Senden von strukturierten Berichten über das SFTP

Häufig gestellte Fragen

Allgemeines

Was versteht man unter SFTP ?

Die Abkürzung SFTP steht für „SSH File Transfer Protocol“ oder „Secure File Transfer Protocol“. Das SFTP ist die Komponente des SSH-Protokolls, die den Datentransfer sichert

Wo findet man das SFTP?

Im Unterschied zu FTP verfügen Windows-Computer nicht über einen Standard-Client. Daher müssen Sie zuerst eine zusätzliche Software installieren.

Über die Suchfunktion (z.B. Suche nach „SFTP Client“) finden Sie im Internet sowohl kostenfreie als auch zahlungspflichtige SFTP-Software-Clients. Linux-Systeme bieten Standardpakete für die Open-Source-Implementierung von SSH (OpenSSH) an.

Ist das SFTP sicher

Das SFTP wird durch Verschlüsselungstechniken geschützt. Das bedeutet, der gesamte Verkehr zwischen einem Client und einem Server, von der Anmeldung bis zum Versand der Dateien, erfolgt vollständig verschlüsselt. Durch diesen Schutz ist das SFTP sehr gut geeignet für den gesicherten Austausch von Dateien über das Internet.

Welche spezifischen Schritte sind für die Verwendung des SFTP erforderlich?

1. Sie müssen eine Zugriffsberechtigung für die gesicherten Anwendungen der Portal-Site der Sozialen Sicherheit haben.
2. Sie müssen über einen SFTP-Client Ihrer Wahl verfügen.
3. Sie generieren in Ihrem SFTP-Client zwei (einen privaten und einen öffentlichen) Schlüssel.
4. Ihr lokaler Mitverwalter meldet sich in der Portal-Site an und wählt unter „Zugriffsverwaltung“ die Option „Verwaltung von strukturierten Berichten“, unter der er den SFTP-Kanal eingeben kann.
5. Der Mitverwalter lädt den in Ihrem SFTP-Client generierten öffentlichen Schlüssel sowie den öffentlichen Schlüssel Ihres qualifizierten Zertifikats.

Wie kann man sich als SFTP-Sender registrieren?

Für die Übermittlung von strukturierten Berichten müssen Sie für jede Funktion, an die Sie senden möchten, zuerst eine Sendernummer generieren.

Nur der lokale Mitverwalter einer jeden Funktion kann eine Sendernummer registrieren.

Es müssen die folgenden Schritte ausgeführt werden:

1. Klicken Sie auf „Strukturierte Berichte“. (*).
2. Klicken Sie auf „Konfigurationsdaten speichern“.
3. Klicken Sie auf „Nächster Schritt“.
4. Geben Sie die Kenndaten des technischen Anwenders ein.
5. Klicken Sie auf „Nächster Schritt“.
6. Wählen Sie den SFTP-Kanaltyp und laden Sie den in Ihrem SFTP-Client generierten öffentlichen Schlüssel.
7. Klicken Sie auf „Nächster Schritt“.
8. Laden Sie den öffentlichen Schlüssel Ihres qualifizierten Zertifikats (Erweiterung: .cer).
9. Geben Sie in der Liste der Anwendungen an, wohin Sie über das SFTP senden möchten.
10. Klicken Sie auf „Nächster Schritt“.
11. Wählen Sie für den technischen Anwender einen Benutzernamen aus. Klicken Sie auf „Nächster Schritt“.
12. Klicken Sie auf „Bestätigen“.

(*) Falls Sie bereits einen Isabel-Kanal festgelegt haben, überspringen Sie die Schritte 2 bis 5 und klicken rechts im Bildschirm unter Punkt 6 auf das Pluszeichen neben dem SFTP.

Welchen Benutzernamen und welches Passwort muss man für das Senden über das SFTP verwenden?

Bei der Aktivierung des SFTP-Kanals Ihrer Sendernummer muss Ihr lokaler Mitverwalter auf der Portal-Site einen Benutzernamen wählen. Für das Senden über das SFTP müssen Sie kein Passwort festlegen.

Zertifikate

Wie generiert man die beiden (den privaten und den öffentlichen) Schlüssel?

SFTP hat ein eigenes Schlüsselformat. Diese Schlüssel können Sie nicht wie ein Zertifikat kaufen, sondern müssen von Ihnen generiert werden. Fast jede SFTP-Client-Software bietet die Möglichkeit der Generierung eines SSH-Schlüsselpaars.

Falls der von Ihnen gewählte SFTP-Client kein Modul für das Generieren von Schlüsseln bietet, können Sie aus dem Internet ein entsprechendes Programm herunterladen. Mit einer Suchmaschine (beispielsweise unter dem Suchbegriff „ssh key generator“) finden Sie im Internet Programme, mit denen Sie die SSH-Schlüssel generieren können. Den öffentlichen Teil Ihres Schlüssels müssen Sie über Ihre Sendernummer in die Portal-Site der Sozialen Sicherheit laden.
Den privaten Teil dieses Schlüssels laden Sie in Ihren SFTP-Client. Der Speicherort Ihres privaten Schlüssels ist abhängig von dem von Ihnen genutzten SFTP-Client. Entsprechende Informationen enthält die Dokumentation Ihres SFTP-Client.

