Verfahrensregeln der Deutschen Bundesbank zur Kommunikation über EBICS mit Einlagenkreditinstituten und sonstigen Kontoinhabern mit Bankleitzahl

(Verfahrensregeln EBICS)

Stand: 19. November 2018

INHALTSVERZEICHNIS

REFERENZDOKUMENTE

	Dokument	Titel
1	Spezifikation für die EBICS-Anbindung	Anlage 1 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen
2	Implementation Guide EBICS	Implementation Guide EBICS, Ergänzung zum aktuellen DFÜ-Abkommen
3	AGB Deutsche Bundesbank	Allgemeine Geschäftsbedingungen der Deutschen Bundesbank
4	Verfahrensregeln SEPA Lastschrift	Verfahrensregeln der Deutschen Bundesbank für die Abwicklung von SEPA-Überweisungen über den SEPA-Clearer des EMZ
5	Verfahrensregeln SEPA Überweisung	Verfahrensregeln der Deutschen Bundesbank für die Abwicklung von SEPA-Lastschriften über den SEPA-Clearer des EMZ
6	Verfahrensregeln SCC-Karteneinzüge	Verfahrensregeln der Deutschen Bundesbank für die Abwicklung von SCC-Karteneinzügen über den SEPA-Clearer des EMZ
7	Verfahrensregeln Scheck	Verfahrensregeln der Deutschen Bundesbank für die Abwicklung von Scheckzahlungen über den EMZ
8	Verfahrensregeln HBV-Individual	Verfahrensregeln der Deutschen Bundesbank zur Abwicklung von taggleichen Zahlungen in Euro sowie von Zahlungen in ausländischen Währungen im Hausbankverfahren-Individual (HBV-Individual)
9	Verfahrensregeln elektronische Kontoinformationen	Verfahrensregeln der Deutschen Bundesbank zum Abruf von elektronischen Kontoinformationen

1 Verfahrensbeschreibung

Im unbaren Zahlungsverkehr unterscheidet die Deutsche Bundesbank zwischen Kreditinstituten i. S. d. Artikels 4 Absatz 1 der Verordnung 2013/575/EU (Einlagenkreditinstitute), für die die Bundesbank PM-, HAM- und Dotationskonten führt und die Teilnehmer an den Zahlungsverkehrssystemen der Deutschen Bundesbank sein können, sowie sonstigen Kontoinhabern. Der Begriff „sonstige Kontoinhaber“ umfasst Zahlungsdienstleister im Sinne des §1 Absatz 1 Nr. 1, 2, 4 und 5 ZAG (Zahlungsdiensteaufsichtsgesetz), Kreditinstitute mit Teilbanklizenz und öffentliche Verwaltungen.

Die Deutsche Bundesbank bietet mit dem **E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard (EBICS)-basierten Zugang für Einlagenkreditinstituten und sonstigen Kontoinhabern mit Bankleitzahl (im Folgenden: Zahlungsdienstleister) einen anerkannten Protokollen und Standards entsprechenden Kommunikationskanal an, der geeignet ist, den zwischenbetrieblichen Datenaustausch effizient, sicher und kostengünstig abzuwickeln.

Der Zugang beruht auf dem Kunde-Bank-Standard EBICS in der Version 2.5 (Schema H004).

Für die Abwicklung des Interbanken-Zahlungsverkehrs sind daher über das EBICS-Protokoll hinausgehende Festlegungen notwendig. Diese beziehen sich im Wesentlichen auf die Abweichungen vom EBICS-typischen Rollenverhalten von Kunde und Bank. Außerdem werden für die Kommunikation mit Zahlungsdienstleistern von der Deutschen Bundesbank Auftragsarten im EBICS-Standard spezifiziert, die den Transport der im Bank-Bank-Verhältnis üblichen Datenformate ermöglichen.

Die nachfolgenden Verfahrensregelungen definieren die für den zwischenbetrieblichen Datenaustausch notwendigen Ergänzungen des EBICS-Standards, Festlegungen für eine voll automatisierte Verarbeitung und das Dienstleistungsangebot der Deutschen Bundesbank über EBICS.

2 Geltung

Diese Verfahrensregeln gelten nur für die EBICS-Kommunikation zwischen der Deutschen Bundesbank und Zahlungsdienstleistern bzw. deren Servicerechenzentren. Für die EBICS-Kommunikation mit öffentlichen Verwaltungen und sonstigen Kontoinhabern finden die „Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)“ Anwendung.

Sie finden für folgende Fachverfahren der Deutschen Bundesbank sowie für den Abruf von elektronischen Kontoinformationen Anwendung:

- SEPA-Clearer des EMZ
- Scheckabwicklungsdienst des EMZ
- Hausbankverfahren-Individual (HBV-Individual)

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen der Deutschen Bundesbank.

3 Voraussetzungen zur Nutzung von EBICS

Das Kommunikationsverfahren EBICS können grundsätzlich alle Zahlungsdienstleister mit einem Konto bei der Deutschen Bundesbank nutzen. Nähere Hinweise ergeben sich aus den jeweiligen Verfahrensregeln der Fachverfahren. Die aktuellen Vordrucke können auf der Internetseite der Deutschen Bundesbank (www.bundesbank.de) unter Aufgaben / Unbarer Zahlungsverkehr / Serviceangebot / Vordrucke abgerufen werden. Sie sind jeweils bei dem zuständigen Kundenbetreuungsservice (KBS) der Deutschen Bundesbank einzureichen. Filialinstitute können die Kommunikation via EBICS bei dem für ihre Hauptniederlassung zuständigen Kundenbetreuungsservice beantragen. In diesem Fall sind die Anträge von Personen zu unterschreiben, die für das Gesamtinstitut vertretungsberechtigt sind.

Folgende Informationen sind vom Kontoinhaber für das EBICS-Banksystem des Zahlungsdienstleisters zur Verfügung zu stellen:

- Host-ID des EBICS-Banksystems
- EBICS URL oder IP des EBICS-Banksystems
- Vom Kontoinhaber unterschriebene Initialisierungsbriefe für die öffentlichen bankfachlichen Schlüssel (INI)
- Vom Kontoinhaber unterschriebene Initialisierungsbriefe für die öffentlichen Authentifikations- sowie Verschlüsselungsschlüssel (HIA)
- Informationen über das TLS-Serverzertifikat des EBICS-Banksystems
- Hashwerte der öffentlichen Schlüssel des EBICS-Banksystems

Der Zahlungsdienstleister erhält nach Eingang der Antragsunterlagen von der Deutschen Bundesbank die notwendigen Zugangsdaten für die Nutzung von EBICS. Er ist verpflichtet, die Deutsche Bundesbank gemäß der schriftlichen Vereinbarung in seinen Stammdaten einzurichten. Gleichzeitig wird der Zahlungsdienstleister auf dem EBICS-System der Deutschen Bundesbank eingerichtet.

Die für die Aktivierung der EBICS-Anbindung notwendigen Initialisierungsbriefe sind, sobald die systemseitigen Vorbereitungen abgeschlossen werden konnten, vom Kontoinhaber unterschrieben und zusammen mit den sonstigen zum Datenabgleich notwendigen Unterlagen (Informationen TLS-Serverzertifikat, Hashwerte öffentliche Schlüssel EBICS-Banksystems) bei dem zuständigen Kundenbetreuungsservice einzureichen, bei welcher der Antrag auf die Kommunikation via EBICS erfolgt bzw. erfolgte. Diese übermittelt die Unterlagen der zuständigen Stammdatenverwaltung. Bei der elektronischen Einreichung der Auftragsarten INI und HIA ist zu beachten, dass die Laufzeit dieser Aufträge auf 72 Stunden begrenzt ist. Wenn die Initialisierungsbriefe zum Ablaufzeitpunkt noch nicht bei der Stammdatenverwaltung der Deutschen Bundesbank vorliegen, muss die Einreichung wiederholt werden.

