# Anhang 2

# Prozessbeschreibung zum erstmaligen Einrichten der Datendrehscheibe

### Allgemeine Information

Diese Anlage zur Zusatzvereinbarung Produkttransformation regelt Einzelheiten zur Nutzung des für den Transformationsprozess eingerichteten Datenraums ("Datendrehscheibe"). Der Datenaustausch zwischen den Vertragspartnern über die Datendrehscheibe garantiert die Einhaltung der Bestimmungen des Datenschutzes.

#### Nutzungsvoraussetzungen

Je Carrier können höchstens drei Nutzer eingerichtet werden.

Es werden die folgenden Informationen je Nutzer benötigt:

- Carriername
- Name des Nutzers
- Telefon-Nr. des Nutzers
- E-Mail-Adresse des Nutzers

Die Netzwerkverbindung zwischen dem Rechner des Nutzers und der Datendrehscheibe wird über einen "SSH Schlüssel" hergestellt. Einen "SSH Schlüssel" kann der Nutzer über das Programm "Puttygen" generieren. Das Programm "Puttygen" ist im Internet als Freeware erhältlich.

Die auf der Datendrehscheibe bereitgestellten Dateien werden mittels eines personenbezogenen "PGP Schlüssel" verschlüsselt.

Der Datenaustausch erfolgt über einen sFTP-Server, welchen die Telekom kostenfrei zur Verfügung stellt.

Der Zugriff auf den Server erfolgt über einen von dem Carrier zur Verfügung gestellten Schlüssel.

#### Installation und Einrichtung des sFTP Client

Wenn noch kein SFTP Client eingerichtet ist, muss der Nutzer diesen zunächst im Internet unter: <u>https://winscp.net/eng/docs/lang:de#winscp</u> herunterladen und installieren. Die Software ist kostenlos erhältlich.

Der Nutzer muss folgende Parameter in der Anmeldemaske von WinSCP eintragen:

- Rechnername: IP-Adresse 94.100.247.67 oder Rechnername: ae7lh108
- Benutzername: **DM\_IPT\_[Carriername]** (unter "[Carriername]" gibt der Nutzer die zutreffende Firmierung ein)
- Kennwort (optional): Eingabe eines Kennworts nur, wenn bei der Erzeugung des privaten Schlüssels mit dem Tool "Puttygen" ein Kennwort vergeben wurde

#### Anlage zur ZV Produkttransformation Vertraulich

🛒 Neues Verbindungsziel	Sitzung Übertragungsprotokoll:	
	Rechnername:	Portnummer:
	94.100.247.67	22 💌
	Benutzername: Ke	nnwort:
	DM_IPT_[Carriername]	Francisco P
	Speichern V	Erweitert

Darstellung der Anmeldemaske für WinSCP

Im Anschluss muss der Nutzer die folgenden erweiterten Einstellungen vornehmen:

• Unter "Umgebung ->Verzeichnisse" gibt der Nutzer als entferntes Verzeichnis "/OUT" ein.

Erweiterte Einstellungen fü	r Verbindungsziele	? ×	
Umgebung 	Verzeichnisse    Synghronisierter Verzeichniswechsel   Letztes Verzeichnis mgrken   gntferntes Verzeichnis:   /OUT   Jokales Verzeichnis:   Die Explorer-Oberfläche verwendet das lokale Verzeichnis nicht.   Verzeichnis Optionen   Ø Besuchte entfernte Verzeichnisse zwischenspeichern   Ø Verz.wechsel zwischenspeichern   Ø Symbolische Links auflösen		
Earbe	OK Abbrechen	Hilfe	]

• Unter "SSH -> Authentifizierung" fügt der Nutzer die Datei mit dem privaten Schlüssel aus "Puttygen" ein. Hierzu wählt er den Pfad / Dateinamen mit dem privaten Schlüssel aus.

