DEUTSCHE BUNDESBANK
EUROSYSTEM

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl

(EBICS-Bedingungen)

Stand: 21. November 2021

DEUTSCHE BUNDESBANK
EUROSYSTEM

EBICS-Bedingungen

Inhaltsverzeichnis

I. Servicebeschreibung ... 3
1. Kunden und Leistungsumfang ... 3
2. Technische Teilnehmer ... 3
3. Einschaltung von IT-Dienstleistern oder Service-Rechenzentren ... 3

II. Allgemeines ... 5
1. Nutzer ... 5
2. EBICS-Teilnehmer ... 5
3. Legitimations- und Sicherungsmedien ... 5

III. Verfahrensbestimmungen ... 6
1. Geltende Regelungen ... 6
2. Beachtung der geltenden Regelungen ... 6
3. Aufbau von Datensätzen, Dateien und Containern ... 7
4. Kundenkennung ... 7
5. Aufzeichnung der zu übertragenden Dateien bzw. Container ... 7
6. Abholung des Kundenprotokolls ... 8
7. Bereitstellung von noch nicht endgültig bearbeiteten Daten ... 8
8. Autorisierung der Auftragsdaten ... 8
9. Wirksamwerden von eingelieferten Auftragsdaten ... 8

IV. Verhaltens- und Sorgfaltspflichten ... 10
1. Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags ... 10
2. Umgang mit den Sicherungsmedien für den Datenaustausch ... 10
3. Sperre der Legitimations- und Sicherungsmedien ... 11

V. Behandlung eingehender Auftragsdaten durch die Bank ... 12
1. Prüfungen ... 12
2. Kundenprotokoll ... 12

VI. Sicherheit des Kundensystems ... 13

VII. Haftung ... 14
1. Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten DFÜ-Verfügung ... 14
2. Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien ... 14
2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige ... 14
2.2 Haftung der Bank ab der Sperranzeige ... 14
3. Haftungsausschluss ... 14

VIII. Änderungen der Besonderen Bedingungen ... 15

EBICS-Bedingungen

I. Servicebeschreibung

1. Kunden und Leistungsumfang

Die Deutsche Bundesbank (im Folgenden Bank) steht sonstigen Kontoinhabern ohne Bankleitzahl (im Folgenden Kunden) für die Datenfernübertragung auf elektronischem Wege – nachfolgend Datenfernübertragung oder DFÜ genannt – über EBICS (Electronic Banking Internet Communication Standard) zur Verfügung. Die Datenfernübertragung über EBICS umfasst die Auftragserteilung sowie den Datenaustausch (Übermittlung von Aufträgen und Informationsabruf). Sie kann für die Einlieferung und Abwicklung von Überweisungsaufträgen, Lastschriften und SCC-Karteneinzügen[1] sowie Widerrufe und Rückrufe zu diesen (alle im Folgenden Zahlungsaufträge), sofern elektronisch zugelassen, und die Bereitstellung von Dateien oder elektronischen Kontoinformationen genutzt werden. Die Zahlungsaufträge können entweder in einer physischen Datei oder in einem XML-Container, der mehrere jeweils voneinander unabhängige physische Dateien umfasst, an die Bank übermittelt werden.

Die EBICS-Kommunikation kann wahlweise mittels der EBICS-Version 2.5 (Nutzung von Auftragsarten) und/oder mittels der EBICS-Version 3.0.1 (Nutzung von BTF-Parametern) erfolgen. Bei Nutzung der EBICS-Version 3.0.1 sind für den Datenaustausch die Spezifikationen in den Anlagen 1a und 2 maßgeblich. Bei Nutzung der EBICS-Version 2.5 sind für den Datenaustausch die Spezifikationen in der Anlage 1b maßgeblich. Eine Unterstützung der EBICS-Version 2.5 wird von der Bank nur noch bis November 2022 angeboten.

2. Technische Teilnehmer

Für den Datenaustausch kann der Kunde Technische Teilnehmer benennen, die lediglich befugt sind, unter der EBICS-Kunden-ID des Kunden den Datenaustausch durchzuführen.

3. Einschaltung von IT-Dienstleistern oder Service-Rechenzentren

(1) Die Übermittlung von Zahlungsaufträgen kann auch unter Einschaltung eines IT-Dienstleisters oder eines Service-Rechenzentrums (im Folgenden gemeinsam SRZ) erfolgen. Das SRZ tritt dabei selbst als EBICS-Kunde mit eigener EBICS-Kunden-ID auf.

(2) Voraussetzung für die Teilnahme eines SRZ am Verfahren (im Folgenden SRZ-Verfahren) ist, dass

a) der Kunde bei der Bank die Teilnahme am beleglosen Datenaustausch unter Einschaltung eines Servicerechenzentrums (SRZ) per Datenfernübertragung (DFÜ) über EBICS zur Abwicklung von SEPA-Zahlungen und SCC-Karteneinzügen im Kunde-Bankverkehr (SRZ-Antrag sonstige Kontoinhaber ohne BLZ)“ beantragt hat und

[1] Verrechnung von Kartenzahlungen auf Basis des SEPA Card Clearing Formats

b) das SRZ mit der Bank eine „Vereinbarung mit einem Service-Rechenzentrum (SRZ), das in den beleglosen Datenaustausch per Datenfernübertragung (DFÜ) über EBICS zur Abwicklung von SEPA-Zahlungen und SCC-Karten-einzügen im Kunde-Bank-Verkehr eingeschaltet wird (SRZ-Vereinbarung)" unter Anerkennung der „Besondere Bedingungen der Deutschen Bundesbank für die Einschaltung von Service-Rechenzentren (SRZ) in die Abwicklung von SEPA-Zahlungen und SCC-Karteneinzügen im Kunde-Bank-Verkehr per Datenfernübertragung (DFÜ) (SRZ-Bedingungen)“ vereinbart hat.

(3) Im Falle der Einschaltung von SRZ gelten für den Kunden die nachfolgenden Bedingungen einschließlich Anlagen 1a und 1b zu diesen Bedingungen; die Übermittlung von Aufträgen durch das SRZ richtet sich nach der von dem SRZ gesondert mit der Bank geschlossen Vereinbarung gemäß Absatz 2 b).

II. Allgemeines

1. Nutzer

Zahlungsaufträge, sofern elektronisch zugelassen, können über die EBICS-Anbindung vom Kunden, einer Person, die gemäß Abschnitt I Nummer 3 Absatz 2 der Allgemeinen Geschäftsbedingungen der Deutschen Bundesbank für das Konto zeichnungsberechtigt ist (Zeichnungsberechtigte) oder einer vom Kunden hierzu gesondert ermächtigten Person erteilt werden. Kunde, Zeichnungsberechtigte und gesondert ermächtigte Personen werden im Folgenden einheitlich als Nutzer bezeichnet. Zur Autorisierung von per DFÜ übermittelten Auftragsdaten mittels Elektronischer Unterschrift benötigt jeder Nutzer jeweils individuelle, von der Bank freigeschaltete Legitimationsmedien. Die Anforderungen an die Legitimationsmedien sind in den Anlagen 1a und 1b definiert.

2. EBICS-Teilnehmer

Nutzer nach Abschnitt II Nummer 1 und Technische Teilnehmer nach Abschnitt I Nummer 2 werden im Folgenden unter dem Begriff EBICS-Teilnehmer zusammengefasst.

3. Legitimations- und Sicherungsmedien

(1) Für die Absicherung des Datenaustauschs benötigt jeder EBICS-Teilnehmer jeweils individuelle, von der Bank freigeschaltete Sicherungsmedien. Die Anforderungen an die Sicherungsmedien sind in den Anlagen 1a und 1b beschrieben.

(2) Sofern der Kunde als Legitimations- oder Sicherungsmedium eine Signaturkarte verwenden und hierfür keine am Markt frei käufliche Signaturkarte erwerben möchte, stellt die Bank für alle entgeltbefreiten Konten auf Antrag unentgeltlich Signaturkarten in der von dem Kunden gewünschten Anzahl zur Verfügung. Die erforderlichen Kartenlesegeräte sind vom Kunden auf eigene Kosten zu beschaffen.

(3) Eine von der Bank einem EBICS-Teilnehmer zur Legitimation/Sicherung bereitgestellte Signaturkarte ist bei Löschung des Zugangs des jeweiligen EBICS-Teilnehmers zu vernichten.

III. Verfahrensbestimmungen

1. Geltende Regelungen

Für das Verfahren gelten die in den Anlagen 1a und 1b zu diesen Bedingungen sowie die in der Anlage 1 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen („Spezifikation für die EBICS-Anbindung“[2]), die im Common Integrative Implementation Guide to Supplement the EBICS Specification und die in den nachfolgenden Verfahrensregeln beschriebenen Anforderungen:

- Verfahrensregeln der Deutschen Bundesbank für sonstige Kontoinhaber ohne Bankleitzahl zur Abwicklung von SEPA-Lastschriften per Datenfernübertragung (DFÜ) (Verfahrensregeln SEPA-Lastschriften für sonstige Kontoinhaber ohne BLZ)
- Verfahrensregeln der Deutschen Bundesbank für sonstige Kontoinhaber ohne Bankleitzahl zur Abwicklung von SEPA-Überweisungen per Datenfernübertragung (DFÜ) (Verfahrensregeln SEPA-Überweisungen für sonstige Kontoinhaber ohne BLZ)
- Verfahrensregeln der Deutschen Bundesbank für sonstige Kontoinhaber ohne Bankleitzahl zur Abwicklung von SCC-Karteneinzügen per Datenfernübertragung (DFÜ) (Verfahrensregeln SCC-Karteneinzüge sonstige Kontoinhaber ohne BLZ)
- Verfahrensregeln der Deutschen Bundesbank für sonstige Kontoinhaber ohne Bankleitzahl zur Abwicklung von SEPA-Echtzeitüberweisungen per Datenfernübertragung (DFÜ) (Verfahrensregeln SEPA-Echtzeitüberweisungen sonstige Kontoinhaber ohne BLZ)
- Verfahrensregeln der Deutschen Bundesbank zur Abwicklung von taggleichen Zahlungen in Euro sowie von Zahlungen in ausländischen Währungen im Hausbankverfahren-Individual (HBV-Individual) (Verfahrensregeln HBV-Individual)
- Verfahrensregeln der Deutschen Bundesbank zur Abwicklung grenzüberschreitender Euro-Massenzahlungen über HBV-IMPay (Verfahrensregeln HBV-IMPay) und
- Verfahrensregeln der Deutschen Bundesbank zum Abruf von elektronischen Kontoinformationen (Verfahrensregeln elektronische Kontoinformationen).

2. Beachtung der geltenden Regelungen

Der Kunde ist verpflichtet sicherzustellen, dass alle EBICS-Teilnehmer die mit der Bank vereinbarten Verfahren und Verfahrensregeln beachten.

