

Anlage 2a: FTAM-Anbindung

1. Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt der Bank die Nutzer und deren Berechtigungen im Rahmen der Datenfernübertragung.

Folgende Legitimations- und Sicherungsverfahren werden in der FTAM-Anbindung eingesetzt:

- Elektronische Unterschrift
- DFÜ-Passwort

1.1 Elektronische Unterschrift

Für die FTAM-Anbindung wird das Legitimationsverfahren der Elektronischen Unterschrift (EU) verwendet.

Mit dem vom Kunden verwendeten Programm können verschiedene Nachrichten (z. B. Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für Initialisierung, den Protokollabwurf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Die Bank teilt dem Kunden mit, welche Nachrichtentypen genutzt werden können und welche mit elektronischer Unterschrift zu übermitteln sind.

Für die Elektronische Unterschrift verfügt der Nutzer über ein Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Der private Schlüssel ist gegen unautorisiertes Auslesen und Veränderung zu schützen. Der öffentliche Schlüssel ist der Bank gemäß dem in Nummer 2.2 beschriebenen Verfahren mitzuteilen. Das Schlüsselpaar des Nutzers kann auch für die Kommunikation mit anderen Banken eingesetzt werden.

1.2 DFÜ-Passwort

Bei der FTAM-Anbindung wird der Datenaustausch zwischen Kunden und Bank mit einem DFÜ-Passwort abgesichert. Jeder Nutzer erhält hierfür ein gesondertes Passwort, das dem Nutzer im Rahmen der Initialisierung der FTAM-Anbindung (siehe Nummer 2.1) von der Bank mitgeteilt wird. Der Nutzer ist verpflichtet, dieses Passwort im Rahmen der Initialisierung zu ändern.

Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person Kenntnis von seinem DFÜ-Passwort erlangt. Denn jede andere Person, die das DFÜ-Passwort kennt, kann den Datenaustausch mit der Bank durchführen.

Für die Durchführung des Datenaustauschs gibt der Nutzer sein DFÜ-Passwort ein.

2. Initialisierung der FTAM-Anbindung

2.1 Einrichtung der Kommunikationsverbindung

Die Bank teilt den vom Kunden benannten Nutzern die zur Aufnahme einer Verbindung über Datenfernübertragung (DFÜ) erforderlichen Daten mit. Dabei handelt es sich um:

- Kunden-ID
- Hostname

- Datex-P NUA oder ISDN-NUA
- Host-Typ
- User-ID
- Erstes DFÜ-Passwort

Der Kunde erstellt mit diesen Angaben eine Bankparameterdatei für die Bank, sofern ihm diese nicht durch seine Bank zur Verfügung gestellt wird. Der Kunde definiert pro Auftragsart die erforderliche Mindestanzahl von Elektronischen Unterschriften.

Jeder Teilnehmer führt in seinem Programm eine Funktion zur Änderung des DFÜ-Passwortes („PWA“) aus.

2.2 Initialisierung der Schlüssel

Das vom Nutzer eingesetzte Schlüsselpaar muss zusätzlich zu den in Nummer 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

- 1) Das Schlüsselpaar ist ausschließlich und eindeutig dem Nutzer zugeordnet.
- 2) Soweit der Nutzer sein Schlüsselpaar eigenständig generiert, ist der private Schlüssel mit Mitteln zu erzeugen, die der Nutzer unter seiner alleinigen Kontrolle halten kann.
- 3) Sofern das Schlüsselpaar von einem Dritten zur Verfügung gestellt wird, ist sicherzustellen, dass der Nutzer in den alleinigen Besitz des privaten Schlüssels gelangt.
- 4) Für die Nutzung des privaten Schlüssels definiert jeder Nutzer ein Schlüssel-Passwort, das den Zugriff auf den privaten Schlüssel absichert.

Für die Initialisierung des Nutzers bei der Bank ist die Übermittlung des öffentlichen Schlüssels des Nutzers an das Banksystem erforderlich. Hierfür übermittelt der Nutzer der Bank seinen öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

- Über die FTAM-Anbindung mittels der hierfür vorgesehenen systembedingten Auftragsarten.
- Mit einem vom Kontoinhaber oder einem Kontobevollmächtigten unterschriebenen Initialisierungsbrief.

