



## DFÜ-Verfahrensbeschreibung

---

### 1. Legitimations-, Authentifizierungs- und Sicherungsverfahren

(1) Im Rahmen der DFÜ werden folgende Legitimations- und Sicherungsverfahren eingesetzt:

- Komprimierung (bei FTAM optional)
- Verschlüsselung (bei EBICS und MCFT)
- Elektronische Unterschriften (EU)
- DFÜ-Passwort (bei FTAM und MCFT)
- Authentifikationssignatur (nur bei EBICS)

(2) Im MCFT und EBICS-Verfahren werden Auftragsdateien und Kontoinformationen verschlüsselt und komprimiert zwischen dem EDV-System des Kunden bzw. dessen beauftragten Dritten und dem Banksystem ausgetauscht. Der Datenaustausch bei EBICS wird grundsätzlich auf Anwendungs- und Transportebene verschlüsselt.

(3) Beim EBICS-Verfahren verfügt der Teilnehmer für jedes Legitimations- und Sicherungsverfahren über ein individuelles Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Die Schlüsselpaare des Teilnehmers können auch für die Kommunikation mit anderen Banken eingesetzt werden. Die öffentlichen Teilnehmerschlüssel sind der Bank gemäß dem in Nummer 2 beschriebenen Verfahren mitzuteilen. Zur Gewährleistung der Geheimhaltung der bankfachlichen Daten auf Anwendungsebene sind die Auftragsdaten vom Kunden bzw. dessen beauftragten Dritten unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation zu verschlüsseln.

#### 1.1 Elektronische Unterschriften (EU)

Mit dem vom Kunden bzw. von dessen beauftragten Dritten verwendete Programm können verschiedene Nachrichten (z. B. Aufträge für den Inlands- und Auslandszahlungsverkehr, aber auch für die Initialisierung, den Protokollabruf und die Abholung von Konto- und Umsatzinformationen etc.) erstellt werden. Die Bank teilt dem Kunden bzw. dessen beauftragten Dritten mit, welche Nachrichtenarten (Sende- bzw. Abholaufträge) genutzt werden können. Die individuellen Verknüpfungen je Teilnehmer zwischen Auftragsart und Elektronischer Unterschrift (EU) wird zwischen dem Kunden bzw. dessen beauftragten Dritten und der Bank vertraglich vereinbart und

auf dem Banksystem hinterlegt. Dabei sind für die Elektronischen Unterschriften (EU) der Teilnehmer

#### 1.1.1 EBICS-Verfahren

folgende EU-Typen definiert:

- „E“ – Einzel-Verfügungsberechtigung
- „A“ – Gemeinsam mit einem anderen Verfügungsberechtigten (allgemein)
- „B“ – Gemeinsam mit einem Verfügungsberechtigten der Gruppe A (beschränkt)
- „T“ – Transport – keine Verfügungsberechtigung

Grundsätzlich gibt es im EBICS-Verfahren keine Übertragung von Nachrichten von Teilnehmern zum Banksystem ohne elektronische Unterschrift. Als bankfachliche EU bezeichnet man EU vom Typ „E“, „A“ oder „B“. Bankfachliche EU dienen der Autorisierung von Aufträgen (siehe Nummer 3). Aufträge können mehrere bankfachliche EU benötigen, die von unterschiedlichen Teilnehmern geleistet werden müssen. EU vom Typ „T“ werden nicht zur bankfachlichen Freigabe von Aufträgen verwendet, sondern lediglich zu deren Übertragung an das Banksystem (Authentizität). „Technische Teilnehmer“ (siehe Nummer 3.7 der Spezifikation der EBICS-Anbindung) können nur eine EU vom Typ „T“ zugewiesen bekommen.