---

2 Die Spezifikation ist auf der Webseite www.ebics.de abrufbar.

3. Aufbau von Datensätzen, Dateien und Containern

(1) Der Satz- und Dateiaufbau sowie der Containeraufbau für die Übermittlung von Zahlungsaufträgen richten sich nach den jeweiligen Verfahrensregeln.

(2) Die Angaben im Verwendungszweck haben sich ausschließlich auf den jeweiligen Zahlungsvorgang im Datensatz zu beziehen. Am Anfang des Datenfeldes „Verwendungszweck“ sind linksbündig solche Angaben unterzubringen, auf die der Zahlungsempfänger bei Überweisungen/Zahler bei Lastschriften bzw. bei SCC-Karteneinzügen maschinell zuzugreifen beabsichtigt oder die der Zahler von Überweisungen/Zahlungsempfänger bei Lastschriften bzw. bei SCC-Karteneinzügen benötigt, falls die Zahlung als unanbringlich beziehungsweise unbezahlt an ihn zurückgeleitet wird.

Die Belegung der Verwendungszweckangaben darf außerdem vom Nutzer nicht für die Vorgabe eines von ihm gewünschten Druckbildes benutzt werden, ohne dass die Stellenkapazität im Datenfeld „Verwendungszweck“ des Datensatzes sowie in den etwaigen nachfolgenden Erweiterungsteilen mit Verwendungszweckangaben voll ausgenutzt ist.

(3) Verwendungszweckangaben dürfen nicht die Übermittlung einer gesonderten Nachricht außerhalb des Zahlungsverkehrs (z. B. Rechnung, Lohn- und Gehaltsabrechnung) ersetzen. Werbetexte dürfen in den Verwendungszweckangaben nicht enthalten sein.

4. Kundenkennung

Der Nutzer hat die Kundenkennung des Zahlungsempfängers bei Überweisungen bzw. des Zahlers bei Lastschriften/SCC-Karteneinzügen (regelmäßig IBAN) zutreffend anzugeben. Die in die Abwicklung des Zahlungsauftrages eingeschalteten Zahlungsdienstleister sind berechtigt, die Bearbeitung ausschließlich anhand der Kundenkennung vorzunehmen. Fehlerhafte Angaben können Fehlleitungen des Auftrags zur Folge haben. Schäden und Nachteile, die hieraus entstehen, gehen zu Lasten des Kunden.

5. Aufzeichnung der zu übertragenden Dateien bzw. Container

Vor der Übertragung von Auftragsdaten an die Bank ist eine Aufzeichnung der zu übertragenden Dateien bzw. Container mit deren vollständigem Inhalt sowie der zur Prüfung der Legitimation übermittelten Daten zu erstellen. Diese ist von dem Kunden mindestens für einen Zeitraum von 10 Kalendertagen ab dem in der Datei angegebenen Ausführungstermin (für Überweisungen) bzw. Fälligkeitstermin (Lastschriften) oder bei mehreren Terminen dem spätesten Termin in der Form nachweisbar zu halten, dass die Datei bzw. der Container auf Anforderung der Bank kurzfristig erneut zur Verfügung gestellt werden kann.

6. Abholung des Kundenprotokolls

Der Kunde ist verpflichtet, das Kundenprotokoll (siehe Anlagen 1a und 1b), das nach Einreichung eines Auftrags vom EBICS-System der Bank automatisch erstellt wird, regelmäßig abzuholen. Das Kundenprotokoll ist zu den Unterlagen zu nehmen und auf Anforderung der Bank zur Verfügung zu stellen.

7. Bereitstellung von noch nicht endgültig bearbeiteten Daten

Soweit die Bank dem Kunden Daten über Zahlungsvorgänge zur Verfügung stellt, die noch nicht endgültig bearbeitet sind, stellen diese lediglich eine unverbindliche Information dar. Die Daten sind jeweils besonders gekennzeichnet.

8. Autorisierung der Auftragsdaten

Die per DFÜ vom Kunden eingelieferten Auftragsdaten sind mit Elektronischer Unterschrift zu autorisieren.

Sofern der Datenaustausch über ein SRZ stattfindet, erfolgt die Autorisierung durch den Kunden bei

- SEPA-Überweisungen mittels Verteilter Elektronischer Unterschrift (VEU)
- SEPA-Lastschriften mittels VEU bzw. pauschal (Pauschalautorisierung)
- SCC-Karteneinzügen pauschal (Pauschalautorisierung).

Bei Pauschalautorisierung ist die Bank berechtigt, den Auftrag gemäß seinem vom SRZ gelieferten Inhalt zu bearbeiten und auszuführen.

9. Wirksamwerden von eingelieferten Auftragsdaten

Eingelieferte Auftragsdaten werden als Auftrag wirksam, wenn

- alle erforderlichen Elektronischen Unterschriften der Nutzer per Datenfernübertragung innerhalb eines Zeitraumes von 120 Stunden nach Auftragseingang eingegangen sind und
- die Elektronischen Unterschriften mit den vereinbarten Schlüsseln erfolgreich geprüft werden können.

Bei Pauschalautorisierung werden die Auftragsdaten bei Einlieferung als Auftrag wirksam.

10. Berechtigung zur Einlieferung von Dateien und zur Abholung bereitgestellter Auslieferungsdaten

Die Einlieferung von Dateien und die Abholung bereitgestellter Zahlungsverkehrs- und Kontoinformationen kann je EBICS-Teilnehmer auf ein oder mehrere Konten beschränkt werden.

IV. Verhaltens- und Sorgfaltspflichten

1. Umgang mit den Legitimationsmedien für die Autorisierung des Auftrags

(1) Der Kunde ist verpflichtet sicherzustellen, dass alle Nutzer die Pflichten aus diesen Bedingungen und die in den Anlagen 1a und 1b beschriebenen Legitimationsverfahren einhalten.

(2) Mit Hilfe eines von der Bank freigeschalteten Legitimationsmediums kann der Nutzer Aufträge erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Legitimationsmediums kommt oder Kenntnis von dem zu dessen Schutz dienenden Passwort erlangt. Die Bank weist darauf hin, dass jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikats ist, in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen kann. Insbesondere Folgendes ist zum Schutz des Legitimationsmediums und des Passwortes zu beachten:

- Das Legitimationsmedium muss vor unberechtigtem Zugriff geschützt und sicher verwahrt werden;
- das zum Schutz des Legitimationsmediums dienende Passwort darf nicht auf dem Legitimationsmedium notiert oder als Abschrift mit diesem zusammen aufbewahrt werden oder ungesichert elektronisch abgespeichert werden;
- das Legitimationsmedium darf nicht dupliziert werden;
- bei Eingabe des Passwortes ist sicherzustellen, dass andere Personen dieses nicht ausspähen können;
- die Bank wird keine Anfragen zum Personalisierten Sicherheitsmerkmal bzw. Aufforderungen zu dessen Eingabe versenden, so dass der EBICS-Teilnehmer davon ausgehen muss, dass es sich bei einer solchen Aufforderung um den Versuch handelt, das Passwort/Personalisierte Sicherheitsmerkmal auszuspähen. Daher dürfen Anfragen, in denen nach vertraulichen Daten wie dem Passwort/der Signatur-PIN gefragt wird, nicht beantwortet werden.

2. Umgang mit den Sicherungsmedien für den Datenaustausch

(1) Der Kunde ist verpflichtet sicherzustellen, dass alle EBICS-Teilnehmer die in den Anlagen 1a und 1b beschriebenen Sicherungsverfahren einhalten.

(2) Mit Hilfe der von der Bank freigeschalteten Sicherungsmedien sichert der EBICS-Teilnehmer den Datenaustausch ab. Der Kunde ist verpflichtet sicherzustellen, dass jeder EBICS-Teilnehmer dafür Sorge trägt, dass keine andere Person in den Besitz seines Sicherungsmediums kommt oder dieses nutzen kann. Insbesondere im Falle der Ablage auf einem

technischen System muss das Sicherungsmedium des EBICS-Teilnehmers in einer technischen Umgebung gespeichert werden, die vor unautorisiertem Zugriff geschützt ist. Die Bank weist darauf hin, dass jede andere Person, die das DFÜ-Passwort kennt, den Datenaustausch mit der Bank missbräuchlich durchführen kann.

3. Sperre der Legitimations- und Sicherungsmedien

(1) Gehen die Legitimations- oder Sicherungsmedien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der EBICS-Teilnehmer unverzüglich seinen DFÜ-Zugang bei der Bank zu sperren bzw. sperren zu lassen. Die Sperre des Legitimations- oder Sicherungsmediums (z. B. bei der Signaturkarte durch fünfmalige Falscheingabe des Passwortes/der Signatur-PIN) alleine reicht nicht aus. Näheres regeln die Anlagen 1a und 1b.

(2) Hat der Kunde Kenntnis von dem Verlust oder dem Bekanntwerden der Legitimations- oder Sicherungsmedien eines EBICS-Teilnehmers oder besteht der Verdacht ihrer missbräuchlichen Nutzung, ist er zur Veranlassung der Sperre des DFÜ-Zugangs des EBICS-Teilnehmers durch Aufgabe einer Sperranzeige bei der Bank verpflichtet. Zudem kann der Kunde auch den gesamten DFÜ-Zugang entsprechend sperren lassen. Näheres regeln die Anlagen 1a und 1b.

(3) Die Bank wird den gesamten DFÜ-Zugang sperren, wenn der Verdacht einer missbräuchlichen Nutzung des DFÜ-Zugangs besteht. Sie wird den Kunden hierüber außerhalb des DFÜ-Verfahrens informieren. Diese Sperre kann mittels DFÜ nicht aufgehoben werden.

V. Behandlung eingehender Auftragsdaten durch die Bank

1. Prüfungen

(1) Die Bank prüft anhand der von den EBICS-Teilnehmern mittels der Sicherungsmedien erstellten Signaturen, ob der Absender berechtigt ist, den Datenaustausch durchzuführen. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht verarbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen.

(2) Die Bank prüft die Legitimation des Nutzers beziehungsweise der Nutzer und die Autorisierung der per DFÜ übermittelten Auftragsdaten anhand der von den Nutzern mittels der Legitimationsmedien erstellten Elektronischen Unterschriften bzw. bei Teilnahme am SRZ-Verfahren und vereinbarter Pauschalautorisierung anhand der im EBICS-System der Bank hinterlegten Pauschalautorisierung sowie die Übereinstimmung der Auftragsdatensätze zu Überweisungsaufträgen und Lastschriften mit den Bestimmungen der „Spezifikation der Datenformate“ entsprechend Anlage 3 des DFÜ-Abkommens[3], den jeweiligen Verfahrensregeln sowie der Anlagen 1a und 1b, Nummer 5.2 zu diesen Bedingungen und die Übereinstimmung der Auftragsdatensätze zu SCC-Karteneinzügen mit den entsprechenden Verfahrensregeln sowie der Anlagen 1a und 1b, Nummer 5.2 zu diesen Bedingungen. Ergibt die Prüfung Unstimmigkeiten, wird die Bank die betreffenden Auftragsdaten nicht bearbeiten und dem Kunden hierüber unverzüglich eine Information zur Verfügung stellen. Die Bank löscht nicht vollständig autorisierte Auftragsdaten automatisiert nach Ablauf von 120 Stunden nach Auftragseingang.

