Edifact – Elektronische Rechnungsübermittlung.

Beschleunigen Sie Ihr Business mit der Rechnung im neuen Standard EDIFACT-Format.

T-Mobile Austria bietet Kunden der elektronischen Rechnung (EDIFACT) eine automatische Zustellung dieser an. Für diese automatisierte Zustellung sind eine Vielzahl von Optionen verfügbar, damit möglichst alle Kundenanforderungen bedient werden können. Im Folgenden werden diese Optionen und Formate beschrieben und die dafür erforderlichen Voraussetzungen dargelegt.

Von Seiten T-Mobile Austria werden 3 verschiedene **Transportlayer** für die Zustellung der EDIFACT Dokumente unterstützt:

- E-Mail
- SCP
- SFTP

Für jeden dieser 3 Transportlayer kann konfiguriert werden, in welchem **Format** die Dateien Übertragen werden sollen. Hier stehen folgende Optionen zur Verfügung:

- Ein gezipptes Tar Archiv – alle Dateien für einen Kunden in einem gezippten tar Archiv –> *.tar.gz
- gezippte Einzeldateien – jedes Dokument in einem Einzigen, gezippten File –> *.gz (Standard)
- Einzeldateien – jedes Dokument in einem Einzigen File

Zusätzlich kann noch eine **Verschlüsselung** aktiviert werden, welche über gpg (GNU Privacy Guard) realisiert wird. Wird eine Verschlüsselung durchgeführt, so wird jede einzelne, zu versendente, Datei vor dem Versand gpg verschlüsselt. Somit wird die Endung *.gpg an den Dateinamen angefügt.

Transportlayer - Voraussetzungen:

1. E-Mail (Typ 1)

E-Mail stellt den einfachsten, aber unsichersten Transport Layer dar. Um einen E-Mail Versand einzurichten muß lediglich die **E-Mail Adresse** des Empfängers (Kunden) bekannt sein. Gerade bei einem E-Mail Versand sollte eine Verschlüsselung der Dateien in Betracht gezogen werden (siehe weiter unten).

2. SCP (Typ 2)

Secure Copy (SCP) ist ein sehr sicherer Transportlayer, welcher die Daten bereits automatisch verschlüsselt überträgt. Eine zusätzliche Verschlüsselung ist daher nicht mehr notwendig - kann aber dennoch eingerichtet werden.

→ Hinweis: Bei der Übertragung mittels SCP werden die einzelnen Dateien (kann auch nur eine sein falls Format 0 konfiguriert ist !) übertragen und danach wird noch ein Kontrollfile geschrieben, welches pro übertragener Datei eine Zeile mit dem Dateinamen enthält. Dies stellt sicher, dass auch alle Dateien korrekt übertragen wurden. Der Kunde darf die übertragenen Dateien erst verwenden, wenn das Kontrollfile übertragen wurde !
Name des Kotrollfiles: **<tma | tra>_<RechnungsDatum(YYYYMMDD)>.ctrl** (Beispiel: tma_20091104.ctrl)

Um SCP zu aktivieren müssen folgende Daten / Voraussetzungen erfüllt sein:

- **Host Adresse** des Kundenrechners auf welchen die Daten übertragen werden sollen.
- **Verzeichnis** in welches die Daten kopiert werden sollen
- **Benutzername** für das SCP Login
- Der Kunde muß das **Public Key File** der T-Mobile Austria einspielen, damit die Anmeldung für SCP funktioniert (mehr Details und das Keyfile bei Bedarf)
- Der Kunde und die T-Mobile Austria müssen die **entsprechenden Ports** für die SCP Übertragung auf den Firewalls freischalten (mehr Details bei Bedarf)

3. **SFTP (Typ 3)**

Secure FTP (SFTP) ist ein sehr sicherer Transportlayer, welcher die Daten bereits automatisch verschlüsselt überträgt. Eine zusätzliche Verschlüsselung ist daher nicht mehr notwendig - kann aber dennoch eingerichtet werden. Im Unterschied zu SCP kann SFTP auch über ein Kennwort anmelden - sprich der Kunde muß nicht das Public Key File der T-Mobile einspielen um eine Anmeldung zu ermöglichen. Außerdem ist auch die Einrichtung auf den Firewalls für SFTP nicht so komplex wie für SCP. SFTP ist daher die "unkompliziertere" Übertragungsart.

