DFÜ-Verfahrensbeschreibung

1 Legitimations-, Authentifizierungs- und Sicherungsverfahren

(1) Im Rahmen der DFÜ werden folgende Legitimations- und Sicherungsverfahren eingesetzt:
- Komprimierung
- Verschlüsselung
- elektronische Unterschriften (EU)
- DFÜ-Passwort (nur bei 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) Der Teilnehmer verfügt 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 (z. B. EBICS- Spezifikation) zu verschlüsseln.

1.1 Elektronische Unterschriften (EU)
(1) Als Standard für die Sicherheit wird die elektronische Unterschrift (EU) gemäß dem RSA-Verfahren (Public Key-Verfahren) angewendet.
(2) Mit dem vom Kunden bzw. von dessen beauftragten Dritten verwendeten 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 stellt unter www.sozialbank.de dem Kunden bzw. dessen beauftragten Dritten eine Aufstellung zur Verfügung, welche Nachrichtenarten (Sende- bzw. Abholaufträge) aktuell 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 bei der Bank für die elektronischen Unterschriften (EU) der Teilnehmer folgende EU-Typen definiert:
- „E“ – Einzel-Verfügungsberechtigung
- „A“ – gemeinsam mit einem anderen Verfügungsberechtigten (allgemein)
- „B“ – gemeinsam mit einem Verfügungsberechtigten der Gruppe A (beschränkt)
- „T“ – Übertragung von Auftragsdateien
- „N“ – Abruf von Kontoinformationen
- „V“ – Verfügung und Freigabe

(3) Im Rahmen der EU-Typen ist die Kombination von „T“ und „N“ möglich.
(4) Der EU-Typ „V“ kann nur an Dienstleister vergeben werden, die für den Kunden spezielle Dienstleistungen (z. B. Spendenverwaltung, Mitgliederverwaltung usw.) übernehmen und im Rahmen dessen zwar Zahlungen ausführen sollen, jedoch selbst keine Kontoinformationen erhalten sollen. Die Regelung der bankfachlichen EU des Dienstleisters wird zwischen dem Dienstleister und der Bank separat vereinbart.

1.2 DFÜ-Passwort (MCFT)
Der Datenaustausch zwischen Teilnehmer und Bank wird mit einem DFÜ-Passwort abgesichert. Dazu erhält jeder Teilnehmer ein gesondertes Passwort, das dem Teilnehmer von der Bank mitgeteilt wird (siehe Nummer 2.1.2). Der Teilnehmer ist verpflichtet, dieses Passwort im Rahmen der Initialisierung zu ändern (siehe Nummer 2.2.2).

1.3 Authentifizierungssignatur (EBICS)
(1) Im Gegensatz zur EU, die Auftragsdaten signiert, wird die Authentifikationssignatur 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 Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom EDV-System des Kunden bzw. dessen beauftragten Dritten als auch vom Banksystem geleistet.
(2) Der Kunde bzw. der durch ihn beauftragte Dritte muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von der Bank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation prüft.

1.4 Verschlüsselung (EBICS)
(1) Zur Gewährleistung der Geheimhaltung der bankfachlichen Daten auf Anwendungsebene sind die Auftragsdaten vom Kunden bzw. vom durch ihn beauftragten Dritten unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Bank gemäß den Vorgaben der EBICS-Spezifikation zu verschlüsseln.
(2) Darüber hinaus ist auf den externen Übertragungsstrecken zwischen Kunden- und Banksystem zusätzlich eine Transportverschlüsselung vorzunehmen. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die gemäß den Vorgaben der EBICS-Spezifikation Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Bank prüft.

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 die nachfolgenden Daten zur Verfügung. Dabei vergibt die Bank jedem Teilnehmer eine eigene Teilnehmer-ID, die den Teilnehmer eindeutig identifiziert.

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

2.1.2 MCFT-Verfahren
- Kunden-ID
- Hostname
- IP-Adresse inkl. Port-Nummer
- Host-Typ
- Teilnehmer-ID
- erstes DFÜ-Passwort
- teilnehmerbezogener Startschlüssel per Bankparameterdatei (BPD)

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 Authentifikationssignatur 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.
- Für die zur Absicherung des Datenaustauschs 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 Teilnehmer unterschriebenen Ausdrucken der Authentifikations-, Verschlüsselungs- und Signaturschlüssel per Fax, per Post oder per E-Mail.