(3) Ergeben sich bei den von der Bank durchgeführten Prüfungen der Dateien oder Datensätze nach den jeweiligen Verfahrensregeln Fehler, so wird die Bank die fehlerhaften Dateien oder Datensätze in geeigneter Form nachweisen und sie dem Nutzer unverzüglich mitteilen. Die Bank ist berechtigt, die fehlerhaften Dateien oder Datensätze von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

2. Kundenprotokoll

Die Bank ist verpflichtet, die vorstehenden Abläufe und die Weiterleitung der Aufträge zur Bearbeitung im Kundenprotokoll (siehe Anlagen 1a und 1b) zu dokumentieren. Der Kunde ist seinerseits verpflichtet, das Kundenprotokoll zeitnah abzurufen und sich über den Status der Auftragsbearbeitung zu informieren. Bei Unstimmigkeiten soll er sich mit der Bank in Verbindung setzen.

---

[3] Die Spezifikation ist auf der Webseite www.ebics.de abrufbar.

VI. Sicherheit des Kundensystems

Der Kunde hat für einen ausreichenden Schutz der von ihm für die Datenfernübertragung eingesetzten Systeme Sorge zu tragen. Die für das EBICS-Verfahren geltenden Sicherheitsanforderungen sind in Anlage 3 beschrieben.

VII. Haftung

1. Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten DFÜ-Verfügung

Die Haftung der Bank bei einer nicht autorisierten DFÜ-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten DFÜ-Verfügung richtet sich nach Abschnitt I Nummer 12 ff. der Allgemeinen Geschäftsbedingungen der Deutschen Bundesbank.

2. Haftung des Kunden bei missbräuchlicher Nutzung der Legitimations- oder Sicherungsmedien

2.1 Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen aufgrund einer missbräuchlichen Nutzung der Legitimations- oder Sicherungsmedien, haftet der Kunde gegenüber der Bank für die ihr dadurch entstehenden Schäden, wenn der EBICS-Teilnehmer fahrlässig oder vorsätzlich gegen seine Verhaltens- und Sorgfaltspflichten verstoßen hat.

(2) Der Kunde ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn der EBICS-Teilnehmer seinen DFÜ-Zugang nicht sperren sowie der Kunde und der EBICS-Teilnehmer die Sperranzeige nach Abschnitt IV Nummer 3 Absatz 1 bzw. Absatz 2 nicht abgeben konnten, weil die Bank nicht die Möglichkeit zur Sperrung bzw. Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch vermieden worden wäre. Satz 1 gilt nicht, wenn der Kunde oder der EBICS-Teilnehmer in betrügerischer Absicht gehandelt hat.

2.2 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige erhalten hat oder der DFÜ-Zugang gesperrt wurde, übernimmt sie alle danach durch nicht autorisierte DFÜ-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Kunde oder ein EBICS-Teilnehmer in betrügerischer Absicht gehandelt hat.

3. Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

VIII. Änderungen der Besonderen Bedingungen

Für Änderungen dieser Besonderen Bedingungen gilt Abschnitt I Nummer 2 Absatz 1 der Allgemeinen Geschäftsbedingungen der Deutschen Bundesbank mit der Maßgabe, dass an Stelle der Bekanntmachung im Bundesanzeiger die schriftliche Mitteilung an den Kunden tritt.

Anhang

Anlage 1a: EBICS-Anbindung sonstige Kontoinhaber ohne BLZ
(Spezifikation für die EBICS-Anbindung, Version 3.0.1)
Anlage 1b: EBICS-Anbindung sonstige Kontoinhaber ohne BLZ
(Spezifikation für die EBICS-Anbindung, Version 2.5)
Anlage 2: BTF-Parameterwerte (Business Transactions & Formats)
Anlage 3: Sicherheitsanforderungen an das EBICS-Kundensystem

DEUTSCHE BUNDESBANK
EUROSYSTEM

Anlage 1a
zu den

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)

(EBICS-Anbindung sonstige Kontoinhaber ohne BLZ)

Spezifikation für die EBICS-Anbindung, Version 3.0.1
.

Stand: 21. November 2021

Inhaltsverzeichnis

1 Zulassung zum Produktionsbetrieb 4

2 Legitimations- und Sicherungsverfahren 6

2.1 Elektronische Unterschriften 6

2.2 Authentifikationssignatur 7

2.3 Verschlüsselung 7

3 Initialisierung der EBICS-Anbindung 8

3.1 Einrichtung der Kommunikationsverbindung 8

3.2 Initialisierung der Schlüssel 8

3.2.1 Neuinitialisierung der Teilnehmerschlüssel 8

3.2.2 Initialisierung der bankseitigen Schlüssel 10

4 Besondere Sorgfaltspflichten bei Erzeugung von Legitimations- und Sicherungsmedien durch den Kunden 11

5 Auftragserteilung an die Deutsche Bundesbank 12

5.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU) 13

5.2 Zulässige BTF-Parameter (BTF = Business Transaction Formats) 13

5.2.1 Einlieferung von Zahlungsaufträgen 13

5.2.2 Auslieferung von Zahlungsverkehrs- und Kontoinformationen 14

5.3 Kundenprotokolle 15

5.3.1 Aufbau des Kundenprotokolls im XML-Format – HAC 16

5.3.1.1 FÜR DIE EINLIEFERUNG TAGGLEICHER EURO-ÜBERWEISUNGEN (GT- ODER DT-DATEI): 16

5.3.1.2 FÜR DIE EINLIEFERUNG VON AZV-ÜBERWEISUNGEN (WT-DATEI) : 17

5.3.1.3 FÜR DIE EBICS-INTERNE ABBILDUNG DER IM SRZ-VERFAHREN EINGEREICHTEN SEPA-ZAHLUNGEN 19

5.4 Auftragsnummer 20

6 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung 21

7 Regelmäßige Änderung des öffentlichen Bankschlüssels 22

8 Sperrung der Teilnehmerschlüssel 23

9 Testanforderungen 24

9.1 Grundsätzliches 24

9.2 Testszenarien 25
9.2.1 Initialisierung der EBICS-Anbindung 25
9.2.2 Download Transaktionen 26
9.2.3 Datenaustausch über die EBICS-Anbindung 26

1 Zulassung zum Produktionsbetrieb

Für die EBICS-Kommunikation ist zunächst von jedem Kunden ein Zulassungs- und Conformancetest zu durchlaufen (nähere Einzelheiten siehe Nummer 9 „Testanforderungen“).

Die Zulassung zum Produktionsbetrieb für die EBICS-Kommunikation ist vom Kunden (Kontoinhaber) mit dem Vordruck 4760 „Antrag auf EBICS-Kommunikation sonstige Kontoinhaber ohne Bankleitzahl“ beim zuständigen Kundenbetreuungsservice (KBS) zu beantragen. Im Antrag ist festzulegen, für welche Konten die Zulassungsberechtigungen für die Einlieferung von Dateien und Abholung von Zahlungsverkehrs- und Kontoinformationen zu einer EBICS-Kunden-ID gelten sollen.

Dabei gilt die kontobezogene Beschränkung der Berechtigung zur Abholung von Informationen für nachstehend genannte EBICS-BTF-Parameter:

- im HBV-Individual:
  DCT/BIL/URG/gtbbksw, REP/BIL/URG/m3bbksw, OTH/BIL/URG/m6bbksw, REP/BIL/URG/m7bbksw, REP/BIL/URG/m8bbksw, REP/BIL/URG/m9bbksw, REP/BIL/URG/wabbksw bzw. STM/DE//camt.054/ZIP,
- im HBV-IMPay:
  REP/BIL/URG/m3bbksw, REP/BIL/URG/m7bbksw, REP/BIL/URG/m8bbksw
- im HBV-SEPA:
  STM/DE//camt.054/ZIP,
- im HBV-Echtzeit:
  STM/DE//camt.054/ZIP, STM/DE/SCI/camt.054/ZIP und
- in der Elektronischen Kontoinformation:
  STM/DE//camt.052/ZIP, EOP/DE//camt.053/ZIP oder EOP/DE//mt940

Die anderen EBICS-BTF-Parameter zur Abholung, d. h. REP/DE/SCT/pain.002/ZIP im HBV-Individual, REP/DE/SCI/pain.002/ZIP im HBV-Echtzeit, OTH/BIL//rfbbkazv im HBV-IMPay, REP/DE/SDD/pain.002/ZIP und REP/DE/SCT/pain.002/ZIP im HBV-SEPA und OTH/DE//wssparam, werden von der kontobezogenen Beschränkung nicht erfasst.

Darüber hinaus sind weitere Antragsvordrucke für die elektronische Ein- und Auslieferung für die Fachverfahren je nach individuellem Bedarf einzureichen. Dazu gehören z. B. die Vordrucke:

- Antrag auf elektronische Ein- und Auslieferung für das Hausbankverfahren-Individual (HBV-Individual) der Deutschen Bundesbank (Vordr. 4781 a)

- Antrag auf elektronische Einlieferung für das Hausbankverfahren-IMPay (HBV-IMPay) der Deutschen Bundesbank (Vordr. 4740)
- Antrag auf elektronische Ein- und Auslieferung für das Hausbankverfahren-SEPA (HBV-SEPA) der Deutschen Bundesbank (Vordr. 4767)
- Antrag auf elektronische Ein- und Auslieferung für das Hausbankverfahren-Echtzeit (HBV-Echtzeit) der Deutschen Bundesbank (Vordr. 4775)

Die aktuellen Vordrucke werden auf der Internetseite der Deutschen Bundesbank unter „*www.*bundesbank.de > *Aufgaben* > *Unbarer Zahlungsverkehr* > *Serviceangebot* >*Vordrucke“* bereitgestellt. Informationen zu den individuell benötigten Unterlagen für den Zugang zu den Fachverfahren sind den jeweiligen anwendungsspezifischen Verfahrensregeln zu entnehmen. Das Kundentestzentrum ist im Rahmen der Testaktivitäten bei der Auswahl der individuell benötigten Vordrucke behilflich.

