Dokumentation zu SFTP

SFTP steht für SSH File Transfer Protocol bzw. auch Secure File Transfer Protocol. Es handelt sich dabei um ein Dateiübertragungsprotokoll, das eine Verschlüsselung ermöglicht, wenn Inhalte auf einen speziellen FTP-Server übertragen werden. Dies gelingt aufgrund des *Secure Shell Netzwerkprotokolls (SSH)*. Das SSH-Protokoll stellt sicher, dass zwei Rechner in einem nicht gesicherten Netzwerk trotzdem über eine sichere, authentifizierte und verschlüsselte Verbindung miteinander kommunizieren können.

Funktionsweise

Ziel ist es, Ihnen einen vertrauenswürdigeren Weg der Datenanlieferung bereitzustellen. Hierfür wurde ein SFTP-Server eingerichtet, auf den Ihre Daten in Form einer csv-Datei übertragen werden sollen. Bitte beachten Sie hier die folgenden Einstellungen.

Anlieferung von MiFID Daten:

prod.import.wmgruppe.de (194.187.221.157) bzw.
test.import.wmgruppe.de (194.187.221.156)[1]
Protokoll / Port / Einschränkung: SFTP, tcp/2222, ssh-key only

Anlieferung von Daten zur Prospektverordnung:

prod.pvo.import.wmgruppe.de = 194.187.221.154
test.pvo.import.wmgruppe.de=194.187.221.155
Protokoll / Port / Einschränkung: SFTP, tcp/2222, ssh-key only

Es ist wichtig, dass der genannte **Port 2222 nicht durch Ihre Firewall blockiert** wird. Für den Upload ist dann die Autorisierung mittels Login-Daten nötig, die Ihnen von WM mitgeteilt werden. Während die Eingabe und Übertragung Ihres Kennwortes bei einer herkömmlichen FTP-Verbindung im Klartext geschieht, erfolgt bei einer SFTP-Verbindung dagegen eine Verschlüsselung. Somit sind sowohl Ihre gesendeten Daten als auch Ihr übermitteltes Passwort jederzeit geschützt.

Vor der Einrichtung der Verbindung müssen Sie zunächst ein sogenanntes Schlüsselpaar erzeugen. Nutzen Sie hierfür zum Beispiel das kostenfreie Programm *PuTTYgen*, das Sie online beziehen können. Eine detaillierte Anleitung zur Erzeugung eines Paares aus Public Key und Private Key folgt nach diesem Abschnitt.

Der Vorteil der Authentifizierung mittels Public Key liegt aber nicht nur in der erhöhten Sicherheit. Dieses Verfahren ermöglicht darüber hinaus eine Einmalanmeldung, wonach ein passwortfreier, automatisierter Datenaustausch zwischen Ihnen und dem SFTP-Server stattfinden kann.

[1] Sie als Bestandskunde haben wir direkt für die Produktion freigeschaltet. Ein Test ist aus unserer Sicht nicht notwendig, könnte im Vorfeld aber durchgeführt werden.

Erzeugung eines neuen Schlüsselpaares

Um ein neues Schlüsselpaar zu generieren, müssen Sie im Programm PuTTYgen zunächst die erforderlichen Parameter einstellen. Dazu gehören die Schlüssellänge (4096 Bits) und die Schlüsselart (RSA, SSH-2, ECDSA und ED25519).

Im nächsten Schritt betätigen Sie den Generate-Button, um das Schlüsselpaar zu erzeugen. Bitte bewegen Sie danach den Mauszeiger, damit das Programm Zufallswerte ermitteln und für die Schlüsselgenerierung nutzen kann. Nun können Sie noch einen Kommentar ergänzen (optional) und eine Passphrase festlegen (erforderlich). Damit wird Ihr privater Schlüssel verschlüsselt, um ihn sicher auf Ihrer Festplatte speichern zu können. Beachten Sie, dass Sie die Passphrase einmal festlegen und in der nächsten Zeile zu Ihrer Sicherheit exakt wiederholen müssen.

Weiteres Vorgehen

Nachdem Sie das Schlüsselpaar erzeugt haben, **schicken Sie bitte den Public Key an** wm-schnittstellenanbindung@wmdaten.de. Wir werden damit diejenigen Ordner für Sie freischalten, an die Sie bisher Daten senden. Teilen Sie uns dafür bitte mit, welche der folgenden Dateitypen Sie an WM übertragen möchten:

1. EMT (European MiFID Template)
2. Standardformat (schließt EMT aus)
    a. Zielmarkt
    b. Zielmarkt Fonds
    c. Kostentransparenz
    d. Kostentransparenz Fonds
    e. Kennzeichen Hebel
    f. Kostentransparenz ex post
3. PRIIPs
4. Daten zur Prospektverordnung-Nachträge