#### 1.1.2 FTAM-/MCFT-Verfahren

folgende EU-Typen definiert:

- „E“ – Einzel-Verfügungsberechtigung
- „A“ – Gemeinsam mit einem anderen Verfügungsberechtigten (allgemein)
- „B“ – Gemeinsam mit einem Verfügungsberechtigten der Gruppe A (beschränkt)
- „N“ – keine Verfügungsberechtigung

Für die elektronische Unterschrift verfügt der Teilnehmer über ein Schlüsselpaar, das aus einem privaten und einen 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 Teilnehmers kann auch für die Kommunikation mit anderen Banken eingesetzt werden



## 1.2 DFÜ-Passwort (FTAM und MCFT)

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

## 1.3 Authentifizierungssignatur (EBICS)

Im Gegensatz zur EU, die Auftragsdaten signiert, wird die Authentifizierungssignatur über die einzelne EBICS-Nachricht einschließlich Steuerungs- und Anmeldedaten und die darin enthaltenen EU gebildet. Mit Ausnahme einiger in der EBICS-Spezifikation definierten systembedingten Auftragsarten wird die Authentifizierungssignatur bei jedem Transaktionsschritt sowohl vom EDV-System des Kunden bzw. dessen beauftragten Dritten als auch vom Banksystem geleistet.

## 2. Initialisierung der DFÜ-Verbindung

### 2.1 Einrichtung der Kommunikationsverbindung

Die Bank stellt den vom Kunden bzw. dessen beauftragten Dritten benannten Teilnehmern zur Aufnahme der DFÜ-Verbindung folgende Daten zur Verfügung:

#### 2.1.1 EBICS-Verfahren

- Adresse der Bank (URL – Uniform Resource Locator)
- Bezeichnung der Bank
- HostID
- zulässige Version(en) für das EBICS-Protokoll und der Sicherungsverfahren
- Kunden –ID
- Teilnehmer-ID und evtl.
- weitere spezifische Angaben zu Kunden- und Teilnehmerberechtigungen

Für die dem Kunden bzw. dessen beauftragten Dritten zugeordneten Teilnehmer (auch den technischen Teilnehmern) vergibt die Bank jeweils eine Teilnehmer-ID, die den Teilnehmer eindeutig identifiziert. Soweit ein technischer Teilnehmer festgelegt ist, sind System-ID und Teilnehmer-ID identisch.

#### 2.1.2 MCFT-Verfahren

- Kunden-ID
- Hostname
- IP-Adresse inkl. Port-Nummer
- Host-Typ
- Teilnehmer-ID
- erstes DFÜ-Passwort

#### 2.1.3 FTAM-Verfahren

- Kunden-ID
- Hostname
- ISDN-NUA
- Host-Typ
- User-ID
- erstes DFÜ-Passwort

## 2.2 Initialisierung der Schlüssel

### 2.2.1 EBICS-Verfahren

(1) Die vom Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten und die Authentifizierungssignatur müssen zusätzlich zu den in Nummer 1 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

- die Schlüsselpaare sind ausschließlich und eindeutig dem Teilnehmer zugeordnet,
- soweit der Teilnehmer seine Schlüssel eigenständig generiert, sind die privaten Schlüssel mit Mitteln zu erzeugen, die der Teilnehmer unter seiner alleinigen Kontrolle halten kann,
- sofern die Schlüssel von einem Dritten zur Verfügung gestellt werden, ist sicherzustellen, dass der Teilnehmer in den alleinigen Besitz der privaten Schlüssel gelangt,
- für die zur Legitimation eingesetzten privaten Schlüssel definiert jeder Teilnehmer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert und
- für die zur Absicherung des Datenaustausches eingesetzten privaten Schlüssel definiert jeder Teilnehmer pro Schlüssel



ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert. Auf dieses Passwort kann verzichtet werden, wenn das Sicherungsmedium des Teilnehmers in einer technischen Umgebung gespeichert ist, die vor unautorisiertem Zugriff geschützt ist.