2 Legitimations- und Sicherungsverfahren

Der Kunde (Kontoinhaber) benennt der Deutschen Bundesbank im Rahmen der Antragsstellung die EBICS-Teilnehmer und deren Berechtigungen im Rahmen der EBICS-Kommunikation.

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

- Elektronische Unterschriften
- Authentifikationssignatur
- Verschlüsselung

Für jedes Legitimations- und Sicherungsverfahren verfügt der EBICS-Teilnehmer über ein individuelles Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Die öffentlichen Teilnehmerschlüssel sind der Deutschen Bundesbank gemäß dem in Nummer 3 beschriebenen Verfahren mitzuteilen. Die öffentlichen Bankschlüssel sind gemäß dem in Nummer 3 beschriebenen Verfahren gegen unautorisiertes Verändern zu schützen. Die Schlüsselpaare des EBICS-Teilnehmers können auch für die Kommunikation mit Dritten eingesetzt werden.

Im Rahmen der EBICS-Kommunikation ist eine MAC-Sicherung nicht mehr erforderlich. Entsprechende Feldbelegungen werden nicht mehr ausgewertet.

2.1 Elektronische Unterschriften

Für die Elektronischen Unterschriften (EU) der EBICS-Teilnehmer sind die folgenden Unterschriftsklassen definiert:

- Einzelunterschrift (Typ „E")
- Erstunterschrift (Typ „A")
- Zweitunterschrift (Typ „B")
- Transportunterschrift (Typ „T")

EU vom Typ „E", „A", oder „B" werden als bankfachliche EU bezeichnet; sie dienen der Autorisierung von Aufträgen. Aufträge können mehrere bankfachliche EU benötigen, die von unterschiedlichen Nutzern (Kontoinhaber, Zeichnungsberechtigte und gesondert ermächtigte Personen) geleistet werden müssen. Die EU bilden die auf dem Unterschriftenblatt hinterlegten Berechtigungen ab. Eine Einschränkung der Unterschriftsklasse der EBICS-Teilnehmer gegenüber der Berechtigung gemäß Unterschriftenblatt ist zulässig. Die EU von gesondert ermächtigten Personen ergibt sich aus dem jeweiligen Antrag auf EBICS-Kommunikation sonstige Kontoinhaber ohne Bankleitzahl.
EU vom Typ „T" können nicht zur Autorisierung von Aufträgen verwendet werden, sondern lediglich zu deren Übertragung an das Banksystem. "Technische Teilnehmer" (siehe Nummer 3.2) können nur eine EU vom Typ „T" zugewiesen bekommen.

Mit dem vom Kunden verwendeten Programm können verschiedene Nachrichten (z. B. SEPA-Überweisungen, Aufträge für Initialisierung, Protokollabruf etc.) erstellt werden. Die Deutsche Bundesbank teilt dem Kunden im Rahmen der Zulassung mit, welche EBICS-BTF-Parameter genutzt werden können und welcher EU-Typ hierfür anzuwenden ist.

2.2 Authentifikationssignatur

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 Kunden- als auch vom Banksystem geleistet. Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Authentifikationssignatur jeder von der Deutschen Bundesbank übermittelten EBICS-Nachricht unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation prüft.

2.3 Verschlüsselung

Zur Gewährleistung der Geheimhaltung der bankfachlichen Daten auf Anwendungsebene sind die Auftragsdaten vom Kunden unter Berücksichtigung der Aktualität und Authentizität der gespeicherten öffentlichen Schlüssel der Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation zu verschlüsseln.

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 Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Deutschen Bundesbank gemäß den Vorgaben der EBICS-Spezifikation überprüft.

3 Initialisierung der EBICS-Anbindung

3.1 Einrichtung der Kommunikationsverbindung

Der Kommunikationsaufbau erfolgt unter Verwendung einer URL (Uniform Resource Locator). Alternativ kann auch die IP-Adresse der Deutschen Bundesbank benutzt werden. Die URL oder die IP-Adresse werden dem Kunden mitgeteilt.

Die Deutsche Bundesbank teilt den vom Kunden benannten EBICS-Teilnehmern zur Aufnahme der EBICS-Anbindung folgende Daten mit:

- URL oder IP-Adressen der Deutschen Bundesbank
- Host-ID
- Zulässige Version für das EBICS-Protokoll und der Sicherungsverfahren (EBICS-Version 3.0.1 sowie Schemaversion H005. Die Version 2.5 mit Schema H004 wird noch bis zum November 2022 unterstützt; die älteren Versionen H002 und H003 werden nicht mehr unterstützt.)
- Kunden-ID
- EBICS-Teilnehmer-ID
- Weitere spezifische Angaben zu Kunden- und EBICS-Teilnehmerberechtigungen

Für die dem Kunden zugeordneten EBICS-Teilnehmer vergibt die Deutsche Bundesbank jeweils eine EBICS-Teilnehmer-ID, die den EBICS-Teilnehmer eindeutig identifiziert. Soweit dem Kunden ein oder mehrere technische Teilnehmer zugeordnet sind (Multi-User-System), vergibt die Deutsche Bundesbank zusätzlich eine EBICS-Teilnehmer-ID für jeden technischen Teilnehmer.

3.2 Initialisierung der Schlüssel

3.2.1 Neuinitialisierung der Teilnehmerschlüssel

Die vom EBICS-Teilnehmer eingesetzten Schlüsselpaare für die bankfachliche EU, die Verschlüsselung der Auftragsdaten und die Authentifikationssignatur müssen zusätzlich zu den in Nummer 2 beschriebenen allgemeinen Bedingungen den nachfolgenden Anforderungen genügen:

1. Die Schlüsselpaare sind ausschließlich und eindeutig dem EBICS-Teilnehmer zuge-ordnet.
2. Soweit der EBICS-Teilnehmer seine Schlüssel eigenständig generiert, sind die privaten Schlüssel mit Mitteln zu erzeugen, die der EBICS-Teilnehmer unter seiner alleinigen Kontrolle halten kann.

3. Sofern die Schlüssel von einem Dritten zur Verfügung gestellt werden, ist sicherzustellen, dass der EBICS-Teilnehmer in den alleinigen Besitz der privaten Schlüssel gelangt.
4. Für die zur Legitimation eingesetzten privaten Schlüssel definiert jeder Nutzer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert.
5. Für die zur Absicherung des Datenaustausches eingesetzten privaten Schlüssel definiert jeder EBICS-Teilnehmer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert. Auf dieses Passwort kann verzichtet werden, wenn das Sicherungsmedium des EBICS-Teilnehmers in einer technischen Umgebung gespeichert wird, die vor unautorisiertem Zugriff geschützt ist.

Für die Initialisierung des EBICS-Teilnehmers bei der Deutschen Bundesbank ist die Übermittlung der öffentlichen Schlüssel des EBICS-Teilnehmers an das Banksystem erforderlich. Hierfür übermittelt der EBICS-Teilnehmer der Deutschen Bundesbank seine öffentlichen Schlüssel auf zwei voneinander unabhängigen Kommunikationswegen:

- Über die EBICS-Anbindung mittels der hierfür vorgesehenen administrativen Auftragsarten INI und HIA.
- Mit einem vom Kontoinhaber oder Zeichnungsberechtigten unterschriebenen Initialisierungsbrief an den zuständigen Kundenbetreuungsservice (KBS). Dieser übermittelt die Unterlagen der zuständigen Stammdatenverwaltung.

Hierbei ist zu beachten, dass bei der elektronischen Einreichung der administrativen Auftragsarten INI und HIA die Laufzeit dieser Aufträge auf 120 Stunden begrenzt ist. Wenn die Initialisierungsbriefe zum Ablaufzeitpunkt noch nicht bei der Stammdatenverwaltung der Deutschen Bundesbank vorliegen, muss die Einreichung wiederholt werden.

Für die Freischaltung des EBICS-Teilnehmers überprüft die Deutsche Bundesbank auf Basis der vom Kontoinhaber, Zeichnungsberechtigten oder von der gesondert ermächtigten Person unterschriebenen Initialisierungsbriefe die Authentizität der über EBICS übermittelten öffentlichen Teilnehmerschlüssel.

Zu jedem öffentlichen Teilnehmerschlüssel enthält der Initialisierungsbrief die folgenden Daten:

- Verwendungszweck des öffentlichen Teilnehmerschlüssels
- Elektronische Unterschrift
- Authentifikationssignatur
- Verschlüsselung
- Die jeweils unterstützte 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
- Datum und Uhrzeit der Generierung
- Kunden-ID und EBICS-Teilnehmer-ID
- Host-ID

Die Deutsche Bundesbank prüft die Unterschrift des Kontoinhabers oder der/des Zeichnungsberechtigten bzw. der gesondert ermächtigten Person auf dem Initialisierungsbrief mit den in der Kontoführung bzw. auf dem Vordruck 4760 hinterlegten Unterschriften sowie die Übereinstimmung zwischen den über die EBICS-Anbindung und den schriftlich übermittelten Hashwerten des öffentlichen Schlüssels des EBICS-Teilnehmers. Bei positivem Prüfergebnis schaltet die Deutsche Bundesbank den betreffenden EBICS-Teilnehmer für die vereinbarten Auftragsarten frei.

3.2.2 Initialisierung der bankseitigen Schlüssel

Der EBICS-Teilnehmer holt den öffentlichen Schlüssel der Deutschen Bundesbank mittels einer eigens dafür vorgesehenen administrativen Auftragsart HPB ab.

Der Hashwert des öffentlichen Bankschlüssels wird dem Kunden von der Deutschen Bundesbank im Rahmen der Antragstellung mitgeteilt. Vor dem ersten Einsatz hat der EBICS-Teilnehmer die Echtheit der ihm per Datenfernübertragung übermittelten öffentlichen Bankschlüssel dadurch zu überprüfen, dass er deren Hashwerte mit den Hashwerten vergleicht, die von der Deutschen Bundesbank im Rahmen der Antragstellung übermittelt wurden.
Der Kunde muss gewährleisten, dass eine Software eingesetzt wird, die die Gültigkeit der im Rahmen der Transportverschlüsselung eingesetzten Serverzertifikate anhand des von der Deutschen Bundesbank im Rahmen der Antragstellung mitgeteilten Zertifizierungspfades überprüft.

4 Besondere Sorgfaltspflichten bei Erzeugung von Legitimations- und Sicherungsmedien durch den Kunden

Soweit der Kunde seine Legitimations- und Sicherungsmedien nach den Vorgaben der EBICS-Spezifikation selbst erzeugt und er diese bei der Deutschen Bundesbank initialisiert, hat er Folgendes sicherzustellen:

- In allen Phasen der Authentifizierung, inklusive Anzeige, Übermittlung und Speicherung sind Vertraulichkeit und Integrität des Legitimationsmediums zu gewährleisten.
- Private Teilnehmerschlüssel auf den Legitimations- und Sicherungsmedien dürfen nicht im Klartext abgespeichert werden.
- Spätestens nach fünfmaliger Fehleingabe des Passwortes wird das Legitimationsmedium gesperrt.
- Die Generierung der privaten und öffentlichen Teilnehmerschlüssel muss in einer sicheren Umgebung erfolgen.
- Die Legitimations- und Sicherungsmedien sind ausschließlich und eindeutig dem Teilnehmer zuzuordnen und zu verwenden.