Im Falle der Nutzung eines Servicerechenzentrums als Kommunikationsstelle wird das Schlüsselmaterial zur Absicherung der EBICS-Transaktionen mit dem Servicerechenzentrum ausgetauscht. Dieses wird als berechtigter Kunde und Teilnehmer für die Konten der beauftragenden Zahlungsdienstleister in den Stammdaten des EBICS-Systems der Deutschen

Bundesbank hinterlegt. Das Servicerechenzentrum erhält für die EBICS-Kommunikation Kunden-ID und Teilnehmer-ID zur Einreichung von Zahlungen.

Die Kommunikation über EBICS erfolgt über ein offenes Netzwerk (Internet) unter Verwendung asymmetrischer kryptographischer Verfahren. Der Zahlungsdienstleister ist verpflichtet, seine DV-Anlagen gemäß den Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gegen Bedrohungen von außen und innen abzusichern. Außerdem sind die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz einzuhalten. Insbesondere die Behandlung der privaten kryptographischen Schlüssel hat mit besonderer Sorgfalt zu erfolgen.

4 Rollenverhalten

Das EBICS-Protokoll wurde für die Abwicklung des elektronischen Zahlungsverkehrs zwischen Kunde und Zahlungsdienstleister entwickelt. Es ist daher ein Client-Server-Protokoll, d. h. die Kommunikation geht immer vom Client aus. Dem entsprechend liegt dem EBICS-Protokoll ein Rollenverhalten zu Grunde, bei dem der Zahlungsdienstleister stets die passive Rolle einnimmt, d. h. Auslieferungsdaten werden ausschließlich zur Abholung bereitgestellt.

Für die Abwicklung des zwischenbetrieblichen Zahlungsverkehrs ist dieses Rollenverhalten nicht anwendbar. Der Datenaustausch im Interbankenzahlungsverkehr geht von einer gleichberechtigten Rolle der Kommunikationspartner aus (Peer-to-Peer-Kommunikation). Im Rahmen der Kommunikation zwischen der Deutschen Bundesbank und einem Zahlungsdienstleister nimmt immer der sendende Kommunikationspartner die aktive Rolle des Clients ein. Dies bedeutet, dass die Einlieferung von Daten an die Deutsche Bundesbank stets aktiv vom Zahlungsdienstleister an die Deutsche Bundesbank erfolgt.

Im Gegenzug werden alle Auslieferungsdaten von der Deutschen Bundesbank aktiv an den Zahlungsdienstleister versendet. In der Terminologie des DFÜ-Abkommens verhält sich die Deutsche Bundesbank bei Einlieferungen durch Zahlungsdienstleister wie ein Banksystem. Im Rahmen von Auslieferungen agiert die Deutsche Bundesbank grundsätzlich als Kundensystem. Das Rollenverhalten ändert sich somit in Abhängigkeit von der Senderichtung. Wie dieses Rollenverhalten auf Seiten des Zahlungsdienstleisters abgebildet wird, ist Gegenstand der Umsetzung durch den Zahlungsdienstleister. Ein Kommunikationssystem, das dieses Rollenverhalten abbildet, wird im Folgenden als EBICS-System bezeichnet.

Zu dem Grundprinzip, dass Daten stets aktiv versendet werden, bestehen zwei wesentliche Ausnahmen:

a) Im Rahmen der Teilnehmerinitialisierung werden EBICS-Mechanismen genutzt, so dass die öffentlichen Schlüssel des Banksystems „zur Abholung bereitgestellt“ werden. Ein aktiver Versand ist nicht vorgesehen.

b) „Kundenprotokolle“ werden von der Deutschen Bundesbank nicht aktiv an den Empfänger versendet, sondern müssen nach Erstellung durch das EBICS-System der Deutschen Bundesbank vom Einreicher des Auftrags, auf den sich das Kundenproto-

koll bezieht, abgeholt werden. Für Auslieferungen erwartet die Deutsche Bundesbank analog die Bereitstellung eines Kundenprotokolls durch den Empfänger, das von ihr im Rahmen der Versandkontrolle periodisch abgeholt wird.

Im Verhältnis zwischen einem Zahlungsdienstleister und der Deutschen Bundesbank kommt dem Kundenprotokoll die Rolle der Protokollierung von Ereignissen zu, die vor der Verarbeitung in den Fachanwendungen auftreten. Im Einzelnen werden analog dem DFÜ-Abkommen folgende Ereignisse protokolliert:

- Die Übertragung der Auftragsart an die Deutsche Bundesbank.
- Das Ergebnis der EU-Verifikation und Dekomprimierung.
- Die Weiterleitung zur Verarbeitung in der Fachanwendung, sofern die Prüfungen auf EBICS-Ebene erfolgreich waren - anderenfalls der aufgetretene Fehlercode.
- Prüfung der Hashwerte des öffentlichen bankfachlichen Schlüssels bei erstmaliger Verwendung eines vorhergehenden öffentlichen Bankschlüssels

Der einreichende Zahlungsdienstleister kann erst dann von einer erfolgreichen Übertragung der eingereichten Dateien an die Fachanwendungen der Deutschen Bundesbank ausgehen, wenn es über das Kundenprotokoll die erfolgreiche Einlieferung und Unterschriftenprüfung angezeigt bekommt. Der Zahlungsdienstleister muss daher das Kundenprotokoll abholen, um sich zeitnah über die erfolgreiche Einlieferung von Daten oder ggf. vor der Verarbeitung in den Fachanwendungen aufgetretene Fehler zu informieren und im Bedarfsfall Gegenmaßnahmen einleiten zu können.

Nachrichtendateien:

Einreicher werden von der Deutschen Bundesbank über fachliche Verarbeitungsfehler/Prüfungen bzw. verarbeitete Zahlungen in den Fachanwendungen informiert.

- Für die Abwicklung von SEPA-Zahlungen mit dem SEPA-Clearer mit dem Nachrichtentyp pacs.002SCL. Zusätzlich erhält jeder Teilnehmer zum Abschluss eines Geschäftstages im SEPA-Clearer für jeden Dienst getrennt eine Abstimmungsdatei (Daily Reconciliation Report for Credit Transfers [DRC] für SEPA-Überweisungen bzw. Daily Reconciliation Report for Direct Debits [DRD] getrennt für SEPA-Core- und SEPA-B2B-Lastschriften bzw. Daily Reconciliation Report for SEPA Card Clearing Collections [DRR SCC] für SCC-Karteneinzüge). Der Report ist eine geschäftsfallabhängige Zusammenstellung der geschäftstäglich eingereichten und ausgelieferten Bulks im SEPA-Clearer.
- Für Aufträge an das HBV-Individual sind dies M-Nachrichten. Die Nachrichtendatei M3 „Mitteilung über eine nicht verarbeitungsfähige Datei“, die Nachrichtendatei M7 „Mitteilung über nicht ausgeführte bzw. annullierte Zahlungen“ und die Nachrichtendatei M8 „Mitteilung über nicht verarbeitbare Datensätze“. Zusätzlich wird eine Nachrichtendatei M9 „Mitteilung über verarbeitete und ausgelieferte Dateien“ erstellt.
- Für Umsatzanfragen im Rahmen des Abrufs von elektronischen Kontoinformationen ist dies eine Nachrichtendatei M3 „Mitteilung über eine nicht bearbeitungsfähige oder doppelt eingereichte Anforderungsdatei“.