(2) Für die Initialisierung des Teilnehmers bei der Bank ist die Übermittlung der öffentlichen Schlüssel des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer der Bank seine öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

- über EBICS mittels der hierfür vorgesehenen systembedingten Auftragsarten und
- mit den vom Kunden bzw. dessen beauftragten Dritten oder einem Kontobevollmächtigten (gemäß Kontovollmacht oder E-Banking-Vollmacht – evtl. zweite Unterschrift notwendig) unterschriebenen Ausdrucken der Authentifikations-, Verschlüsselungs- und Signaturschlüssel per Fax an: Bank für Sozialwirtschaft AG, electronic banking support, Fax-Nr.: 0221/97356470. Besitzt der Teilnehmer nur den EU-Typ „T“ (Transportunterschrift) reicht die Unterschrift des Teilnehmers aus.

(3) Zu jeden öffentlichen Teilnehmerschlüssel enthalten die Ausdrücke der Authentifikations-, Verschlüsselungs- und Signaturschlüssel die folgenden Daten:

- Verwendungszweck des öffentlichen Teilnehmerschlüssels
- Elektronische Unterschrift
- Authentifikationssignatur
- Verschlüsselung
- die jeweils unterstützten Versionen 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

(4) Die Bank prüft die Unterschrift des Kunden bzw. dessen beauftragten Dritten oder des Kontobevollmächtigten (gemäß Kontovollmacht oder E-Banking-Vollmacht – evtl. zweite Unterschrift notwendig. Besitzt der Teilnehmer nur den EU-Typ „T“ reicht die Unterschrift des Teilnehmers aus.) auf den Ausdrucken der Authentifikations-, Verschlüsselungs- und Signaturschlüssel sowie die Übereinstimmung zwischen den per EBICS und den per Fax übermittelten Hashwerten des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer frei.

(5) Der Teilnehmer holt den öffentlichen Schlüssel der Bank mittels der eigens dafür vorgesehenen systembedingten Auftragsart ab.

(6) Der Hashwert des öffentlichen Bankschlüssels wird von der Bank dem Teilnehmer zusätzlich schriftlich über einen separaten Kommunikationsweg außerhalb des EBICS-Verfahrens bereitgestellt.

(7) Vor dem ersten Einsatz von EBICS, hat der Teilnehmer die Echtheit der ihm per Datenfernübertragung übermittelten öffentlichen Bankschlüssel dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von der Bank schriftlich über einen separaten Kommunikationsweg außerhalb des EBICS-Verfahrens mitgeteilt wurden.

(8) Der Kunde bzw. dessen beauftragter Dritte muss gewährleisten, dass eine Software eingesetzt wird, die die Gültigkeit der im Rahmen der Transportverschlüsselung eingesetzten Serverzertifikate anhand des von der Bank gesondert mitgeteilten Zertifizierungspfades überprüft.

(9) Die öffentlichen Bankschlüssel sind gegen unautorisiertes Verändern zu schützen. Andernfalls ist die Kommunikation mit dem Banksystem nicht mehr gegeben.



## 2.2.2 MCFT- und FTAM-Verfahren

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

- das Schlüsselpaar ist ausschließlich und eindeutig dem Teilnehmer zugeordnet,
- soweit der Teilnehmer sein Schlüsselpaar eigenständig generiert, ist der private Schlüssel mit Mitteln zu erzeugen, die der Teilnehmer unter seiner alleinigen Kontrolle halten kann,
- sofern das Schlüsselpaar von einem Dritten zur Verfügung gestellt wird, ist sicherzustellen, dass der Teilnehmer in den alleinigen Besitz des privaten Schlüssels gelangt und
- für die Nutzung des privaten Schlüssels definiert jeder Teilnehmer ein Schlüssel-Passwort (EU-Passwort), das den Zugriff auf den privaten Schlüssel absichert.

(2) Für die Initialisierung des Teilnehmers bei der Bank ist die Übermittlung des öffentlichen Schlüssels des Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der Teilnehmer der Bank seinen öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

- über MCFT bzw. FTAM mittels der hierfür vorgesehenen systembedingten Auftragsarten und
- mit dem vom Kunden bzw. dessen beauftragten Dritten oder einem Kontobevollmächtigten (gemäß Kontovollmacht oder E-Banking-Vollmacht – evtl. zweite Unterschrift notwendig) unterschriebenen Ausdruck des Signaturschlüssels bei MCFT bzw. des INI-Briefes bei FTAM per Fax an: Bank für Sozialwirtschaft AG, electronic banking support, Fax-Nr.: 0221/97356470. Besitzt der Teilnehmer nur den EU-Typ „N“ (keine Verfügungsberechtigung) reicht die Unterschrift des Teilnehmers aus.