5 Auftragserteilung an die Deutsche Bundesbank

Der Nutzer überprüft die Auftragsdaten auf ihre Richtigkeit und stellt sicher, dass genau diese Daten elektronisch unterschrieben werden.

Bei jeder Aufnahme der Kommunikation wird seitens der Bundesbank zunächst die Überprüfung der Auftragsparameter vorgenommen. Im Falle einer ungültigen administrativen Auftragsart oder einer unzulässigen BTF-Parameterwertkombination erfolgt eine Rückweisung mit dem technischen Returncode „EBICS_INVALID_ORDER_IDENTIFIER“ oder „EBICS_UNSUPPORTED_ORDER_TYPE“ bei einem gültigen, jedoch nicht von der Deutschen Bundesbank unterstützten Auftrag. Um eine Rückweisung zu vermeiden sind daher in der Kommunikation mit der Deutschen Bundesbank nur die von der Deutschen Bundesbank definierten BTF-Parameterwertkombinationen zu verwenden. Auch die Belegung von optionalen Feldern zu MessageName in den BTF-Parametern führen zur Abweisung der Aufträge.

Nach erfolgreicher Prüfung der Auftragsparameter wird seitens der Deutschen Bundesbank der Hashwert des aktuell gültigen öffentlichen Bankschlüssels geprüft. Sofern die Deutsche Bundesbank neben dem aktuellen Bankschlüssel vorübergehend auch noch den vorhergehenden Bankschlüssel unterstützt, erhält der Kunde bei der ersten Dateieinreichung, die noch unter Verwendung des vorhergehenden Bankschlüssels erfolgt, eine Rückweisung mit dem EBICS Return Code „EBICS_BANK_PUBKEY_UPDATE_REQUIRED“. Die Fehlermeldung weist auf die Verwendung des vorhergehenden Bankschlüssels und die Notwendigkeit einer Aktualisierung desselben hin. Zusätzlich wird einmalig ein Eintrag im Kundenprotokoll geschrieben, der auf den veralteten öffentlichen Bankschlüssel hinweist. Die abgewiesene Datei ist erneut – mit dem vorhergehenden oder dem aktuell gültigen Bankschlüssel – einzureichen. Weitere Aufträge kann der EBICS-Kunde bzw. EBICS-Teilnehmer während des Übergangszeitraums mit dem vorhergehenden öffentlichen Bankschlüssel bzw. dem vorhergehenden Hashwert schicken; diese werden ohne weitere Fehlermeldung und ohne weiteren Eintrag in das Kundenprotokoll akzeptiert.

Im Anschluss werden EBICS-teilnehmerbezogene Berechtigungsprüfungen durchgeführt, wie etwa die Berechtigung für die BTF-Parameter. Die Ergebnisse weiterer bankfachlicher Prüfungen, wie beispielsweise Kontoberechtigungsprüfungen, werden dem Kunden im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt. Eine Doppeleinreichungsprüfung auf Basis des Hashwerts des eingereichten Auftrags durch die Deutsche Bundesbank findet nicht statt.

Auftragsdaten, die an das Banksystem übermittelt werden, können wie folgt autorisiert werden:

1. Alle erforderlichen bankfachlichen EU werden zusammen mit den Auftragsdaten übertragen.

2. Sofern mit dem Kunden für den jeweiligen BTF-Parameter die Verteilte Elektronische 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, längstens bis zur Löschung des Auftrags nach Abschnitt V Nummer 1 Absatz 2 der EBICS-Bedingungen, gespeichert.

5.1 Auftragserteilung mittels Verteilter Elektronischer Unterschrift (VEU)

Die Verteilte Elektronische Unterschrift (VEU) ist dann einzusetzen, wenn die Autorisierung von Aufträgen unabhängig vom Transport der Auftragsdaten und ggf. auch durch mehrere EBICS-Teilnehmer erfolgen soll.

Hinweis:

Zur Steuerung der Auftragserteilung mittels VEU wird im EBICS-System zur Kontoberechtigungsprüfung der Debtor bei SEPA-Überweisungen und der Creditor bei SEPA-Lastschriften und SCC-Karteneinzügen herangezogen und nicht wie in HBV-SEPA zur Bestimmung eines abweichenden Auftraggeberkontos (Belastungs-/Gutschriftskontos) der Ultimate Debtor oder der Ultimate Creditor.

Solange noch nicht alle zur Autorisierung erforderlichen bankfachlichen EU vorliegen, kann der Auftrag von einem hierzu berechtigten Nutzer gelöscht werden.

Die Deutsche Bundesbank löscht nicht vollständig autorisierte Aufträge automatisiert nach Ablauf des in Abschnitt V Nummer 1 Absatz 2 der EBICS-Bedingungen genannten Zeitlimits.

Es besteht die Möglichkeit, mit Transportunterschrift irrtümlicherweise Zahlungsverkehrsdateien einzureichen, für die keine Kontoberechtigung besteht. Im Kundenprotokoll findet sich in diesem Fall kein direkter Hinweis auf die fehlende Berechtigung. Dort wird lediglich vermerkt, dass für die fachliche Freigabe die Übermittlung der VEU aussteht, welche jedoch aufgrund einer fehlenden Kontoberechtigung gar nicht erteilt werden kann. Es ist in diesem Fall auch nicht möglich, den Status der Datei abzurufen. Nach Ablauf des Zeitlimits wird die Zahlungsverkehrsdatei automatisiert gelöscht.

5.2 Zulässige BTF-Parameter (BTF = Business Transaction Formats)

5.2.1 Einlieferung von Zahlungsaufträgen

Die Auftragserteilung erfolgt über BTF-Parameterwerte (Business Transactions & Formats). Ein BTF-Parameter setzt sich aus den folgenden Elementen zusammen:

<

Die im Geschäftsverkehr mit der Deutschen Bundesbank relevanten BTF-Parameter sind in der Anlage 2 aufgeführt.

Jedem BTF-Parameter ist genau ein Datenformat zugeordnet. Dabei muss in „multibankfähige“ BTF-Parameter und Datenformate gemäß Anlage 1 bzw. Anlage 3 des DFÜ-Abkommens und in institutsspezifische BTF-Parameter und Datenformate unterschieden werden. Multibankfähige Datenformate sind im deutschen Kreditgewerbe einheitlich spezifiziert. Institutsspezifische BTF-Parameter und Datenformate können nur im Datenaustausch mit der Deutschen Bundesbank verwendet werden und sind in den jeweiligen Verfahrensregeln der Deutschen Bundesbank festgelegt. Bei allen BTF-Parametern, die im Element <Service/Scope> die Angabe „BIL“ enthalten, handelt es sich um bundesbankeigene BTF-Parameter. Alle anderen BTF-Parameter sind multibankfähige BTF-Parameter. Dateien, deren Aufbau nicht den zu dem BTF-Parameter gehörenden Spezifikationen entspricht, werden von der Deutschen Bundesbank entweder direkt vom EBICS-Bankrechner zurückgewiesen (siehe Nummer 0) oder von der verarbeitenden Fachanwendung mittels einer Fehlernachricht zurückgewiesen (siehe Nummer 5.2.2).

5.2.2 Auslieferung von Zahlungsverkehrs- und Kontoinformationen

Alle Auslieferungsdaten werden gemäß EBICS-Standard zur Abholung bereitgestellt, das heißt nicht aktiv an den Empfänger verschickt. Liegen mehrere nicht abgeholte (logische) Dateien zu einem BTF-Parameter vor, so werden alle nicht abgeholten logischen Dateien für den Transfer zu einer physikalischen Datei zusammengefasst.

Die Deutsche Bundesbank bietet bei Aktualisierungen der Schemaversionen der Zahlungsverkehrsdateien durch die Deutsche Kreditwirtschaft regelmäßig für einen Übergangszeitraum einen Parallelbetrieb und somit die weitere Nutzung der Vorgängerversion an. Bei der Abholung von camt-Nachrichten können in einem Zip-Container Dateien sowohl mit der alten als auch mit der neuen Schemaversion enthalten sein, sofern camt-Nachrichten für mehrere Konten oder aus verschiedenen Zahlungsverkehrssystemen der Deutschen Bundesbank abholt werden und die Umstellung auf die neue Schemaversion für die Konten bzw. in den Zahlungsverkehrssystemen der Deutschen Bundesbank zu einem unterschiedlichen Zeitpunkt erfolgt.

Die für die Übertragung via EBICS relevanten Parameter und Informationen werden nicht im Dateinamen, sondern über den EBICS-XML-Umschlag übermittelt. Eine Auswertung des lokalen Dateinamens der Bereitstellungsdatei im Bankrechner der Deutschen Bundesbank wird für die weitere Verarbeitung in den Systemen des Kunden nicht empfohlen. Die Deutsche Bundesbank behält sich vor, unangekündigt Änderungen des lokalen Dateinamens durchzuführen.

Der Empfänger der Auslieferungsdateien muss selbst dafür sorgen, dass diese in angemessenen Abständen abgerufen werden. Die Zeitdauer von regelmäßigen Abfragezyklen sollte nicht

unter fünf Minuten liegen. Abfragen außerhalb der individuellen Geschäftszeiten des EBICS-Kunden sollten auf das tatsächlich notwendige Maß beschränkt werden.

Die gleichzeitige Abfrage bzw. der Abruf von mehreren BTF-Parametern sollte nach Möglichkeit mit der optionalen administrativen Auftragsart HAA (Abrufbare Auftragsarten abholen) erfolgen, um die Anzahl der Abfragen zu reduzieren. Nicht abgeholte Dateien werden 10 Geschäftstage zur Abholung auf dem EBICS-System bereitgehalten.

Die Deutsche Bundesbank unterstützt die in der Anlage 2 aufgeführten BTF-Parameter für die Auslieferung von Zahlungsverkehrsinformationen. Hierzu zählen Nachrichtendateien der Zahlungsverkehrsanwendungen sowie Umsatz- und Saldeninformationen der Kontoführung.

Die zur Abholung bereitgestellten Auslieferungsdaten können wie folgt durch einen oder mehrere EBICS-Teilnehmer des EBICS-Kunden abgeholt werden:

Über die zyklische Abholung müssen Zahlungsverkehrs- und Kontoinformationen **einmal ohne Vorgabe eines bestimmten Zeitraums** abgeholt werden. In diesem Fall werden die zur Abholung bereitgestellten Auslieferungsdaten vom EBICS-System der Deutschen Bundesbank technisch als „abgeholt“ gekennzeichnet und gelten infolgedessen für dieses als abgeholt. Eine erneute zyklische Abholung dieser Informationen ist systemseitig nicht mehr möglich.