- Für Aufträge an den Scheckabwicklungsdienst des EMZ der Deutschen Bundesbank sind dies Nachrichten mit dem Typ pacs.002SVV. Zusätzlich erhält jeder Teilnehmer zum Abschluss eines Geschäftstages für jeden Dienst getrennt eine Abstimmungsdatei (Daily Reconciliation Report for SVV BSE [DRD BSE] für BSE-Schecks, Daily Reconciliation Report for SVV ISE [DRD ISE] für ISE-Schecks und Daily Reconciliation Report for ISR [DRD ISR] für ISE Rückschecks). Der Report ist eine geschäftsfallabhängige Zusammenstellung der geschäftstäglich eingereichten und ausgelieferten Bulks in den Scheckabwicklungsdienst des EMZ der Deutschen Bundesbank.

Servicerechenzentren:

Im Fall der Nutzung eines Servicerechenzentrums wird das Schlüsselmaterial zur Absicherung der EBICS-Transaktionen mit diesem ausgetauscht (siehe auch Ziffer 3). Das Servicerechenzentrum tritt als berechtigter Kunde und Teilnehmer für die Konten der beauftragenden Zahlungsdienstleister auf. Es erhält für die EBICS-Kommunikation Kunden-ID und Teilnehmer-ID zur Einreichung von Zahlungen. Geprüft werden die Signaturen des Servicerechenzentrums. Das Servicerechenzentrum ist aufgrund dieser Berechtigungen ein vollwertiger EBICS-Teilnehmer und nicht nur ein technischer Teilnehmer gemäß der EBICS Terminologie (vergleiche hierzu „Spezifikation für die EBICS-Anbindung“, Tz 3.7, Technische Teilnehmer).

Im SEPA-Clearer des EMZ und im Scheckabwicklungsdienst des EMZ wird der 11-stelllige BIC im XML-File-Header (Feld „Sending Institution“) der eingereichten Datei zur Kontoberechtigungsprüfung herangezogen. Im Falle der Einreichung über ein Servicerechenzentrum ist dies der (technische) BIC des Servicerechenzentrums, bei direkter Einreichung des Zahlungsdienstleisters für seine Konten der BIC des Kontoinhabers. Für alle anderen Einreichungen wird die Bankleitzahl bzw. die bankleitzahlfreie Girokontonummer des Zahlungsdienstleisters im A-Satz der Dateien zur Berechtigungsprüfung herangezogen.

5 Detaillierte Verfahrensbeschreibung

5.1 Sicherungsverfahren

5.1.1 Grundsätzliche Festlegungen

Für die Absicherung der Transaktionen über EBICS werden die im EBICS-Protokoll vorgesehenen Sicherungsverfahren genutzt. Analog den Vorgaben des DFÜ-Abkommens sind für jeden Teilnehmer drei RSA-Schlüsselpaare vorgesehen:

- Öffentliche / private bankfachliche Schlüssel
- Öffentliche / private Authentifikationsschlüssel
- Öffentliche / private Verschlüsselungsschlüssel

Für die bankfachliche Signatur der Aufträge wird exklusiv ein Schlüsselpaar verwendet. Für die Authentifikation des Teilnehmers gegenüber dem Banksystem und die Entschlüsselung von Transaktionsschlüsseln kann ein einziges Schlüsselpaar verwendet werden. Die Deut-

sche Bundesbank verwendet für die Authentifikationsschlüssel und die Verschlüsselungsschlüssel das gleiche physische Schlüsselpaar. Dabei kommen für die Einlieferung bei der Deutschen Bundesbank und für die Auslieferung durch die Deutsche Bundesbank unterschiedliche Schlüsselpaare zum Einsatz.

Sämtliche aktiven Sendeaufträge sind mit einer elektronischen Signatur gesichert. Dies gilt für Einlieferungen bei der Deutschen Bundesbank ebenso wie für Auslieferungen durch die Deutsche Bundesbank an Zahlungsdienstleister. Im Rahmen des Datenaustausches mit Zahlungsdienstleistern werden keine Begleitzettel zur Autorisierung von Transaktionen zugelassen, das Auftragsattribut „DZHNN“ ist für Sendeaufträge nicht zulässig.

Die erfolgreiche Verifikation der elektronischen Signatur eines Zahlungsdienstleisters berechtigt die Deutsche Bundesbank zur Weitergabe der Daten an die Fachanwendung zur Verarbeitung. Auslieferungsdaten der Deutschen Bundesbank sind ebenfalls mit einer elektronischen Signatur gesichert und sollten nur nach erfolgreicher EU-Verifikation verarbeitet werden. Die elektronische Signatur entspricht einer bankfachlichen EU der Klasse E des DFÜ-Abkommens.

Eine Ausnahme zur Sicherung aller Daten mit elektronischer Signatur stellen Download-Transaktionen dar. Bis zur Umsetzung der elektronischen Unterschrift des Zahlungsdienstleisters im DFÜ-Abkommen dürfen Abholdaten mit dem Auftragsattribut „DZHNN“ angefordert werden. Nach Umsetzung der EU im Bank-Kunde-Verhältnis wird für die Kommunikation mit der Deutschen Bundesbank nur noch das Auftragsattribut „OZHNN“ möglich sein.

Es sind die Sicherungsverfahren der EBICS-Version 2.5 zulässig:

- Authentifikationssignatur gem. „X002“
- Verschlüsselung gem. „E002“
- Elektronische Unterschrift gem. A006

Die Verteilte Elektronische Unterschrift und X.509-Zertifikate werden gegenwärtig nicht unterstützt.

Die Gültigkeitsdauer der verwendeten Schlüssel richtet sich nach den Empfehlungen der Bundesnetzagentur sowie des BSI.

5.1.2 Übersicht der verwendeten Schlüssel

Die Verwendung der EBICS-Sicherheitsverfahren in der Kommunikation zwischen der Deutschen Bundesbank und den Zahlungsdienstleistern bedingt, dass je nach Rolle und Kommunikationsrichtung unterschiedliche „logische“ Schlüssel bzw. Schlüsselpaare für die unterschiedlichen Sicherheitsverfahren zum Einsatz kommen.

„Logisch“ bedeutet in diesem Zusammenhang die Verwendung separater Schlüssel je nach Art der Kommunikationsbeziehung und Art der Implementierung des EBICS-Systems (separates Client- und Serversystem, kombiniertes Client- und Serversystem).

Physikalisch können mehrere „logische“ Schlüssel identisch sein (siehe Ziffer 5.1.1).

Die folgende Aufstellung dient allein dem Zweck, darzustellen, welche Schlüssel in der Kommunikation zwischen Deutsche Bundesbank und Zahlungsdienstleistern zum Einsatz kommen können:

BACp =	Bundesbank-Authentifikationsschlüssel Client Public-Key
BACs =	Bundesbank-Authentifikationsschlüssel Client Secret-Key
BASp =	Bundesbank-Authentifikationsschlüssel Server Public-Key
BASs =	Bundesbank-Authentifikationsschlüssel Server Secret-Key
BECp =	Bundesbank-EU-Schlüssel Client Public-Key
BECs =	Bundesbank-EU-Schlüssel Client Secret-Key
BESp =	Bundesbank-EU-Schlüssel Server Public-Key (z. Zt. in EBICS nicht definiert)
BESs =	Bundesbank-EU-Schlüssel Server Secret-Key (z. Zt. in EBICS nicht definiert)
BVCp =	Bundesbank-Verschlüsselungsschlüssel Client Public-Key
BVCs =	Bundesbank-Verschlüsselungsschlüssel Client Secret-Key
BVSp =	Bundesbank-Verschlüsselungsschlüssel Server Public-Key
BVSs =	Bundesbank-Verschlüsselungsschlüssel Server Secret-Key
KACp =	Zahlungsdienstleister-Authentifikationsschlüssel Client Public-Key
KACs =	Zahlungsdienstleister-Authentifikationsschlüssel Client Secret-Key
KAp =	Zahlungsdienstleister-Authentifikationsschlüssel Public-Key
KAs =	Zahlungsdienstleister-Authentifikationsschlüssel Secret-Key
KASp =	Zahlungsdienstleister-Authentifikationsschlüssel Server Public-Key
KASs =	Zahlungsdienstleister-Authentifikationsschlüssel Server Secret-Key
KECp =	Zahlungsdienstleister-EU-Schlüssel Client Public-Key
KECs =	Zahlungsdienstleister-EU-Schlüssel Client Secret-Key
KEp =	Zahlungsdienstleister-EU-Schlüssel Public-Key
KEs =	Zahlungsdienstleister-EU-Schlüssel Secret-Key
KESp	Zahlungsdienstleister-EU-Schlüssel Server Public-Key (z. Zt. in EBICS nicht definiert)
KESs =	Zahlungsdienstleister-EU-Schlüssel Server Secret-Key (z. Zt. in EBICS nicht definiert)
KVCp =	Zahlungsdienstleister-Verschlüsselungsschlüssel Client Public-Key
KVCs =	Zahlungsdienstleister-Verschlüsselungsschlüssel Client Secret-Key
KVp =	Zahlungsdienstleister-Verschlüsselungsschlüssel Public-Key
KVs =	Zahlungsdienstleister-Verschlüsselungsschlüssel Secret-Key
KVSp =	Zahlungsdienstleister-Verschlüsselungsschlüssel Server Public-Key
KVSs =	Zahlungsdienstleister-Verschlüsselungsschlüssel Sever Secret-Key

Tabelle 1: Gesamtübersicht Schlüssel

Die hier verwendeten Abkürzungen für die Schlüssel werden nur in diesem Dokument verwendet und entsprechen nicht den in der EBICS-Spezifikation verwendeten Begriffen.

Es werden zwei unterschiedliche Szenarien betrachtet:

1. Der Zahlungsdienstleister verwendet jeweils separate Schlüssel für Client und Server.
2. Der Zahlungsdienstleister verwendet jeweils gemeinsame Schlüssel für Client und Server.

5.1.2.1 Verwendung separater Client- und Serverschlüssel durch den Zahlungsdienstleister

Folgende Schlüssel werden verwendet:

	Deutsche Bundesbank		Zahlungsdienstleister	
	Client	Server	Client	Server
Authentifikation	BACs BACp	BASs BASp	KACs KACp	KASs KASp
Verschlüsselung	BVCs BVCp	BVSs BVSp	KVCs KVCp	KVSs KVSp
EU	BECs BECp	(BESs)[1] (BESp)[1]	KECs KECp	(KESs)[1] (KESp)[1]

Tabelle 2: Einsatz separater Schlüssel

Diese kommen in Abhängigkeit von der Senderichtung bzw. Art der Übertragung (Upload-/ Download-Transaktion) zum Einsatz (siehe Ziffer 5.2)

Der Zahlungsdienstleister besitzt folgende geheime Schlüssel:

KACs = Zahlungsdienstleister -Authentifikationsschlüssel Client
KASs = Zahlungsdienstleister -Authentifikationsschlüssel Server
KVCs = Zahlungsdienstleister -Verschlüsselungsschlüssel Client
KVSs = Zahlungsdienstleister -Verschlüsselungsschlüssel Server
KECs = Zahlungsdienstleister -EU-Schlüssel Client

Es handelt sich hier um logische Schlüssel, die in einer jeweiligen Rolle eingesetzt werden. Physikalisch können KACs, KASs, KVCs und KVSs identisch sein, so dass statt 5 nur 3 Secret-Keys Verwendung finden bzw. gesichert gespeichert sind. Auf Seiten der Bundesbank werden für BVCs/BACs und BASs/BVSs physikalisch identische Schlüssel verwendet. Die geheimen Schlüssel BESs und KESs sind in EBICS nur vorgesehen und werden in der Kommunikation mit der Deutschen Bundesbank derzeit nicht verwendet.

Die Deutsche Bundesbank verwaltet folgende öffentliche Schlüssel des Zahlungsdienstleisters:

KACp = Zahlungsdienstleister -Authentifikationsschlüssel Client
KASp = Zahlungsdienstleister -Authentifikationsschlüssel Server
KVCp = Zahlungsdienstleister -Verschlüsselungsschlüssel Client
KVSp = Zahlungsdienstleister -Verschlüsselungsschlüssel Server
KECp = Zahlungsdienstleister -EU-Schlüssel Client

Es handelt sich hier um logische Schlüssel. Die Anzahl der physikalischen Schlüssel hängt von der Implementierung beim Zahlungsdienstleister ab. Es kann sein, dass ein Zahlungsdienstleister einen physikalischen Schlüssel für mehrere logische Schlüssel verwendet (z. B. KACp, KASp, KVCp und KVSp könnten physikalisch identisch sein). Auf Seiten der Deutschen Bundesbank werden für BVCp/BACp und BASp/BVSp physikalisch identische Schlüs-

[1] In EBICS derzeit nur vorgesehen

sel verwendet. Die öffentlichen Schlüssel BESp und KESp sind in EBICS nur vorgesehen und werden in der Kommunikation mit der Deutschen Bundesbank derzeit nicht verwendet.

5.1.2.2 Verwendung gemeinsamer Client- und Serverschlüssel durch den Zahlungsdienstleister

Folgende Schlüssel werden verwendet:

	Deutsche Bundesbank		**Zahlungsdienstleister**
	Client	Server	
Authentifikation	BACs BACp	BASs BASp	KAs KAp
Verschlüsselung	BVCs BVCp	BVSs BVSp	KVs KVp
EU	BECs BECp	(BESs)[1] (BESp)[1]	KEs KEp

Tabelle 3: Einsatz gemeinsamer Schlüssel

Diese kommen in Abhängigkeit von der Senderichtung bzw. Art der Übertragung (Upload-/ Download-Transaktion) zum Einsatz (siehe Ziffer 5.2).

Der Zahlungsdienstleister besitzt folgende geheime Schlüssel:

KAs = Zahlungsdienstleister -Authentifikationsschlüssel
KVs = Zahlungsdienstleister -Verschlüsselungsschlüssel
KEs = Zahlungsdienstleister -EU-Schlüssel

Es handelt sich hier um logische Schlüssel, die in einer jeweiligen Rolle eingesetzt werden. Physikalisch können KAs und KVs identisch sein, so dass statt 3 nur 2 Secret-Keys Verwendung finden bzw. gesichert gespeichert sind. Auf Seiten der Bundesbank werden für BVCs/BACs und BASs/BVSs physikalisch identische Schlüssel verwendet. Der geheime Schlüssel BESs ist in EBICS nur vorgesehen und wird in der Kommunikation mit der Deutschen Bundesbank derzeit nicht verwendet.

Die Deutsche Bundesbank verwaltet folgende öffentliche Schlüssel des Zahlungsdienstleisters:

KAp = Zahlungsdienstleister -Authentifikationsschlüssel
KVp = Zahlungsdienstleister -Verschlüsselungsschlüssel
KEp = Zahlungsdienstleister -EU-Schlüssel

Es handelt sich hier um logische Schlüssel. Die Anzahl der physikalischen Schlüssel hängt von der Implementierung beim Zahlungsdienstleister ab. Es kann sein, dass ein Zahlungsdienstleister einen physikalischen Schlüssel für mehrere logische Schlüssel verwendet (KAp und KVp könnten physikalisch identisch sein). Auf Seiten der Deutschen Bundesbank werden für BVCp/BACp und BASp/BVSp physikalisch identische Schlüssel verwendet. Der öffentliche Schlüssel BESp ist in EBICS nur vorgesehen und wird in der Kommunikation mit der Deutschen Bundesbank derzeit nicht verwendet.