→ Hinweis: Bei der Übertragung mittels SFTP werden die einzelnen Dateien (kann auch nur eine sein falls Format 0 konfiguriert ist !) übertragen und danach wird noch ein Kontrollfile geschrieben, welches pro übertragener Datei eine Zeile mit dem Dateinamen enthält. Dies stellt sicher, dass auch alle Dateien korrekt übertragen wurden. Der Kunde darf die übertragenen Dateien erst verwenden, wenn das Kontrollfile übertragen wurde ! Name des Kotrollfiles: **<tma | tra>_<RechnungsDatum(YYYYMMDD)>.ctrl** (Beispiel: tma_20091104.ctrl)

Um SFTP zu aktivieren müssen folgende Daten / Voraussetzungen erfüllt sein:

- **Host Adresse** des Kundenrechners auf welchen die Daten übertragen werden sollen.
- **Verzeichnis** in welches die Daten kopiert werden sollen
- **Benutzername** für das SCP Login
- SFTP kann entweder über ein **Public Key File** oder über ein **Kennwort** autentifizieren. Sprich entweder spielt der Kunde das Public Key File der T-Mobile Austria ein oder er stellt ein Kennwort für die Anmeldung des angegebenen Benutzers zur Verfügung (Details wiederum bei Bedarf).
- Der Kunde muss die **entsprechenden Ports** für die SFTP Übertragung auf den Firewalls freischalten (mehr Details bei Bedarf)

Formate – Namensgebung und Übertragung:

Der Kunde kann sich aussuchen, in welchem Format seine Dateien übertragen werden:

- **Gezipptes Tar Archiv (Format 0)**

Alle Dateien an den Kunden werden in ein tar Archiv gepackt und anschließend gezippt (und eventuell noch verschlüsselt). Die entstandene Datei wird dann über den gewählten Transportlayer übertragen (E-Mail - als Attachment, SCP - mit Kontrollfile, SFTP - mit Kontrollfile). Somit bekommt der Kunde genau eine Datei (exklusive Kontrollfile) zugestellt.

Der Dateiname lautet: **<tma | tra>_<RechnungsDatum(YYYYMMDD)>.tar.gz[.gpg]**
Beispiel: tma_20091125.tar.gz

- **Einzelne gezippte Dateien (Format 1) – Standard !!!**

Alle Dateien an den Kunden werden gezippt (und eventuell noch verschlüsselt). Die entstandenen Dateien werden dann über den gewählten Transportlayer übertragen (E-Mail - als Attachments, SCP - mit Kontrollfile, SFTP - mit Kontrollfile). Es können viele Files anfallen !

Dateinamen: **<tma | tra>_<itemized-bill | invoice | structure>_<cust_code>_<RechnungsDatum(YYYYMMDD)>.<edi | csv>.gz[.gpg]**
Beispiel: tma_invoice_1.14613787_20091125.edi.gz, ...

- **Einzelne Dateien (Format 2)**

Alle Dateien an den Kunden werden eventuell verschlüsselt und über den gewählten Transportlayer übertragen (E-Mail - als Attachments, SCP - mit Kontrollfile, SFTP - mit Kontrollfile). Es können viele Files anfallen und diese können sehr groß werden !

Dateinamen: **<tma | tra>_<itemized-bill | invoice | structure>_<cust_code>_<RechnungsDatum(YYYYMMDD)>.<edi | csv>[.gpg]**
Beispiel: tma_invoice_1.14613787_20091125.edi, ...

Verschlüsselung - Voraussetzungen:

Um die Verschlüsselung durchführen zu können, muß auf Seite der T-Mobile Austria der Public GPG Key des Kunden eingespielt werden. Dies bedeutet, dass der Kunde einen GPG Schlüssel haben muß und uns den öffentlichen Teil dafür zur Verfügung stellt. Mit Hilfe dieser Information kann dann eine entsprechende Verschlüsselung eingerichtet werden.

Wie bereits erwähnt werden die übertragenen Dateien bei einer Verschlüsselung um die Endung "*.gpg" erweitert!

Informationen zum Anfordern einer EDIFACT Zustellung:

Übertragungsart: 1 (E-Mail) / 2 (SCP) / 3 (SFTP) ___

E-Mail Adresse(n) (Nur bei E-Mail): _____

Host Adresse (Nur bei SFTP und SCP): _____

Verzeichnis (Nur bei SFTP und SCP): _____

Benutzername (Nur bei SFTP und SCP): _____

Passwort (Nur bei SFTP falls nicht über Keys gearbeitet wird): _____

Format: 0 (*.tar.gz) / 1 (*.gz) / 2 (*) ___

Verschlüsselung: Ja –> Name des Schlüssels: _____
(der Öffentliche Schlüssel muß auch zur Verfügung stehen !)

→ Hinweis: Bei SFTP ohne Kennwort oder SCP muß der Kunde das Public Key File der T-Mobile Austria einspielen, damit sich das Versandservice anmelden kann. Bitte bei T-Mobile Austria / IT nachfragen und das Key File anfordern.

Außerdem müssen im Fall von SCP die entsprechenden Ports bei den T-Mobile Firewalls freigeschalten werden !