Zusätzlich können über die historische Abholung Zahlungsverkehrs- und Kontoinformationen **mehrfach (ein- bis n-mal) mit Vorgabe eines bestimmten Zeitraums** ohne Auswirkungen auf die zyklische Abholung abgeholt werden.

Die historische Abholung hat keinerlei Auswirkungen auf den Abholstatus im EBICS-System der Deutschen Bundesbank. Folglich bleibt

- bei einer vor der zyklischen Abholung erfolgenden historischen Abholung der Abholstatus auf „nicht abgeholt“ und
- bei einer nach der zyklischen Abholung erfolgenden historischen Abholung der Abholstatus auf „abgeholt“.

5.3 Kundenprotokolle

Die Deutsche Bundesbank dokumentiert in Kundenprotokollen die folgenden Vorgänge:

- Übertragung der BTF-Parameter an das Banksystem (EBICS-Kommunikationsrechner)
- Abholung von Informationsdateien vom Banksystem durch das Kundensystem
- Ergebnis einer jeden Legitimationsprüfung von Aufträgen des Kunden an das Bank-system

- Weiterverarbeitung von Aufträgen, sofern sie die Unterschriftsprüfung und die Anzeige von Auftragsdaten betreffen
- Gültigkeitsdauer der genutzten Schemaversion einer eingereichten pain-Nachricht
- Prüfung der Hashwerte des öffentlichen bankfachlichen Schlüssels bei erstmaliger Verwendung eines vorhergehenden öffentlichen Bankschlüssels

Kundenprotokolle werden von der Deutschen Bundesbank 10 Kalendertage vorgehalten. Der EBICS-Teilnehmer hat sich durch Abruf des Kundenprotokolls über das Ergebnis der auf Seiten der Deutschen Bundesbank durchgeführten Prüfungen zu informieren.

Das Kundenprotokoll kann im XML-Format mit der administrativen Auftragsart HAC abgerufen werden.

Der Aufbau der Kundenprotokolle entspricht den Bestimmungen von Kapitel 10 der Spezifikation für die EBICS-Anbindung. Der EBICS-Teilnehmer hat das Protokoll zu seinen Unterlagen zu nehmen und auf Anforderung der Deutschen Bundesbank zur Verfügung zu stellen.

Die Dateianzeige (Anzeige der Dateiinhalte bei Uploadtransaktionen) für bundesbankspezifische BTF-Parameter ist für die administrative Auftragsart HAC in der Spezifikation für die EBICS-Anbindung nicht enthalten. Die Dateianzeige im Kundenprotokoll für bundesbankspezifische BTF-Parameter ist wie folgt aufgebaut:

5.3.1 Aufbau des Kundenprotokolls im XML-Format – HAC

5.3.1.1 Für die Einlieferung taggleicher Euro-Überweisungen (GT- oder DT-Datei):

Beschreibung	Feldname Auftragsdatei	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bank-Code (BLZ)	Leitzahl des Empfängers der Datei; BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei; Girokontonummer	A9
Auftraggeber	Bezeichnung des Absenders der Datei	A5
Erstellungsdatum	Datum der Dateierstellung	A6
Dateinummer	Eindeutige Nummer der Datei	A7
Anzahl der Zahlungssätze	Anzahl der Datensätze	E3
Summe der Beträge	Summe der Beträge in Euro	E9a

Tabelle 1: Aufbau Dateianzeige des Kundenprotokolls HAC für BBk-DTA/SWIFT-Format, EBCDIC/ungepackt

Beispiel:

…
<StsRsnInf>
<AddtlInf>Ueberweisungen Prior 1 Inland</AddtlInf>
<AddtlInf>Bank-Code :30000000</AddtlInf>
<AddtlInf>Kontonummer :30009999</AddtlInf>
<AddtlInf>Auftraggeber :Stadtkasse XYZ</AddtlInf>
<AddtlInf>Erstellungsdatum :05.09.16</AddtlInf>
<AddtlInf>Dateinummer :35357</AddtlInf>
<AddtlInf>Anzahl der Zahlungssaetze :1</AddtlInf>
<AddtlInf>Summe der Betraege :5000</AddtlInf>
</StsRsnInf>
…

5.3.1.2 Für die Einlieferung von AZV-Überweisungen (WT-Datei) :

Beschreibung	Feldname Auftragsdatei	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bank-Code (BLZ)	Leitzahl des Empfängers der Datei; Bei Einlieferungen BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei	A9
Auftraggeber	Bezeichnung des Absenders der Datei/Bankbezeichnung	A5
Erstellungsdatum	Datum der Dateierstellung	A6
Dateinummer	Eindeutige Nummer der Datei	A7
Anzahl der Zahlungssätze	Anzahl der Datensätze	E3
Summe der Beträge	Summe der Betragsfelder	E5

Tabelle 2: Aufbau Dateianzeige des Kundenprotokolls HAC für BBk-SWIFT-Format, EBCDIC/ungepackt

Beispiel:

…
<StsRsnInf>
<AddtlInf>AZV-Zahlung in Fremdwaehrung</AddtlInf>
<AddtlInf>Bank-Code :52000000</AddtlInf>
<AddtlInf>Kontonummer :52003999</AddtlInf>
<AddtlInf>Auftraggeber :Finanzamt ABC</AddtlInf>
<AddtlInf>Erstellungsdatum :05.09.16</AddtlInf>

<AddtlInf>Dateinummer :20160</AddtlInf>
<AddtlInf>Anzahl der Zahlungssaetze :7</AddtlInf>
<AddtlInf>Summe der Betraege :896679</AddtlInf>
</StsRsnInf>
…

5.3.1.3 Für die EBICS-interne Abbildung der im SRZ-Verfahren eingereichten SEPA-Zahlungen

Beispiel für Überweisungen:

…

<StsRsnInf>

<AddtlInf>Gutschriften </AddtlInf>

< AddtlInf>Datei-ID :CT-0094-KLT10041-000047K.xmlYXXXXX1 </AddtlInf>

< AddtlInf>Datum/ Zeit :21.11.2017/11:45:41.604Z </AddtlInf>

<AddtlInf>Initiator :Servicerechenzentrum</AddtlInf>

<AddtlInf>Initiator-ID :1234567890</AddtlInf>

<AddtlInf>Sammlerreferenz :MARKDEF1-30001500-160823:093310-001-</AddtlInf>

<AddtlInf>Bank-Code :MARKDEF1300</AddtlInf>

<AddtlInf>Kontonummer :DE05300000000030003999</AddtlInf>

<AddtlInf>Auftraggeberdaten : Finanzamt XYZ</AddtlInf>

<AddtlInf>Anzahl der Zahlungssaetze :3</AddtlInf>

<AddtlInf>Summe der Betraege :30,00</AddtlInf>

<AddtlInf>Ausfuehrungstermin :23.08.16</AddtlInf>

<AddtlInf>Hash-Wert :80 A9 E0 73 45 C1 00 54 F4 78 C9 4E E4 26 3F 7D 5A D4 D7 78 25 EB 04 6C 45 74 4D 6C CE 89 EB D0 </AddtlInf>

</StsRsnInf>

Beispiel für Lastschriften:

…

<StsRsnInf>

<AddtlInf>Lastschriften </AddtlInf>

< AddtlInf>Datei-ID :CT-0094-KLT10041-000047K.xmlYXXXXX1 </AddtlInf>

< AddtlInf>Datum/ Zeit :21.11.2017/11:45:41.604Z </AddtlInf>

<AddtlInf>Initiator :Servicerechenzentrum</AddtlInf>

<AddtlInf>Initiator-ID :1234567890</AddtlInf>

<AddtlInf>Sammlerreferenz :MARKDEF1-76001601-160823:093308-001</AddtlInf>

<AddtlInf>Bank-Code :MARKDEF1300</AddtlInf>

<AddtlInf>Kontonummer :DE05300000000030003999 </AddtlInf>
<AddtlInf>Auftraggeberdaten :Finanzamt XYZ</AddtlInf>
<AddtlInf>Anzahl der Zahlungssaetze :3</AddtlInf>
<AddtlInf>Summe der Betraege :30,00</AddtlInf>
<AddtlInf>Faelligkeitsdatum :23.08.16</AddtlInf>
<AddtlInf>Hash-Wert :80 A9 E0 73 45 C1 00 54 F4 78 C9 4E E4 26 3F 7D 5A D4 D7 78 25 EB 04 6C 45 74 4D 6C CE 89 EB D0 </AddtlInf>

</StsRsnInf>

5.4 Auftragsnummer

Gem. Spezifikation für die EBICS-Anbindung wird die Auftragsnummer durch den Bankserver zugewiesen.

Im Falle einer kundenseitigen Auftragsnummernvergabe wird immer die Fehlermeldung „EBICS_INCOMPATIBLE_ORDER_ATTRIBUTE“ erfolgen.

6 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom EBICS-Teilnehmer eingesetzten Legitimations- und Sicherungsmedien in ihrer Gültigkeit zeitlich begrenzt sind, hat der EBICS-Teilnehmer der Deutschen Bundesbank die neuen öffentlichen Teilnehmerschlüssel rechtzeitig vor dem Erreichen des Ablaufdatums zu übermitteln. Nach dem Erreichen des Ablaufdatums der alten Schlüssel ist eine Neuinitialisierung vorzunehmen.

Wenn der EBICS-Teilnehmer seine Schlüssel selbst generiert, so hat er die Teilnehmerschlüssel unter Verwendung der dafür vorgesehenen systembedingten Auftragsarten zu erneuern und rechtzeitig vor dem Erreichen des Ablaufdatums der alten Schlüssel zu übermitteln. Die Gültigkeitsdauer der Schlüssel richtet sich nach den Empfehlungen der Bundesnetzagentur sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die drei Schlüsselpaare der Deutschen Bundesbank werden grundsätzlich jedes Jahr ausgetauscht.

Für eine automatische Freischaltung der neuen Schlüssel ohne eine erneute Teilnehmerinitialisierung sind die folgenden administrativen Auftragsarten zu nutzen:

- Aktualisierung des öffentlichen bankfachlichen Schlüssels (PUB)
- Aktualisierung des öffentlichen Authentifikationsschlüssels und des öffentlichen Verschlüsselungsschlüssels (HCA)

Die administrativen Auftragsarten PUB und HCA sind hierfür mit einer gültigen bankfachlichen EU des Nutzers zu versehen. Nach erfolgreicher Änderung sind nur noch die neuen Schlüssel zu verwenden.