5.1.3 Schlüsselmanagement

5.1.3.1 Initialisierung

Der Zahlungsdienstleister hat sich nach Erhalt der Bankparameter der Deutschen Bundesbank auf dem EBICS-System der Deutschen Bundesbank zu initialisieren. Die Initialisierung erfolgt mit den Auftragsarten „INI“ und „HIA“ nach den Vorgaben des DFÜ-Abkommens.

Die Deutsche Bundesbank setzt den Status der übertragenen Schlüssel des Zahlungsdienstleisters nach positivem Abgleich mit den im Zulassungsantrag gelieferten Hashwerten auf „freigeschaltet“. Der Zahlungsdienstleister holt sich die öffentlichen Schlüssel der Deutschen Bundesbank mit der Auftragsart „HPB“ ab. Die öffentlichen Schlüssel der Deutschen Bundesbank sind nach positivem Abgleich mit den von der Deutschen Bundesbank über einen separaten Kanal veröffentlichten Hashwerten durch den Zahlungsdienstleister freizuschalten. Die aktuell gültigen Hashwerte für die Einlieferung werden dem Zahlungsdienstleister mit den Bankparametern mitgeteilt.

Mit der Auftragsart „HPB“ werden die öffentlichen Schlüssel der Deutschen Bundesbank für die Verschlüsselung und die Authentifikationssignatur ausgeliefert, der Signaturschlüssel wird bis zur Einführung der EU für Zahlungsdienstleister im DFÜ-Abkommen nicht bereitgestellt. Nach Abschluss dieses Teilschritts ist der Zahlungsdienstleister in der Lage Sendeaufträge an die Deutsche Bundesbank zu übertragen.

Für die Auslieferung von Daten durch die Deutsche Bundesbank an einen Zahlungsdienstleister initialisiert sich die Deutsche Bundesbank auf dem EBICS-System des Zahlungsdienstleisters. Dies erfolgt analog der Initialisierung des Zahlungsdienstleisters auf dem EBICS-System der Deutsche Bundesbank mit den Auftragsarten „INI“ und „HIA“. Die Deutsche Bundesbank benötigt hierzu die Bankparameter des Zahlungsdienstleisters, die mit dem Zulassungsantrag eingereicht werden. Die Hashwerte der von der Deutschen Bundesbank für die Auslieferung verwendeten Schlüssel werden dem Zahlungsdienstleister per Initialisierungsbrief zugestellt. Die Werte der mit EBICS übertragenen Schlüssel sind durch den Zahlungsdienstleister mit Werten der Initialisierungsbriefe abzugleichen. Nach einem positiven Abgleich sind diese Schlüssel freizuschalten. Die Deutsche Bundesbank holt sich die öffentlichen Schlüssel des Zahlungsdienstleisters mit der Auftragsart „HPB“ ab und schaltet diese nach Abgleich mit den vom Zahlungsdienstleister separat bekannt gemachten Hashwerten frei.

5.1.3.2 Schlüsselaustausch

Die Schlüssel der Deutschen Bundesbank haben eine definierte Gültigkeitsdauer; die Deutsche Bundesbank generiert einmal jährlich einen neuen öffentlichen Schlüssel. Über den genauen Zeitpunkt der Schlüsseländerung sowie über die neuen Hashwerte werden die Zahlungsdienstleister per E-Mail an die zu der EBICS-Kunden-ID gemäß Vordruck 4750 „Antrag auf EBICS-Kommunikation“ hinterlegte funktionale E-Mail-Adresse informiert. Zusätzlich werden diese Informationen auf der Internetseite der Deutschen Bundesbank unter www.bundesbank.de > Aufgaben > Unbarer Zahlungsverkehr > Veröffentlichungen > Verfah-

rensregeln zur Verfügung gestellt. Der Zahlungsdienstleister ist verpflichtet, die neuen öffentlichen Schlüssel für die Einlieferung mit der Auftragsart „HPB“ abzuholen und freizuschalten.

Bei stichtagsbezogener Einführung eines neuen öffentlichen Schlüssels wird der neue und der vorhergehende Schlüssel auf drei Monate befristet parallel unterstützt. Wegen der Besonderheit bei erstmaliger Einreichung einer Datei mit dem vorhergehenden Schlüssel (nach der Generierung eines neuen Schlüssels) siehe auch Ziffer 5.2.3.1.

Die Aktualisierung der öffentlichen Schlüssel auf dem EBICS-System des Zahlungsdienstleisters für die Auslieferung nimmt die Deutsche Bundesbank selbst mit den Auftragsarten „PUB“ und „HCA“ vor.

Die Deutsche Bundesbank ist vor dem Austausch der Schlüssel durch den Zahlungsdienstleister rechtzeitig zu informieren. Der Zahlungsdienstleister muss die Schlüssel für die Einlieferung selbst mittels der Auftragsarten „PUB“ und „HCA“ auf dem EBICS-System der Deutschen Bundesbank aktualisieren. Für die Auslieferung sind der Deutschen Bundesbank die Hashwerte der neuen Schlüssel zuzusenden. Die Aktualisierung der Schlüssel erfolgt in diesem Fall durch die Deutschen Bundesbank mit der Auftragsart „HPB“ und anschließender Freischaltung der neuen Schlüssel nach positivem Abgleich mit den neuen Hashwerten.

5.1.3.3 Sperre

Die Kompromittierung von aktiven Schlüsseln des Zahlungsdienstleisters ist der Deutschen Bundesbank unverzüglich mitzuteilen. Gleichzeitig ist eine Sperre der betroffenen Schlüssel vorzunehmen. Die Sperre kann auf zwei unterschiedlichen Wegen erfolgen:

- Schriftliche Anweisung an die Deutsche Bundesbank, Zentrale, Z 201-2 (Telefaxnummer: +49 69 9566-50 8067) die betroffenen öffentlichen Schlüssel zu sperren. Die Anweisung ist von vertretungs- oder zeichnungsberechtigten Personen zu unterzeichnen.
- Sperrung der Schlüssel durch die Auftragsart „SPR“ auf dem EBICS-System der Deutschen Bundesbank

Die Sperrung mit „SPR“ bewirkt unmittelbar, dass alle mit den gesperrten Schlüsseln gesicherten Einlieferungen zurückgewiesen werden. Zusätzlich sind die betroffenen öffentlichen Schlüssel auf dem EBICS-System des Zahlungsdienstleisters zu sperren, so dass keine Auslieferungen mit den kompromittierten Schlüsseln durch die Deutsche Bundesbank mehr möglich sind. Um die Kommunikation wieder zu ermöglichen, sind vom Zahlungsdienstleister neue Schlüsselpaare zu generieren und die Initialisierungsbriefe an die Deutsche Bundesbank zu übermitteln.

Werden die Schlüssel der Deutschen Bundesbank kompromittiert, so wird sich diese unmittelbar neu mit gültigen Schlüsseln initialisieren.

5.1.4 TLS-Serverzertifikate

5.1.4.1 Allgemein

Auf Transportebene wird für die Serverauthentifizierung auf Basis von TLS zum Aufbau einer verschlüsselten Verbindung (Standard-Port 443) zwischen der Bundesbank und den Kundensystemen ein SSL-Zertifikat benötigt.

Um die Verifikation des Zertifikats auf Kundenseite zu erleichtern, wird von der Deutschen Bundesbank die Zertifikation durch ein kommerzielles Trustcenter unterstützt, dessen CA Zertifikate bereits in den meisten Keystores integriert sind. Auf Kundenseite kann damit die Authentizität des öffentlichen Schlüssels der Deutschen Bundesbank durch automatische Prüfung der digitalen Signatur der CA bestätigt werden.