Für die Freischaltung des Nutzers überprüft die Bank auf Basis der vom Kontoinhaber oder einem Kontobevollmächtigten händisch unterschriebenen Initialisierungsbrief die Authentizität des über FTAM übermittelten öffentlichen Schlüssels.

Zu dem öffentlichen Schlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck „Elektronische Unterschrift“ des öffentlichen Schlüssels
- Die jeweils unterstützten Version pro Schlüsselpaar
- Längenangabe des Exponenten
- Exponent des öffentlichen Schlüssels in hexadezimaler Darstellung
- Längenangabe des Modulus

- Modulus des öffentlichen Schlüssels in hexadezimaler Darstellung
- Hashwert des öffentlichen Schlüssels in hexadezimaler Darstellung

Die Bank prüft die eigenhändige Unterschrift des Kontoinhabers beziehungsweise des Kontobevollmächtigten auf dem Initialisierungsbrief sowie die Übereinstimmung zwischen den über die FTAM-Anbindung und den schriftlich übermittelten Hashwert des öffentlichen Schlüssels des Nutzers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Nutzer für die vereinbarten Auftragsarten frei.

3. Auftragserteilung an die Bank

3.1 Auftragserteilung mit Elektronischer Unterschrift

Der Nutzer überprüft die zu unterschreibenden Dateien auf Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden. Zu jeder Datei mit Auftragsdaten werden entsprechend der Vereinbarung mit der Bank eine oder mehrere Elektronische Unterschriften erzeugt.

Auftragsdaten und zugehörige Elektronische Unterschrift(en) befinden sich in je einer Datei, die gemeinsam oder getrennt an die Bank übertragen werden können.

Die Aufträge sind gegenüber der Bank erst dann erteilt, wenn zusätzlich zur Datei mit den Auftragsdaten (z. B. Zahlungsverkehrsauftrag) auch eine entsprechende Unterschriftdatei – gegebenenfalls zu einem von der Übermittlung der Auftragsdatei abweichenden Zeitpunkt – übertragen wurde.

Kunde und Bank können vereinbaren, dass die Autorisierung von per DFÜ übermittelten Auftragsdaten mittels gesondert übermittelten Begleitzettels erfolgen kann. Die Freigabe des Auftrags erfolgt in diesem Fall nach erfolgreicher Prüfung der Unterschrift des Nutzers auf dem Begleitzettel durch die Bank.

Für die Abfrage von Informationen bei der Bank sind die gewünschten Abholaufträge zu erstellen und an die Bank zu übermitteln. Hierzu ist das entsprechende DFÜ-Passwort des Nutzers einzugeben. Eine bankfachliche EU ist für die Abfrage von Informationen nicht erforderlich.

3.2 Legitimationsprüfung durch die Bank

Eine empfangene Auftragsdatei wird durch die Bank erst dann ausgeführt, wenn die erforderliche Anzahl von Elektronischen Unterschriften beziehungsweise der unterschriebene Begleitzettel eingegangen ist und mit positivem Ergebnis geprüft wurden.

Die Bank ist dazu berechtigt, nicht vollständig autorisierte Auftragsdaten nach Ablauf des von der Bank gesondert mitgeteilten Zeitlimits zu löschen.

3.3 Kundenprotokolle

Die Bank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem

- Übertragung von Informationsdateien von dem Banksystem an das Kundensystem
- Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Banksystem
- Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftenprüfung und die Anzeige von Auftragsdaten betreffen.
- Fehler bei der Dekomprimierung

Der Nutzer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten der Bank durchgeführten Prüfungen zu informieren.

Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 1.7 der Anlage 2b entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

4. Änderung der Schlüssel eines Nutzers

4.1 Änderung der Schlüssel mit automatischer Freischaltung

Wenn die vom Nutzer eingesetzten Legitimationsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der Nutzer seiner Bank die neuen öffentlichen Schlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neuinitialisierung gemäß Nummer 2.2 vorzunehmen.

Wenn der Nutzer seine Schlüssel selbst generiert, so hat er zu dem mit der Bank vereinbarten Zeitpunkt die Schlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu erneuern und rechtzeitig vor dem Erreichen des Ablaufdatums des alten Schlüssels zu übermitteln.