Wenn die Elektronische Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Abschnitt V Nummer 1 Absatz 2 der EBICS-Bedingungen verfahren.

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

7 Regelmäßige Änderung des öffentlichen Bankschlüssels

Die Deutsche Bundesbank generiert einmal jährlich einen neuen öffentlichen Bankschlüssel mit einer Länge von 2.048 Bit. Über den genauen Zeitpunkt der Bankschlüsseländerung und über die Hashwerte des neuen Bankschlüssels werden die EBICS-Kunden per E-Mail an die zu der EBICS-Kunden-ID gem. Vordruck 4760 „Antrag auf EBICS-Kommunikation sonstige Kontoinhaber ohne Bankleitzahl“ bzw. 4759 „EBICS Kommunikation sonstige Kontoinhaber ohne Bankleitzahl – Änderung der EBICS-Kontaktperson(en)“ hinterlegte funktionale E-Mail-Adresse informiert. Zusätzlich werden diese Informationen auf der Internetseite der Deutschen Bundesbank unter *www.bundesbank.de* > *Bundesbank* > *Organisation* > *AGB & Regelungen* zur Verfügung gestellt.

Gemäß Kapitel 4.6.2 der Anlage 1 der „Spezifikation für die EBICS-Anbindung“ werden auf Bankseite geänderte öffentliche Bankschlüssel sofort gültig. Dem EBICS-Kunden wird daher empfohlen, zeitnah die neuen Bankschlüssel mit der administrativen Auftragsart HPB abzuholen.

Bei stichtagsbezogener Einführung eines neuen öffentlichen Bankschlüssels wird der neue und der vorhergehende Bankschlüssel auf drei Monate befristet parallel unterstützt. Wegen der Besonderheit bei erstmaliger Einreichung einer Datei mit dem vorhergehenden Bankschlüssel (nach der Generierung des neuen Schlüssels) siehe Nummer 5.

8 Sperrung der Teilnehmerschlüssel

Soweit der EBICS-Teilnehmer über gültige Legitimations- und Sicherungsmedien verfügt, kann er seinen DFÜ-Zugang via EBICS sperren. Hierbei wird durch Senden einer Nachricht mit der administrativen Auftragsart "SPR" der Zugang für den jeweiligen EBICS-Teilnehmer, unter dessen User-ID die Nachricht gesendet wird, gesperrt. Nach einer Sperre können bis zu der unter Nummer 3 beschriebenen Neuinitialisierung keine Aufträge von diesem EBICS-Teilnehmer per EBICS-Anbindung mehr erteilt werden. Ansonsten ist eine Sperranzeige außerhalb des DFÜ-Verfahrens vom EBICS-Teilnehmer abzugeben.

Sperranzeigen sind gegenüber der Deutschen Bundesbank, Zentrale, Z 201-2 (Telefon: 069 9566 8868/ Telefax: 069 9566 508067), abzugeben. Telefonische Sperranzeigen sind unverzüglich per Telefax mit Unterschrift/en von zeichnungsberechtigten Personen zu bestätigen.

Der EBICS-Teilnehmer hat jeden Diebstahl oder Missbrauch seiner Legitimations- und Sicherungsmedien zudem unverzüglich bei der Polizei zur Anzeige zu bringen.

9 Testanforderungen

9.1 Grundsätzliches

Vor Verfahrensaufnahme ist durch einen erfolgreich absolvierten Zulassungs- und Conformancetest die Einhaltung der technischen Vorgaben und die Funktionalität des getesteten Produkts nachzuweisen. Die Eröffnung eines Testverfahrens über den Kommunikationskanal EBICS erfolgt über ein Online-Anmeldeformular auf der Internetseite der Deutschen Bundesbank unter „www.bundesbank.de > Aufgaben > *Unbarer Zahlungsverkehr* > *Serviceangebot* > *Kundentestzentrum*“.

Die Tests werden vom Kundentestzentrum koordiniert:

Deutsche Bundesbank
Kundentestzentrum Z 421
Postfach 10 11 48
40002 Düsseldorf
Telefon: +49 211 874-2343
E-Mail: testzentrum@bundesbank.de

Dem Kunden bietet sich bei diesem Test die Möglichkeit, die grundsätzlichen Verfahrensabläufe zu testen. Dies geschieht durch mehrere Einzeltests, die in Nummer 9.2 aufgeführt sind.

Es ist zu beachten, dass es sich bei den der Deutschen Bundesbank im Rahmen des Zulassungs- und Conformancetests übermittelten Testdaten um anonymisierte Echtdaten handeln soll, wobei der Einlieferer die Verantwortung für die Anonymisierung trägt. Bei ggf. anderen erforderlichen Tests können beliebige Testdaten eingereicht werden. Die Deutsche Bundesbank behält sich das Recht vor, eingereichte Testdaten z. B. für Tests mit der Empfängerbank einer Zahlung zu verwenden.

Änderungen am EBICS-Zugang (Hard- bzw. Software) oder Erweiterungen des Leistungsspektrums (z. B. Hinzunahme eines weiteren Dienstes) erfordern vor dem Produktionseinsatz einen erneuten Abnahmetest durch das Kundentestzentrum. Dafür ist frühzeitig ein Testverfahren mit dem Kundentestzentrum abzustimmen. Die formale Anmeldung erfolgt ebenfalls über das Online-Anmeldeformular auf der Internetseite der Deutschen Bundesbank (s. Absatz 1).

Für weiterführende Kundentests gelten die in den jeweiligen Verfahrensregeln dargestellten Regelungen.

Zum Kundenkreis des Testverfahrens gehören sowohl Neukunden als auch Kunden, die bereits produktiv Zahlungen einreichen und die aufgrund von Änderungen in der Infrastruktur einen neuen Test für erforderlich halten. Bereits produktiven EBICS-Teilnehmern wird vor erstmaliger

Nutzung einer neuen Auftragsart bzw. eines neuen Formats/Schemas diesbezüglich ein Testverfahren empfohlen. Näheres regelt der „Testleitfaden für sonstige Kontoinhaber ohne Bankleitzahl“. Dieser wird in Abhängigkeit von den empfohlenen Testaktivitäten auf der Internetseite der Deutschen Bundesbank unter „*www.bundesbank.de* > *Aufgaben* > *Unbarer Zahlungsverkehr* > *Veröffentlichungen*“ bereitgestellt. Tests mit dem Testzentrum der Deutschen Bundesbank ersetzen keinesfalls die Programmiertests und die Abnahme des Verfahrens, die im Rahmen der internen Qualitätssicherung durch den Kunden zu erfolgen haben.

Sofern ein Testverfahren aufgrund von Problemen auf Kundenseite nicht innerhalb eines halben Jahres nach der Eröffnung des Verfahrens abgeschlossen werden konnte, ist die Deutsche Bundesbank berechtigt, das Testverfahren (ohne Zulassung) zu beenden; der Kunde wird hierüber durch die Deutsche Bundesbank unter Rückgabe des Vordrucks 4760 „Antrag auf EBICS-Kommunikation sonstige Kontoinhaber ohne Bankleitzahl“ entsprechend informiert. Für eine Zulassung ist in diesem Fall zu gegebener Zeit der Vordruck 4760 neu einzureichen sowie das Testverfahren über das Online-Anmeldeformular auf der Internetseite der Deutschen Bundesbank neu zu beantragen.

9.2 Testszenarien

9.2.1 Initialisierung der EBICS-Anbindung

Testfall	Auftrag	Beschreibung
Test EBICS/I01	HIA	Senden des öffentlichen Authentifikationsschlüssels sowie des öffentlichen Verschlüsselungsschlüssels
Test EBICS/I02	INI	Senden des öffentlichen bankfachlichen Schlüssels
Test EBICS/I03	HPB	Abholen der öffentlichen Schlüssel der Bank

Tabelle 3: Test der Initialisierung der EBICS-Anbindung

9.2.2 Download Transaktionen

Testfall	Auftrag	Beschreibung
Test EBICS/D01	HAC	Abholung Kundenprotokolle im XML-Format nach Initialisierung

Tabelle 4: Test des Download von Transaktionen

9.2.3 Datenaustausch über die EBICS-Anbindung

Im Testschritt „Datenaustausch“ sind der erfolgreiche Datenaustausch über EBICS mit der bzw. den individuell beantragten Fachverfahren sowie der elektronische Abruf von Kontoinformationen zu testen.

Fachverfahren der Deutschen Bundesbank sind:

- Hausbankverfahren-SEPA (HBV-SEPA)
- Hausbankverfahren-Echtzeit (HBV-Echtzeit)
- Hausbankverfahren-Individual (HBV-Individual)
- Hausbankverfahren-IMPay (HBV-IMPay)

Basis für den Datenaustausch sind die unter Nummer 5.2.1 und 5.2.2 beschriebenen Datenformate. Die individuell notwendigen Test-Stammdaten werden vom Kundentestzentrum mit den EBICS-Testteilnehmern abgestimmt.

Nach Bedarf können Massentests mit dem Kundentestzentrum durchgeführt werden bei denen vom Kunden geeignete Testdaten mit einem Datenvolumen entsprechend des zu erwartenden Tagesspitzenwertes bereitzustellen sind.

DEUTSCHE BUNDESBANK
EUROSYSTEM

Anlage 1b
zu den

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)

(EBICS-Anbindung sonstige Kontoinhaber ohne BLZ)

Spezifikation für die EBICS-Anbindung, Version 2.5

Stand: 21. November 2021

DEUTSCHE BUNDESBANK EUROSYSTEM

EBICS-Anbindung sonstige Kontoinhaber ohne BLZ

Entspricht der zum November 2020 gültigen Anlage 1 der EBICS-Bedingungen auf Basis der EBICS-Spezifikation, Version 2.5. Die Anlage 1b entfällt zum November 2022.