Für den Produktionsbetrieb wird von der Deutschen Bundesbank auf Kundenseite ebenfalls die Ausgabe von Zertifikaten, die von einem kommerziellen Trustcenter ausgestellt wurden, vorausgesetzt.

Entsprechend einer Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[2] wird ausschließlich die aktuelle Verschlüsselungsversion TLS 1.2 mit den im Rahmen von TLS 1.2 unterstützten und empfohlenen „Cipher-Suiten“ unterstützt.

5.1.4.2 Fingerprintvergleich

Als zusätzliche Hilfestellung zur Überprüfung der Echtheit eines Zertifikates wird der jeweils gültige Fingerprint auf der Internetseite der Deutschen Bundesbank als gesonderter Anhang zu diesem Dokument veröffentlicht.

5.2 Technische Verfahrensbeschreibung

5.2.1 EBICS-Parameter

Für die Kommunikation zwischen einem Zahlungsdienstleister und der Deutschen Bundesbank werden Parameter analog dem DFÜ-Abkommen genutzt. Dabei ist die Teilnehmer-ID und Kunden-ID der Deutschen Bundesbank vorgegeben und wird mit den Zulassungsunterlagen bekannt gemacht. Die Teilnehmer-ID und Kunden-ID für Zahlungsdienstleister vergibt ebenfalls die Deutsche Bundesbank. Der Aufbau der Kunden-ID richtet sich nach den Vorgaben der EBICS-Spezifikation. Sie ist immer 8-stellig, beginnend mit einem Alphazeichen.

Die Bankparameter der Deutschen Bundesbank können vom EBICS-System mit der Auftragsart „HPD“ abgerufen werden.

Alle Ein- und Auslieferungen erfolgen verschlüsselt (Ausnahme Auftragsarten INI und HIA) und komprimiert. Die Verschlüsselung (Hybrid-Verfahren 3DES/RSA) und die Komprimierung (ZIP-Komprimierung) entsprechen den Vorgaben des DFÜ-Abkommens.

[2] BSI TR-02102-2 (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html)

Die für die Übertragung via EBICS relevanten Parameter und Informationen werden nicht im Dateinamen, sondern über den EBICS-XML-Umschlag übermittelt.

5.2.2 Auftragsnummervergabe

Gemäß der Spezifikation für die EBICS-Anbindung wird seit Version 2.5 (Schemaversion H004) die Auftragsnummer durch den Bankserver zugewiesen.

Im Falle einer kundenseitigen Auftragsnummernvergabe erfolgt eine Fehlermeldung.

5.2.3 Upload Transaktionen

5.2.3.1 Senderichtung Zahlungsdienstleister ⇨ Deutsche Bundesbank

Sämtliche Dateieinreichungen bei der Deutschen Bundesbank erfolgen als EBICS-Upload-Transaktionen auf das EBICS-System der Deutschen Bundesbank.

Bei jeder Aufnahme der Kommunikation wird seitens der Deutschen Bundesbank der Hashwert des aktuell gültigen öffentlichen Schlüssels geprüft. Fällt die Prüfung während des Zeitraums negativ aus, in dem die Deutsche Bundesbank parallel zwei öffentliche Schlüssel unterstützt (siehe Ziffer 5.1.3.2), so erhält der Kunde bei der ersten Dateieinreichungen nach der Generierung eines neuen Schlüssels und der systemseitigen Registrierung der Verwendung des vorhergehenden Schlüssels eine Fehlermeldung mit dem EBICS Return Code „EBICS_BANK_PUBKEY_UPDATE_REQUIRED“. Die Fehlermeldung weist auf die Verwendung des vorhergehenden Schlüssels und die Notwendigkeit einer Aktualisierung desselben hin. Zusätzlich wird einmalig ein Eintrag im Kundenprotokoll geschrieben, der auf den veralteten öffentlichen Schlüssel hinweist. Die zurückgewiesene Datei ist erneut – mit dem vorhergehenden oder neuen Schlüssel – einzureichen.

Weitere Aufträge während des Übergangszeitraums kann der Zahlungsdienstleister mit dem vorhergehenden öffentlichen Schlüssel 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 Auftragsartberechtigung. Die Ergebnisse weiterer bankfachlicher Prüfungen, wie beispielsweise Kontoberechtigungsprüfungen, werden dem Zahlungsdienstleister im Kundenprotokoll zu einem späteren Zeitpunkt mitgeteilt.

Folgende Auftragsarten können für Einreichungen bei der Deutschen Bundesbank genutzt werden:

5.2.3.1.1 Einreichungen in den SEPA-Clearer des EMZ

Auftragsart	Text	Format
QB1	BILATERAL INPUT CREDIT FILE (BCF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029) SEPA Request for Status Update on a Request for Recall by the Originator (pacs.028)	BBkBCFBlkCdtTrf
QC1	INPUT CREDIT FILE (ICF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029) SEPA Request for Status Update on a Request for Recall by the Originator (pacs.028)	BBkICFBlkCdtTrf
QD5	INPUT CORE DEBIT FILE (CORE IDF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002) SEPA Reversal (pacs.007) SEPA Return/Refund (pacs.004 SDD)	BBkIDFBlkDirDeb
QD6	INPUT B2B DEBIT FILE (B2B IDF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002) SEPA Reversal (pacs.007) SEPA Return (pacs.004 SDD)	BBkIDFBlkDirDeb
QK1	SCC INPUT DEBIT FILE (SCC IDF) Interbank Card Clearing Collection (pacs.003 SCC) Interbank Reversal (pacs.007 SCC) Interbank Return/Refund (pacs.004 SCC) Supplementary Data Field (supl.017)	BBkIDFBlkSCC

Tabelle 4: Auftragsarten für die Einreichung in den SEPA-Clearer des EMZ

5.2.3.1.2 Einreichungen in das HBV-Individual

Auftragsart	Text	Format
QG2	GT-Datei, Taggleiche Euro-Überweisungen von Zahlungs-dienstleistern	BBk-SWIFT gemäß Anlage der Verfahrensregeln HBV-Individual[3], Tz 1.8.1 > EBCDIC/ungepackt > SLF: 6Bn[4]
QWT	WT-Datei, AZV-Überweisung in Fremdwährung von Zahlungs-dienstleistern	BBk-SWIFT gemäß Anlage der Verfahrensregeln HBV-Individual[3], Tz 1.8.2 > EBCDIC/ungepackt > SLF: 6Bn[4]

Tabelle 5: Auftragsarten für die Einreichung in das HBV-Individual

5.2.3.1.3 Umsatzanfragen an KTO2 / elektronische Kontoinformationen

Auftragsart	Text	Format
QMA	MA-Datei, untertägige Umsatz- und Saldenanfrage	BBk-SWIFT gemäß Anlage der Verfahrensregeln elektronische Konto-informationen[3], Tz 1.5 > A- und E-Satz EBCDIC/ungepackt > SLF: 6Bn[4]

Tabelle 6: Auftragsart für Umsatzanfragen an KTO2 / elektronische Kontoinformationen

5.2.3.1.4 Einreichungen in den Scheckabwicklungsdienst des EMZ

Auftragsart	Text	Format
QS1	SVV BSE INPUT DEBIT FILE BSE-Scheck (pacs.003 SVV) BSE-Rückrechnung (pacs.004 SVV)	BBkIDFBlkSVV
QS2	SVV ISE INPUT DEBIT FILE ISE-Scheck (pacs.003 SVV)	BBkIDFBlkSVV
QS3	SVV ISR INPUT DEBIT FILE ISE-Rückrechnung (pacs.004 SVV)	BBkIDFBlkSVV

Tabelle 7: Auftragsart für Einreichung in Scheckabwicklungsdienst des EMZ der Deutschen Bundesbank

Die Transaktionsinitialisierung erfolgt gemäß EBICS-Standard. Da die Deutsche Bundesbank derzeit für Einlieferungen keinen öffentlichen Signaturschlüssel mit der Auftragsart „HPB“ bereitstellt, ist für das Element `BankPubKeyDigests/Signature` die maximale Häufigkeit (maxOccurs) auf 0 zu setzen. Die Übertragung der Nutzdaten erfolgt gemäß EBICS-Standard.