(3) Zu dem öffentlichen Schlüssel enthält der Ausdruck des Signaturschlüssels die folgenden Daten:

- Verwendungszweck „Elektronische Unterschrift“ des öffentlichen Schlüssels

- die jeweils unterstützten Versionen 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

(4) Die Bank prüft die Unterschrift des Kunden bzw. dessen beauftragten Dritten oder des Kontobevollmächtigten (gemäß Kontovollmacht oder E-Banking-Vollmacht – evtl. zweite Unterschrift notwendig. Besitzt der Teilnehmer nur den EU-Typ „N“ reicht die Unterschrift des Teilnehmers aus.) auf dem Ausdruck des Signaturschlüssels bei MCFT bzw. des INI-Briefes bei FTAM sowie die Übereinstimmung zwischen den per MCFT bzw. per FTAM und den per Fax übermittelten Hashwert des öffentlichen Schlüssels des Teilnehmers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer frei.

## 3. Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

### 3.1 EBICS-Verfahren

(1) Wenn der Teilnehmer seine Schlüssel selbst generiert, so hat er der Bank die Teilnehmerschlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu übermitteln.

(2) Für eine automatische Freischaltung der neuen Schlüssel ohne eine erneute Teilnehmerinitialisierung (siehe Nummer 2.2.1) sind die folgenden Auftragsarten zu nutzen und mit der bisher gültigen bankfachlichen EU des Teilnehmers zu versehen:

- PUB – Public-Key senden (Aktualisierung des öffentlichen bankfachlichen Schlüssels) und



- HCA – Schlüssel ändern EBICS (Aktualisierung des öffentlichen Authentifikationsschlüssels und des öffentlichen Verschlüsselungsschlüssels).

(3) Nach erfolgreicher Änderung sind nur noch die neuen Schlüssel zu verwenden.

(4) Wenn die elektronische Unterschrift nicht erfolgreich geprüft werden konnte, ist wie unter Nummer 2.2.1, Sätze 2, 3 und 4 zu verfahren.

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

### 3.2 MCFT- und FTAM-Verfahren

(1) Wenn der Teilnehmer seine Schlüssel selbst generiert, so hat er der Bank die Teilnehmerschlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu übermitteln.

(2) Für eine automatische Freischaltung des neuen Schlüssels ohne eine erneute Teilnehmerinitialisierung ist die folgende Auftragsart zu nutzen und mit der bisher gültigen EU des Teilnehmers zu versehen:

- PUB – Public-Key senden (Aktualisierung des öffentlichen bankfachlichen Schlüssels)

(3) Nach erfolgreicher Änderung ist nur noch der neue Schlüssel zu verwenden.

(4) Wenn die elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Nummer 2.2.2, Sätze 2, 1 und 4 zu verfahren.

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

## 4. Bankseitige Prüfung von eingereichten Auftragsdaten

### 4.1 EBICS-Verfahren

(1) Bei Aufnahme der Kommunikation werden seitens der Bank zuerst teilnehmerbezogene Berechtigungsprüfungen durchge-

führt, wie etwa die Auftragsberechtigung oder ggf. vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.

(2) Sofern mit dem Kunden bzw. dessen beauftragten Dritten die Funktionalität der ggfs. Kunden-ID übergreifenden Verteilten Elektronischen Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.