Umgebung 	Autentifizierung komplett umgehen (SSH-2)		
Papierkorb	Authentifizierungseinstellungen		
SFTP	Versuche Autentifizierung über Pagent		
Shell	Versuche TIS oder CryptoCard Authentifizierung (SSH-1)		
Proxy	Versuche 'keyboard-interactive' Authentifizierung (SSH-2)		
Tunnel SSH	V Auf das erste Prompt mit dem Passwort antworten		
Schlüsseltausch	Authentifizierungsparameter		
- Authentifizierung - Fehler Hinweis	Erlaube SSH-Agent Weiterleitung		
	Datei mit privatem Schlüssel:		
	C:\Users\User\Desktop\[Carriername]_private_key.ppk		
	GSSAPI		
	Versuche GSSAPI/SSPI Autentifizierung (SSH-2)		
	Erlaube GSSAPI Berechtigungsübergabe		

## Installation und Einrichtung des privaten Schlüssels mit dem Tool "Puttygen"

Das Tool "Puttygen" ist im Internet unter <u>http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe</u> kostenlos verfügbar. Eine Installation ist nicht notwendig.

Die Datei speichert der Nutzer in einem beliebigen Verzeichnis, z.B. unter "Downloads", ab.

#### Erzeugung von SSH-Schlüsseln

- Um einen Open SSH Schlüssel zu erzeugen, muss der Nutzer nach Programmstart auf die Schaltfläche "Generate" klicken.
- Anschließend muss der Nutzer den Mauszeiger in der grauen Fenstermitte solange bewegen, bis der durch die Bewegung generierte Schlüssel erstellt ist und über die Fortschrittsanzeige angezeigt wird.

#### Anlage zur ZV Produkttransformation Vertraulich

e Key Conversions Help		
Key		
Please generate some randomness by moving	the mouse over the bla	ank area.
Actions		
Actions Generate a public/private key pair		Generate
Actions Generate a public/private key pair Load an existing private key file		Generate
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate: SSH-2 (RSA) ()) SSH-2 RSA	Save public key	Generate Load Save private key H-2 DSA

- Im Feld "Key Comment" trägt der Nutzer ein: **DM\_IPT\_[Carriername]** (unter "[Carriername]" gibt der Nutzer die zutreffende Firmierung ein)
- In den Feldern "Key Passphrase" und "Confirm Passphrase" kann der Nutzer optional ein Passwort vergeben.

ile Key Conversio	ns Help		
Key			
Public key for pasting	into OpenSSH authorized	_keys file:	
sshrsa AAAAB3Nza( +ZIOzWd3hRWNWk +VTM0miwh8CoG7u +hEdff7ifHNu6Z8ab( +1j1AD8o0NC14UbN	C1yc2EAAAABJQAAAQE, DcNyWorsLYo2riJdZeeD &S99w5KYWDWhORXni CH10wuQWpBv5Uwuk IsLxBUTIDswv4D5tN/vM	AptiKOqEsESiU+c0r1p giSEchigtzH904GyL0 K21wQm6vrjk6ySUNE	W0cQVs4lz16Mr 1Qt5A 3igJbWDv8rELzu
Key fingerprint:	ssh-rsa 2048 6c:3f a2:0a df 54:ca 58:b8:11:a2:bb:b9:52:14:e6		
Key comment:	DM_IPT_[Carriemame]		
Key passphrase:			
Confirm passphrase:			
Actions			
Generate a public/priv	vate key pair		Generate
Load an existing priva	te key file		Load
Save the generated k	ey [	Save public key	Save private key
Parameters			
Type of key to genera	te: SSH-2 RSA	O SSI	H-2 DSA
SSH-1 (RSA)			

Sicherung der erzeugten Schlüssel

- Den privaten Schlüssel speichert der Nutzer mit Klick auf die Schaltfläche "Save private Key". Als Dateiname verwendet der Nutzer: [Carriername]\_private\_key.ppk (unter "[Carriername]" gibt der Nutzer die zutreffende Firmierung ein).
- Den öffentlichen Schlüssel speichert der Nutzer mit Klick auf die Schaltfläche "Save Public Key". Als Dateiname verwendet der Nutzer: [Carriername]\_public\_key.pub (unter "[Carriername]" gibt der Nutzer die zutreffende Firmierung ein)

Den öffentlichen Schlüssel übermittelt der Nutzer umgehend dem zuständigen Carrier-Manager der Telekom. Im Anschluss richtet die Telekom unverzüglich den Zugang zur Datendrehscheibe für den Carrier bzw. die jeweiligen Nutzer ein und stellt die weiteren Zugangsdaten "IP-Adresse" und "Benutzername" zur Verfügung.