird nicht angeboten, wenn zeitkritische Daten in einem Intervall kürzer als 30 Minuten abgeholt werden müssen.
- Die abzuholenden Dateien müssen sich in fix definierten Verzeichnissen befinden. Eine Abholung in variablen Verzeichnissen (z.B. Verzeichnisnamen, die das heutige Datum beinhalten) ist nicht unterstützt.

7. Anhang B. Glossar

D	DMZ	Demilitarisierte Zone – Eine DMZ befindet sich an einem separaten LAN-Anschluss einer Firewall zwischen einem internen Netzwerk und einem unsicheren Netz, z.B. dem Internet. In der DMZ werden häufig Server, die Dienste für Internet-Nutzer (z.B. www oder Mail) zur Verfügung stellen, eingerichtet. Im Idealfall liegt eine DMZ zwischen zwei physikalisch getrennten Firewalls. Die äussere Firewall schützt vor Angriffen von aussen und kontrolliert jeglichen Internet-Zugriff auf die DMZ. Die innere Firewall kontrolliert den Zugriff aus der DMZ in das interne Netzwerk und umgekehrt. Sie stellt somit eine zweite Verteidigungslinie dar, falls die äussere Firewall durchbrochen werden sollte. Dies hat den Vorteil, dass das interne Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum Web-Server gelangt.
	DNS	Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Umsetzung von "Internetadressen" in die zugehörige IP-Adresse.
E	End-to-End	Beziehung zwischen einer Applikation (z.B. EGA-B) eines Geschäftsbereichs der Schweizerischen Post (z.B. PostFinance AG) und der Applikation des externen Kunden.
F	FDS	File Delivery Services ist ein Dienstleistungsangebot des Servicebereichs Informationstechnologie (IT) der Post CH AG. FDS spielt die Rolle eines Proxys im IT-Sicherheitssystem zwischen dem Intranet der Schweizerischen Post und den externen Netzwerken und ermöglicht das gegenseitige Austauschen von Dateien zwischen postinternen und externen Partnern sowie Applikationen.
	FTP	Das File Transfer Protocol ist ein im RFC 959 von 1985 spezifiziertes Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. Es ist ein Protokoll, das es erlaubt Dateien zwischen verschiedenen Rechnern unabhängig von ihrem Betriebssystem und Standort auszutauschen.
I	IPSS	LAN Interconnect over IPSS ist ein Service der Swisscom. Sie kann lokale Netzwerke zu einer einzigen unternehmensweiten Kommunikationsinfrastruktur vernetzen. IPSS ist eine „Swisscom-eigene“ Lösung mit modernster Technologie. Die dabei verwendete MPLS-Technologie (Multi Protocol Label Switching) ermöglicht eine grosse Flexibilität in Bezug auf die Bandbreite. Der Dienst wird vollständig durch Swisscom Enterprise Solution erbracht. http://www.swisscom.com/es/
M	MPLS	Beim Multiprotocol Label Switching (MPLS) handelt es sich um eine Implementation des Label Switching. Bei solchen Verfahren werden die am Transport eines Datenpaketes beteiligten Router stark entlastet, da sich das Komplexitätsniveau auf das eines Switches reduziert. Dies wird erzielt, indem zu Beginn der Datenübertragung ein fester Verbindungsweg eingerichtet wird. Router auf diesem Weg müssen weiterzuleitende Datenpakete nicht mehr auf ihren Empfänger untersuchen, sondern geben diese ohne weitere Bearbeitung entsprechend des zuvor geschalteten Weges weiter.
S	SFTP	SSH File Transfer Protocol (kurz SFTP) ist eine Weiterentwicklung von SCP und erlaubt sichere Datenübertragung und Dateizugriffe von einem Client auf entfernte Systeme. Das Protokoll beinhaltet weder die Authentifizierung noch die Verschlüsselung, diese Funktionen müssen von dem darunterliegenden SSH Protokoll übernommen werden. SFTP ist nicht zu verwechseln mit Secure FTP oder mit FTP über SSL.