(3) Soweit mit dem Kunden und mit dem Service-Rechenzentrum bzw. Dienstleister vereinbart wurde, dass die Autorisierung von vom Service-Rechenzentrum, bzw. Dienstleister eingereichten Auftragsdaten durch den Kunden bzw. dessen Teilnehmer(n) mit Personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggfs. mit Token-PIN) erfolgt, ist vom Teilnehmer des Service-Rechenzentrums bzw. Dienstleisters an Stelle der bankfachlichen EU eine Transportunterschrift (EU-Typ „T“) für die technische Absicherung der Auftragsdaten zu leisten. Hierfür ist die Datei mit einer speziellen Auftragsart zu versehen. Auch hier wird der Auftrag bis zur Abgabe aller erforderlichen EU durch die Teilnehmer des Kunden im Banksystem gespeichert.

### 4.2 MCFT-Verfahren

(1) Bei Aufnahme der Kommunikation wird zuerst ein Startblock vorgelagert. Dieser Startblock enthält alle zur Prüfung erforderlichen Informationen, wie Kunden-ID, Teilnehmer-ID, zu belastendes Konto, die Elektronische Unterschrift und Prüfsummen zur gesamten Datei. Dadurch ist es möglich, frühzeitig Fehler/Manipulationen festzustellen und die eigentliche Datenübertragung zu unterbinden.

(2) Wird eine Elektronische Unterschrift per MCFT übermittelt, dann enthält der Startblock zusätzlich den „Fingerabdruck“ zur Originaldatei und auch die Elektronische Unterschrift selbst. Dies hat den Vorteil, dass die EU – sofern alle erforderlichen Unterschriften geleistet wurden – bereits während der Kommunikation verifiziert werden kann. Im Startblock können bis zu 6 Unterschriften übermittelt werden.

(3) Ergibt die Prüfung auf der Bankseite, dass



- eine der im Startblock enthaltene Unterschrift nicht korrekt ist, wird die DFÜ vor der Übertragung der Originaldatei abgebrochen.
- alle Unterschriften korrekt sind, wird die Originaldatei übertragen. Nach der Übertragung der Originaldatei wird auf Bankseite der „Fingerabdruck“ nachgerechnet und mit demjenigen verglichen, der im Startblock mit übertragen und für korrekt befunden wurde. Ergibt die Nachberechnung des „Fingerabdrucks“ eine Übereinstimmung mit den übertragenen Werten, wird dies dem System des Kunden bzw. des durch ihn beauftragten Dritten im Schlussblock mit einem „OK“ mitgeteilt. Stimmt der nachgerechnete „Fingerabdruck“ nicht mit dem im Startblock übermittelten überein, wird die Originaldatei zurückgewiesen.

(4) Die Schlussnachrichten werden entweder bei Beendigung der Kommunikation oder des Dialoges übermittelt. Der Inhalt der Schlussnachrichten sowie die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.

(5) Sofern mit dem Kunden bzw. dessen beauftragten Dritten die Funktionalität der ggfs. Kunden-ID übergreifenden Verteilten Elektronischen Unterschrift (VEU) vereinbart wurde und die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.

### 4.3 FTAM-Verfahren

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

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

(3) Bei Aufnahme der Kommunikation werden seitens der Bank zuerst teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Auftragsberechtigung oder ggf. vereinbarte Limitprüfungen. Die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Limitprüfungen oder Kontoberechtigungsprüfungen werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.

gungsprüfungen werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.

(4) Kunde bzw. dessen beauftragter Dritter und Bank können vereinbaren, dass die Autorisierung von Aufträgen mittels gesondert übermittelten Begleitzettels erfolgen kann. Die Freigabe des Auftrags erfolgt in diesem Fall nach erfolgreicher Prüfung der Unterschrift des Kunden bzw. der jeweiligen Bevollmächtigten auf dem Begleitzettel durch die Bank.

### 5. DFÜ-Protokoll

Im DFÜ-Protokoll dokumentiert die Bank folgende Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem
- Übertragung von Informationsdateien vom Banksystem an das System des Kunden bzw. an das System des von ihm beauftragten Dritten
- Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden bzw. dessen beauftragten Dritten an das Banksystem
- Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung, die Anzeige von Auftragsdaten betreffen
- Fehler bei der Dekomprimierung