(3) Zu jedem öffentlichen Teilnehmerschlüssel enthalten die Authentifikations-, Verschlüsselungs- und Signaturschlüssel die Ausdrucke der 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 Teilnehmers auf den Ausdrucken der Authentifikations-, Verschlüsselungs- und Signaturschlüssel sowie die Übereinstimmung zwischen den per EBICS und den per Fax, per Post oder per E-Mail übermittelten Hashwerten des öffentlichen Teilnehmerschlüssels. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer endgültig 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 Dritter 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-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.
- 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 mittels der hierfür vorgesehenen systembedingten Auftragsarten und
- mit den vom Teilnehmer unterschriebenen Ausdrucken seiner Schlüssel per Fax, per Post oder per E-Mail.

(3) Zu dem öffentlichen Teilnehmerschlüssel enthalten die Ausdrucke der Schlüssel 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 Teilnehmers auf den Ausdrucken der Teilnehmerschlüssel sowie die Übereinstimmung zwischen den per MCFT und den per Fax, per Post oder per E-Mail übermittelten Hashwerten der öffentlichen Teilnehmerschlüssel. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Teilnehmer endgültig 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)

oder alternativ

- HCS – Aktualisierung aller drei oben genannten Schlüssel

(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 7 Absatz 3 der Bedingungen zur elektronischen Kontoführung 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-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 7 Absatz 3 der Bedingungen zur elektronischen Kontoführung 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 durchgeführt, wie etwa die Auftragsberechtigung. Die Ergebnisse weiterer bankfachlicher Prüfungen, wie beispielsweise Kontoberechtigungsprüfungen, werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.
(2) Sofern bei der Anwendung der Kunden-ID übergreifenden verteilten elektronischen Unterschrift (VEU) die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU für maximal 120 Tage im Banksystem gespeichert.
(3) Reicht ein Service-Rechenzentrum Auftragsdaten ein, deren Autorisierung durch den Kunden bzw. dessen Teilnehmer(n) mit personalisiertem Sicherheitsmerkmal (PIN/TAN) und Authentifizierungsinstrument (BFS-Token ggf. mit Token-PIN) erfolgt, ist vom Teilnehmer des Service-Rechenzentrums 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 sechs Unterschriften übermittelt werden.
(3) Ergibt die Prüfung auf der Bankseite, dass
- eine der im Startblock enthaltenen Unterschriften 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 bei Beendigung der Kommunikation oder des Dialogs übermittelt. Der Inhalt der Schlussnachrichten sowie die Ergebnisse weiterer bankfachlicher Prüfungen wie beispielsweise Kontoberechtigungsprüfungen werden dem Teilnehmer im DFÜ-Protokoll mitgeteilt.
(5) Sofern bei der Anwendung der Kunden-ID übergreifenden verteilten elektronischen Unterschrift (VEU) die übermittelten EU für die bankfachliche Freigabe nicht ausreichen, wird der Auftrag bis zur Abgabe aller erforderlichen EU im Banksystem gespeichert.

5 Protokollierung

5.1 DFÜ-Protokoll

(1) Die Bank dokumentiert jede erfolgreich durchgeführte Kommunikation, wie z. B.:
- Übertragung von 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,
- Fehler bei der Dekomprimierung.

(2) Der Teilnehmer hat dieses Protokoll, das inhaltlich den Bestimmungen von Kapitel 10 der Spezifikation der EBICS-Anbindung entspricht, zu seinen Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

5.2 Antwortcodes/Returncodes

Neben dem DFÜ-Protokoll gibt die Bank zusätzlich an den jeweiligen Kommunikationsweg gekoppelte Antwortcodes/ Returncodes aus, die nicht im DFÜ-Protokoll dokumentiert werden, sondern dem Kunden bzw. dessen beauftragten Dritten direkt im Dialog bzw. nach Abbau der Verbindung zum Banksystem mitgeteilt werden.

Stand: 13.01.2018