Die eingelieferten Daten sind für eine Versandwiederholung mindestens 10 Geschäftstage vorzuhalten.

[3] Verfahrensregeln der Deutschen Bundesbank zum Abruf elektronischer Kontoinformationen

Für die o. g. Auftragsarten ist nur das Auftragsattribut „OZHNN“ zulässig. Folgende Schlüssel werden verwendet:

1. Fall: Zahlungsdienstleister verwendet separate Schlüssel

	Deutsche Bundesbank		**Zahlungsdienstleister**	
	Signieren, Verschlüsseln	Prüfen, Entschlüsseln	Signieren, Verschlüsseln	Prüfen, Entschlüsseln
Authentifikation	BASs	KACp	KACs	BASp
Verschlüsselung	-	BVSs	BVSp	-
EU	-	KECp	KECs	-

Tabelle 8: Separate Schlüssel bei der Einreichung

2. Fall: Zahlungsdienstleister verwendet gemeinsame Schlüssel

	Deutsche Bundesbank		**Zahlungsdienstleister**	
	Signieren, Verschlüsseln	Prüfen, Entschlüsseln	Signieren, Verschlüsseln	Prüfen, Entschlüsseln
Authentifikation	BASs	KAp	KAs	BASp
Verschlüsselung	-	BVSs	BVSp	-
EU	-	KEp	KEs	-

Tabelle 9: Gemeinsame Schlüssel bei der Einreichung

5.2.3.2 Senderichtung Deutsche Bundesbank ⇨ Zahlungsdienstleister

Sämtliche Dateiauslieferungen durch die Deutsche Bundesbank erfolgen als EBICS-Upload-Transaktionen auf das EBICS-System des Zahlungsdienstleisters. Folgende Auftragsarten werden für Auslieferungen durch die Deutsche Bundesbank genutzt:

5.2.3.2.1 Auslieferungen aus dem SEPA-Clearer des EMZ

Auftragsart	**Text**	**Format**
QB2	BILATERAL SETTLED CREDIT FILE (BCF) SEPA Credit Transfer (pacs.008) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Credit Transfer Return (pacs.004 SCT) SEPA Resolution of Investigation (camt.029) SEPA Request for Status Update on a Request for Recall by the Originator (pacs.028)	BBkBCFBlkCdtTrf
QC2	CREDIT VALIDATION FILE (CVF) SEPA Reject Credit Transfer durch den SEPA-Clearer (pacs.002 SCLSCT)	BBkCVFBlkCdtTrf

Auftragsart	Text	Format
QC3	SETTLED CREDIT FILE (SCF) SEPA Credit Transfer (pacs.008) SEPA Return (pacs.004 SCT) SEPA Payment Cancellation Request (camt.056 SCT) SEPA Resolution of Investigation (camt.029) SEPA Request for Status Update on a Request for Recall by the Originator (pacs.028)	BBkSCFBlkCdtTrf
QK2	SCC DEBIT VALIDATION FILE (SCC DVF) SCC Reject Card Clearing Collection durch den SEPA-Clearer (pacs.002SCLSCC)	BBkDVFBlkSCC
QK3	SCC DEBIT NOTIFICATION FILE (SCC DNF) Interbank Card Clearing Collection (pacs.003 SCC) Supplementary Data Field (supl.017)	BBkDNFBlkSCC
QK4	SCC SETTLED DEBIT FILE (SCC SDF) Interbank Reversal (pacs.007 SCC) Interbank Return/Refund (pacs.004 SCC) Supplementary Data Field (supl.017)	BBkSDFBlkSCC
QK5	SCC UNSETTLED DEBIT FILE (UDF) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004)	BBkUDFBlkSCC
QK6	SCC RESULT OF SETTLEMENT FILE (RSF) SEPA Reject (pacs.002SCLSCC)	BBkRSFBlkSCC
QR1	DAILY RECONCILIATION REPORT FOR CREDIT Transfers (DRC) – keine XML Struktur –	EBCDIC
QR5	DAILY RECONCILIATION REPORT FOR SCC (DRR SCC) – keine XML-Struktur –	EBCDIC
QD7	DEBIT CORE VALIDATION FILE (DVF) SEPA Reject Direct Debit durch den SEPA-Clearer (pacs.002 SCLSDD)	BBkDVFBlkDirDeb
QD8	DEBIT CORE NOTIFICATION FILE (DNF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002)	BBkDNFBlkDirDeb
QD9	SETTLED CORE DEBIT FILE (SDF) SEPA Return/Refund (pacs.004 SDD) SEPA Reversal (pacs.007)	BBkSDFBlkDirDeb

Auftragsart	Text	Format
QDA	DEBIT B2B VALIDATION FILE (DVF) SEPA Reject Direct Debit durch den SEPA-Clearer (pacs.002 SCLSDD)	BBkDVFBlkDirDeb
QDB	DEBIT B2B NOTIFICATION FILE (DNF) SEPA Direct Debit (pacs.003) SEPA Payment Cancellation Request (camt.056 SDD) SEPA Reject (pacs.002)	BBkDNFBlkDirDeb
QDC	SETTLED B2B DEBIT FILE (SDF) SEPA Return (pacs.004 SDD) SEPA Reversal (pacs.007)	BBkSDFBlkDirDeb
QDD	UNSETTLED DEBIT CORE FILE (UDF) SEPA Reject (pacs.002SDD) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004SDD)	BBkUDFBlkDirDeb
QDE	UNSETTLED DEBIT B2B FILE (UDF) SEPA Reject (pacs.002SDD) SEPA Direct Debit (pacs.003) SEPA Return/Refund (pacs.004 SDD)	BBkUDFBlkDirDeb
QDF	RESULT OF SETTLEMENT CORE FILE (RSF) SEPA Reject (pacs.002 SCLSDD)	BBkRSFBlkDirDeb
QDG	RESULT OF SETTLEMENT B2B FILE (RSF) SEPA Reject (pacs.002 SCLSDD)	BBkRSFBlkDirDeb
QR3	DAILY RECONCILIATION REPORT FOR CORE DIRECT DEBITS (DRD CORE) – keine XML-Struktur –	EBCDIC
QR4	DAILY RECONCILIATION REPORT FOR B2B DIRECT DEBITS (DRD B2B) - keine XML-Struktur -	EBCDIC
QSD	SEPA-Clearer Directory Übermittlung im rocs-Datensatzformat der European Automated Clearing House Association (EACHA)	Gemäß XML-Schema: Rocs.001.001.06