Für eine automatische Freischaltung des neuen Schlüssels ohne eine erneute Initialisierung ist die folgende Auftragsart zu nutzen:

- Aktualisierung des öffentlichen Schlüssels (PUB)

Die Auftragsart PUB ist hierfür mit einer gültigen elektronischen Unterschrift des Nutzers zu versehen. Nach erfolgreicher Prüfung der Elektronischen Unterschrift ist nur noch der neue Schlüssel zu verwenden.

Wenn die elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Nummer 7 Absatz 3 der Bedingungen für die Datenfernübertragung verfahren.

Die Schlüsseländerung darf erst nach Abarbeitung aller Aufträge erfolgen. Ansonsten sind die noch nicht ausgeführten Aufträge mit dem neuen Schlüssel neu zu erteilen.

4.2 Änderung der Schlüssel mit Neuinitialisierung

Der Nutzer kann per DFÜ durch Übermittlung eines neuen öffentlichen Schlüssels (Auftragsart „PUB“) sein bisheriges Schlüsselpaar ersetzen. Das neue Schlüsselpaar wird erst nach Eingang des hierzu erstellten entsprechenden Initialisierungsprotokolls (Ini-Brief) bei der Bank freigeschaltet. Erst danach können mit dem neuen Schlüssel unterschriebene Aufträge ausgeführt werden.

Nach der Übermittlung des neuen öffentlichen Schlüssels werden aus Sicherheitsgründen alle mit dem alten Schlüssel unterschriebenen und noch nicht von der Bank bearbeiteten Aufträge nicht ausgeführt und der Nutzer hierüber beispielsweise über das Kundenprotokoll unverzüglich informiert. Dies betrifft insbesondere Aufträge,

- für die die Prüfung der Elektronischen Unterschrift bankseitig noch nicht abgeschlossen wurde oder
- die bis zu diesem Zeitpunkt noch nicht an die Bank übermittelt wurden.

Diese Aufträge sind daher – sofern deren Ausführung gewünscht wird – komplett neu zu erteilen.

Bis das zugehörige händisch unterschriebene Initialisierungsprotokoll der Bank vorliegt und der neue öffentliche Schlüssel nach Prüfung von der Bank zur Nutzung freigeschaltet wurde, kann für den dazwischen liegenden Zeitraum, der unter Einschluss der Postlaufzeit durchaus mehrere Tage betragen kann, bei Bedarf mit der Bank ein anderes Legitimationsverfahren für die Auftragslegitimierung (Ersatzverfahren) vereinbart werden.

Nach bankseitiger Freischaltung des neuen öffentlichen Schlüssels sind Aufträge, die noch nicht an die Bank übertragen wurden, mit dem neuen Schlüsselpaar neu zu legitimieren und der Bank zu übermitteln.

5. Sperrung der Schlüssel eines Nutzers

Besteht der Verdacht des Missbrauchs des Schlüssels, ist der Nutzer dazu verpflichtet, seine Zugangsberechtigung zu allen Banksystemen zu sperren, die den kompromittierten Schlüssel verwenden.

Soweit der Nutzer über gültige Legitimationsmedien verfügt, kann er seine Zugangsberechtigung via FTAM-Anbindung sperren. Hierbei wird durch Senden einer Nachricht mit der Auftragsart „SPR“ der Zugang, d. h. der öffentliche Schlüssel und das DFÜ-Passwort, für den jeweiligen Nutzer, unter dessen User-ID die Nachricht gesendet wird, gesperrt. Nach einer Sperre können bis zu der unter Nummer 2 beschriebenen Neuinitialisierung keine Aufträge von diesem Nutzer per FTAM-Anbindung mehr erteilt werden.

Wenn der Nutzer nicht mehr über gültige Legitimationsmedien verfügt, kann er außerhalb des DFÜ-Verfahrens seine Legitimationsmedien über die von der Bank gesondert bekannt gegebenen Sperrfazität sperren lassen.

Der Kunde kann außerhalb des DFÜ-Verfahrens die Legitimations- und Sicherungsmedien eines Nutzers oder den gesamten DFÜ-Zugang über die von der Bank bekannt gegebene Sperrfazität sperren lassen.