DEUTSCHE BUNDESBANK
EUROSYSTEM

Anlage 2
zu den

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)

(BTF-Parameterwerte)

Stand: 21. November 2021

Verfahren		Geschäftsfall	*EBICS-Auftragsart Altformat*	Upload/ Down -load	Bank Transaction Format (BTF)				
					Service/ Name	Service/ Scope	Service/ Option	Service/ Msg Name	Container Typ (Container Flag)
HBV-Individual	**Einlieferung**	Einlieferung Taggleiche Euro-Überweisung, XML-Format (pain.001-Nachricht)	*CCU*	U	XCT	DE	URG	pain.001	
		Einlieferung Taggleiche Euro-Überweisung, GT-Datei	*XG2*	U	DCT	BIL	URG	gtbbksw	
		Einlieferung Taggleiche Euro-Überweisung, DT-Datei	*XDT*	U	XCT	BIL	URG	dtbbksw	
		Einlieferung AZV-Überweisung, WT-Datei	*XWT*	U	XCT	BIL	URG	wtbbksw	
		Einlieferung Taggleiche Euro-Überweisung sowie AZV-Überweisung, DTAZV-Format	*XDZ*	U	XCT	BIL	URG	dtazv	
	Bereitstellung	Information M3-Nachricht	*YM3*	D	REP	BIL	URG	m3bbksw	
		Information M6-Nachricht	*YM6*	D	OTH	BIL	URG	m6bbksw	
		Information M7-Nachricht	*YM7*	D	REP	BIL	URG	m7bbksw	
		Information M8-Nachricht	*YM8*	D	REP	BIL	URG	m8bbksw	
		Information M9-Nachricht	*YM9*	D	REP	BIL	URG	m9bbksw	
		Information über Nichtausführung einer Taggleichen Euro-Überweisung im XML-Format (pain.002-Nachricht)	*CRZ*	D	REP	DE	SCT	pain.002	ZIP
		Auslieferung camt-Datei (camt.054) zur Verfügungstellung von Zahlungsinformationen zu Taggleichen Euro-Überweisungen, die von sonstigen Kontoinhabern ohne BLZ im XML-Format (CCU) eingeliefert wurden und für andere sonstige Kontoinhaber ohne BLZ bei der Deutschen Bundesbank bestimmt sind	*C54*	D	STM	DE		camt.054	ZIP
		Auslieferung Inlands- und Inlandsanschlusszahlung, GT-Datei (BBk-SWIFT-Format)	*YG2*	D	DCT	BIL	URG	gtbbksw	
		Auslieferung Währungsabrechnungen, WA-Dateien	*YWA*	D	REP	BIL	URG	wabbksw	
HBV-IMPay	**Einlieferung**	Einlieferung grenzüberschreitender Euro-Massenzahlungen	*AZV*	U	XCT	DE		dtazv	
		Einlieferung von Rückforderungen für bereits ausgeführte Euro-Massenzahlungen, RF-Datei	*FTB*	U	OTH	BIL		rfbbkazv	
	Bereitstellung	Auslieferung RR-Nachricht	*FTB*	D	OTH	BIL		rfbbkazv	
		Information M3-Nachricht	*YM3*	D	REP	BIL	URG	m3bbksw	
		Information M7-Nachricht	*YM7*	D	REP	BIL	URG	m7bbksw	
		Information M8-Nachricht	*YM8*	D	REP	BIL	URG	m8bbksw	

Verfahren		Geschäftsfall	*EBICS-Auftragsart Altformat*	Upload/ Down -load	Bank Transaction Format (BTF)				
					Service/ Name	Service/ Scope	Service/ Option	Service/ Msg Name	Container Typ (Container Flag)
HBV-SEPA	**SEPA-Über-weisungen**	Einlieferung SEPA-Überweisung (pain.001-Nachricht)	*CCT*	U	SCT			pain.001	
		Einlieferung von elektronischen Widerrufen zu SEPA-Terminüberweisungen, SCT-Recalls und Requests for Recall by the Originator (camt.055-Nachricht)	*C55*	U	SCT	DE		camt.055	
		Information über Verarbeitungsergebnis zu mittels camt.055-Nachricht eingereichten Widerrufen zu SEPA-Terminüberweisungen, SCT-Recalls bzw. Requests for Recall by the Originator (camt.029-Nachricht)	*C29*	D	REP	DE		camt.029	ZIP
		Informations- oder Rückweisungsnachricht mittels Payment Status Report for Credit Transfer – Positiv- oder Negativmeldung (pain.002-Nachricht)	*CRZ*	D	REP	DE	SCT	pain.002	ZIP
	SEPA-Lastschriften	Einlieferung SEPA-Basislastschriften, CORE-Lastschrift (pain.008-Nachricht)	*CDD*	U	SDD		COR	pain.008	
		Einlieferung SEPA-Firmenlastschriften (pain.008-Nachricht)	*CDB*	U	SDD		B2B	pain.008	
		Informations- oder Rückweisungsnachricht mittels Payment Status Report for Direct Debit – Positiv- oder Negativmeldung (pain.002-Nachricht)	*CDZ*	D	REP	DE	SDD	pain.002	ZIP
	SCC-Karten-einzüge	Einlieferung SCC-Karteneinzüge (pain.008-Nachricht)	*CX8*	U	SCC	BGR		pain.008	
		Rückweisungsnachricht mittels Payment Status Report for Direct Debit – Negativmeldung (pain.002-Nachricht)	*CDZ*	D	REP	DE	SDD	pain.002	ZIP
	Bereitstellung - alle -	Auslieferung camt-Datei (camt.054-Nachricht)	*C54*	D	STM	DE		camt.054	ZIP
HBV-SEPA XML-Container	**SEPA-Über-weisungen**	Einlieferung von SEPA-Überweisungen in einem XML-Container (pain.001-Nachricht)	*CCC*	U	SCT	DE		pain.001	XML
	SEPA-Lastschriften	Einlieferung von SEPA-Basislastschriften (CORE-Lastschrift) in einem XML-Container (pain.008-Nachricht)	*CDC*	U	SDD	DE	COR	pain.008	XML
		Einlieferung von SEPA-Firmenlastschriften in einem XML-Container (pain.008-Nachricht)	*C2C*	U	SDD	DE	B2B	pain.008	XML

Verfahren		Geschäftsfall	*EBICS-Auftragsart Altformat*	Upload/ Down-load	Bank Transaction Format (BTF)				
					Service/ Name	Service/ Scope	Service/ Option	Service/ Msg Name	Container Typ (Container Flag)
HBV-Echtzeit	**Einlieferung**	Einlieferung SEPA-Echtzeitüberweisungen (pain.001-Nachricht)	*CIP*	U	SCI	DE		pain.001	
	Bereitstellung	Informations- oder Rückweisungsnachricht mittels Payment Status Report (pain.002-Nachricht)	*CIZ*	D	REP	DE	SCI	pain.002	ZIP
		Auslieferung camt-Datei (camt.054-Nachricht)	*C54*	D	STM	DE		camt.054	ZIP
		Auslieferung Customer Credit Notification (Haben-Avis) (camt.054-Nachricht)	*C5N*	D	STM	DE	SCI	camt.054	ZIP
Web-Socket	**Bereitstellung**	Abholung Daten WSS-Parameter (JASON)	*WSS*	D	OTH	DE		wssparam	
Elektronische Kontoinformation	**Abruf MT 940**	Auslieferung SWIFT-Tagesauszug MT 940	*STA*	D	EOP	DE		mt940	
	Abruf camt	Auslieferung Umsatz- und Saldeninformationen (camt.052-Nachricht)	*C52*	D	STM	DE		camt.052	ZIP
		Auslieferung Tagesauszug (camt.053-Nachricht)	*C53*	D	EOP	DE		camt.053	ZIP
SRZ-Verfahren	**SEPA-Überweisungen**	Senden von SEPA-Überweisungen in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	*CCS*	U	SCT	DE		pain.001	SVC
	SEPA-Lastschriften	Senden von SEPA-Basis-Lastschriften (CORE) in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	*CDS*	U	SDD	DE	COR	pain.008	SVC
		Senden von SEPA-Firmen-Lastschriften (B2B) in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	*C2S*	U	SDD	DE	B2B	pain.008	SVC
		Senden von vom Kunden pauschalautorisierten SEPA-Basis-Lastschriften (CORE) in einem Container durch SRZ	*XDS*	U	SDD	BIL	COR	pain.008	SVC
	SCC-Karteneinzüge	Senden von vom Kunden pauschalautorisierten SCC-Karteneinzügen in einem Container durch SRZ	*CK8*	U	SCC	BGR		pain.008	SVC
SRZ-Verfahren (bei Nutzung der VEU)	**SEPA-Überweisungen**	EBICS-interne Abbildung von über CCS im SRZ-Verfahren eingereichte SEPA-Überweisung bei Nutzung der Verteilten Elektronischen Unterschrift (VEU) (pain.001-Nachricht)	*CCX*		SCT	DE	0CCX	pain.001	
	SEPA-Lastschriften	EBICS-interne Abbildung von über CDS im SRZ-Verfahren eingereichte SEPA-Basislastschrift (CORE-Lastschrift) bei Nutzung der Verteilten Elektronischen Unterschrift (VEU) (pain.008-Nachricht)	*CDX*		SDD	DE	0CDX	pain.008	
		EBICS-interne Abbildung von über C2S im SRZ-Verfahren eingereichte SEPA-Firmenlastschrift bei Nutzung der Verteilten Elektronischen Unterschrift (VEU) (pain.008-Nachricht)	*C2X*		SDD	DE	0C2X	pain.008	

DEUTSCHE BUNDESBANK
EUROSYSTEM

Anlage 3
zu den

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)

(Sicherheitsanforderungen an das EBICS-Kundensystem)

Stand: 21. November 2021

DEUTSCHE BUNDESBANK EUROSYSTEM

Sicherheitsanforderungen an das EBICS-Kundensystem

Über die in den Anlagen 1a und 1b beschriebenen Sicherheitsmaßnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:

- Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in den Anlage 1a und 1b beschriebenen Anforderungen erfüllen. Die eingesetzte Software ist immer auf dem neuesten Stand zu halten.
- EBICS-Kundensysteme dürfen nicht ohne Firewall eingesetzt werden. Eine Firewall ist eine Einrichtung, die den gesamten ein- und ausgehenden Nachrichtenverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt.
- Es ist ein Virenscanner zu installieren, der regelmäßig mit den neuesten Virendefinitions-Dateien auszustatten ist.
- Das EBICS-Kundensystem ist so einzurichten, dass sich der EBICS-Teilnehmer vor dessen Nutzung anmelden muss. Die Anmeldung hat als normaler Benutzer und nicht als Administrator, der z. B. berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche Daten oder für unverschlüsselte EBICS-Nachrichten sind gegen Abhören und Manipulationen zu schützen.
- Wenn sicherheitsrelevante Updates für das jeweils eingesetzte Betriebssystem und weiterer installierter sicherheitsrelevanter Software-Programme vorliegen, sollten die eingesetzten EBICS-Kundensysteme mit diesen aktualisiert werden.
- Entsprechend einer Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[1] ist zu verwenden:
  a) ausschließlich die aktuelle Verschlüsselungsversion TLS 1.2 mit den im Rahmen von TLS 1.2 unterstützten und empfohlenen „Cipher-Suiten“,
  b) eine Schlüssellänge von mindestens 2048 Bit für RSA-Schlüssel im Rahmen der EBICS-Sicherheitsverfahren Elektronische Unterschrift (A006), Authentifikationssignatur (X002) und Verschlüsselung (E002)
  c) Version A006 für die Elektronische Unterschrift mit mindestens 2048 Bit Schlüssellänge (s. oben) für die Elektronische Unterschrift.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.

[1] BSI TR-02102-2 (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html)