Welche Schlüsselpaarversion muss generiert werden?

Es wird unterschieden zwischen Schlüsseln, die mit Version 1 und die mit Version 2 von SHH kompatibel sind. Da die Version 1 als unsicher gilt, wird diese nicht akzeptiert. Ausschließlich die Version 2 wird akzeptiert.

Für öffentliche Schlüssel werden ausschließlich die Formate von OpenSSH und SSH unterstützt.

Sie müssen bei der Generierung der Schlüssel darauf achten, den richtigen Schlüsseltyp und die richtige Schlüssellänge zu wählen.

Es stehen zwei Typen (RSA und DSA) zur Auswahl, von denen ausschließlich RSA akzeptiert wird.

Als Schlüssellänge wählen Sie 2048 oder höher (3072, 4096). Kürzere Schlüssel werden nicht akzeptiert.

Wir empfehlen, bei der Speicherung der Schlüssel den privaten Schlüssel mit einem Passwort zu schützen.

Kurze Zusammenfassung:

- mit SSH Version 2 kompatible Schlüssel
- die Formate OpenSSH und SSH
- Schlüsseltyp: RSA,
- Schlüssellänge: 2048<Länge<4096

Was bedeutet die Fehlermeldung „Falsche Länge des SSH-Schlüssels“ bei der Festlegung der Sendernummer für das SFTP?

Die Schlüssellänge muss mindestens 2048 Bit und darf maximal 4096 Bits umfassen.
Kürzere oder längere Schlüssel werden nicht akzeptiert.
Zur Behebung des Fehlers muss ein neues Schlüsselpaar mit einer Länge von mindestens 2048 bis höchstens 4096 Bit festgelegt werden

Was bedeutet die Fehlermeldung „Ungültiger SSH-Schlüssel“ bei der Festlegung der Sendernummer für SFTP?

Dieser Fehler kann verschiedene Ursachen haben:

- Sie haben versucht, Ihren privaten statt öffentlichen Schlüssel zu laden. Lösung: Laden Sie Ihren öffentlichen Schlüssel.
- Sie haben Ihren öffentlichen Schlüssel in einem falschen Format generiert (z.B. SSH1-RSA oder SSH2-DSA) Lösung: Generieren Sie Ihre Schlüssel im Format SSH2-RSA.

Wie wird der öffentliche SSH-Schlüssel übertragen?

Ihr lokaler Mitverwalter muss Ihren öffentlichen SSH-Schlüssel anhand Ihrer Sendernummer in die Portal-Site laden.

Bericht senden

Wie sendet man einen strukturierten Bericht?

1. Stellen Sie mit Ihrem SFTP-Client eine Verbindung mit sftp.socialsecurity.be (eine einmalige Anmeldung, der Host-Key des Servers) her.
2. Identifizieren Sie sich mit Ihrem technischen Benutzernamen (UMxxxxxx oder EXPxxxxxx) und privaten SSH-Schlüssel. Geben Sie das Passwort ein, mit dem Ihr privater Schlüssel geschützt ist.
3. Laden Sie Ihre Dateien (FI, FS und Go) in das IN-Verzeichnis (für Circuit-Testdateien das INTEST-Verzeichnis, für Meldungstestdateien das INTEST-S-Verzeichnis)

Nach der Verarbeitung und Prüfung Ihrer Dateien werden im OUT-Verzeichnis Akzeptanz- (ACRF) und Benachrichtigungsdateien für Sie bereitgestellt (für Circuit-Testdateien im OUTTEST-Verzeichnis, für Meldungstestdateien im OUTTEST-S-Verzeichnis).

Ist die Dateigröße beschränkt?

Zur Kontrolle der Signatur ist die Dateigröße auf 200 MB beschränkt.

Welche Dateien müssen den strukturierten Berichten angehängt werden?

Beim Senden über das SFTP müssen Sie gemeinsam mit Ihrer Meldungsdatei (FI) auch eine Signaturdatei (FS-Datei) und eine GO-Datei senden.**Falls nicht, wie sind diese dann beschaffen?**

Die Meldungsdateien (FI-Dateien) sind bei jedem verwendeten Sendekanal identisch.
Sowohl die Struktur als auch der Name der Dateien bleiben unverändert

Verbindungen

Kann das SFTP über eine Standleitung verwendet werden?

Diese Möglichkeit ist zurzeit nicht vorgesehen.

Host

Der Host-Name ist sftp.socialsecurity.be.
Die Port-Nummer ist 8022.

Wie richtet man einen SFTP-Client ein?

1. Geben Sie den Host-Namen unter sftp.socialsecurity.be ein
2. Geben Sie die Host-Nummer 8022 ein.
3. Geben Sie den Benutzernamen des technischen Anwenders ein.
4. Laden Sie Ihren privaten SSH-Schlüssel.