Tabelle 10: Auftragsarten für die Auslieferung aus dem SEPA-Clearer des EMZ

5.2.3.2.2 Auslieferungen aus dem HBV-Individual

Auftragsart	Text	Format
QG4	GT-Datei, Taggleiche Euro-Überweisungen an Zahlungs-dienstleister	BBk-SWIFT gemäß Anlage der Verfahrensregeln HBV-Individual[3], Tz. 1.8.1 > A- und E-Satz EBCDIC/ungepackt > SLF: 6Bn[4]
QWA	Abrechnung über Fremdwährungen (WA)	BBk-SWIFT gemäß Anlage der Verfahrensregeln HBV-Individual[3], Tz. 1.8.2 > A- und E-Satz EBCDIC/ungepackt > SLF: 6Bn[4]
QM3	M3-Nachricht; Mitteilung über eine nicht verarbeitbare Datei	M-Dateien gemäß Anlage der Verfahrensregeln HBV-Individual[3], Tz. 1.9 > EBCDIC/ungepackt > SLF: 4Bn[4]
QMH	M6-Nachricht; Freie Textnachricht	
QM7	M7-Nachricht; Mitteilung über nicht ausgeführte bzw. annullierte Zahlungen	
QM8	M8-Nachricht; Mitteilung über nicht verarbeitbare Datensätze	
QM9	M9-Nachricht; Mitteilung über verarbeitete Zahlungen und ausgelieferte Dateien	

Tabelle 11: Auftragsarten für die Auslieferung aus dem HBV-Individual

5.2.3.2.3 Auslieferungen aus KTO2 / elektronische Kontoinformationen

Auftragsart	Text	Format
QMU	Untertägige Umsatz- und Saldeninformation	BBk-SWIFT gemäß Anlage der Verfahrensregeln elektronische Kontoinformationen[5], Tz 1.5 > A- und E-Satz EBCDIC/ungepackt > SLF: 6Bn[4]
QMK	MK-Datei, Tagesendeauszug	
QMN	M3-Datei, Mitteilung über eine nicht verarbeitungsfähige MA-Datei	

Tabelle 12: Auftragsarten für die Auslieferung aus KTO2 / elektronische Kontoinformationen

5.2.3.2.4 Auslieferungen aus dem Scheckabwicklungsdienst des EMZ

Auftragsart	Text	Format
QS4	SVV BSE DEBIT VALIDATION FILE BSE Reject durch Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QS5	SVV BSE DEBIT NOTIFICATION FILE BSE Scheck (pacs.003 SVV)	BBkDNFBlkSVV
QS6	SVV BSE SETTLED DEBIT FILE BSE-Rückrechnung (pacs.004SVV)	BBkSDFBlkSVV
QS7	SVV ISE DEBIT VALIDATION FILE ISE Reject durch Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QS8	SVV ISE DEBIT NOTIFICATION FILE ISE Scheck (pacs.003 SVV)	BBkDNFBlkSVV
QS9	SVV ISR SETTLED DEBIT FILE ISE Rückrechnung (pacs.004 SVV)	BBkSDFBlkSVV
QSA	SVV ISR DEBIT VALIDATION FILE ISE Rückrechnung Reject durch Deutsche Bundesbank (pacs.002 SVV)	BBkDVFBlkSVV
QSB	SVV BSE UNSETTLED DEBIT FILE (UDF) BSE cheque (pacs.003SVV) BSE return account (pacs.004SVV)	BBkUDFBlkSVV
QSC	SVV ISE UNSETTLED DEBIT FILE (UDF) ISE cheque (pacs.003SVV)	BBkUDFBlkSVV
QSE	SVV ISR UNSETTLED DEBIT FILE (UDF) ISE return account (pacs.004SVV)	BBkUDFBlkSVV
QSF	SVV BSE RESULT OF SETTLEMENT FILE (RSF) BSE reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QSG	SVV ISE RESULT OF SETTLEMENT FILE (RSF) ISE reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QSH	SVV ISR RESULT OF SETTLEMENT FILE (RSF) ISE return account reject by Deutsche Bundesbank (pacs.002SVV)	BBkRSFBlkSVV
QR6	DAILY RECONCILIATION REPORT FOR SVV BSE (DRD BSE)	EBCDIC
QR7	DAILY RECONCILIATION REPORT FOR SVV ISE (DRD ISE)	EBCDIC
QR8	DAILY RECONCILIATION REPORT FOR SVV ISR (DRD ISR)	EBCDIC

Tabelle 13: Auftragsarten für die Auslieferung aus Scheckabwicklungsdienst

Die Transaktionsinitialisierung erfolgt gemäß EBICS-Standard. Da für Auslieferungen kein öffentlicher Signaturschlüssel des Zahlungsdienstleisters mit der Auftragsart HPB ausgeliefert wird, wird für das Element `BankPubKeyDigests/Signature` die maximale Häufigkeit (maxOccurs) auf 0 gesetzt. Die Übertragung der Nutzdaten erfolgt gemäß EBICS-Standard.

Eine Zweitauslieferung der Daten ist bis maximal 10 Geschäftstage nach der erstmaligen erfolgreichen Auslieferung auf Anforderung möglich.

Die oben genannten Auftragsarten werden nur mit dem Auftragsattribut „OZHNN“ ausgeliefert. Folgende Schlüssel werden verwendet:

1. Fall: Zahlungsdienstleister verwendet separate Schlüssel

	Deutsche Bundesbank		**Zahlungsdienstleister**	
	Signieren, Verschlüsseln	Prüfen, Entschlüsseln	Signieren, Verschlüsseln	Prüfen, Entschlüsseln
Authentifikation	BACs	KASp	KASs	BACp
Verschlüsselung	KVSp	-	-	KVSs
EU	BECs	-	-	BECp

Tabelle 14: Separate Schlüssel bei der Auslieferung

2. Fall: Zahlungsdienstleister verwendet gemeinsame Schlüssel

	Deutsche Bundesbank		**Zahlungsdienstleister**	
	Signieren, Verschlüsseln	Prüfen, Entschlüsseln	Signieren, Verschlüsseln	Prüfen, Entschlüsseln
Authentifikation	BACs	KAp	KAs	BACp
Verschlüsselung	KVp	-	-	KVs
EU	BECs	-	-	BECp

Tabelle 15: Gemeinsame Schlüssel bei der Auslieferung

5.2.4 Download-Transaktionen

Download-Transaktionen bilden in der EBICS-Kommunikation mit der Deutschen Bundesbank eine Ausnahme. Folgende Auftragsarten sind als Download-Transaktionen realisiert:

Auftragskennung	**Beschreibung**
HPB	Abholen der Öffentlichen Schlüssel der Bank oder des Zahlungsdienstleisters
HPD	Bankparameter abholen
HAC	Kundenprotokoll im XML-Format abrufen
PTK	Kundenprotokoll im DTAUS0-Format
HKD	Kunden- und Teilnehmerinformationen abholen
HTD	Kunden- und Teilnehmerinformationen abrufen

Tabelle 16: Auftragsarten für die Abholung vom EBICS-System

Die Auftragsarten „HPB“, „HPD“ und „PTK“/„HAC“ müssen verpflichtend vom EBICS-System des Zahlungsdienstleisters für den Abruf der Daten durch die Deutschen Bundesbank angeboten werden.

Mit der Auftragsart „HPD“ stellt die Deutsche Bundesbank ihre jeweils aktuellen Bankparameterdaten für die Kommunikation über EBICS bereit, Kundenprotokolle werden mit der Auftragsart „HAC“ bzw. „PTK“ bereitgestellt.

5.2.5 Kundenprotokoll

Die Kundenprotokolle werden zum Download mit der Auftragsart „HAC“ und übergangsweise auch noch mit der Auftragsart „PTK“ bereitgestellt.

Der Abruf der Kundenprotokolle mit der Auftragsart „HAC“ bzw. übergangsweise mit der Auftragsart „PTK“ ist mit Vordruck 4750 „Antrag auf EBICS-Kommunikation Zahlungsdienstleister mit BLZ“ zu beantragen.

Hinweis:
Bereits produktive EBICS-Teilnehmer haben bei Erweiterung des Leistungsspektrums, d. h. Hinzunahme von „HAC“, vor dem Produktionseinsatz einen erneuten Abnahmetest durch das Kundentestzentrum zu absolvieren.

Das Kundenprotokoll der Deutschen Bundesbank ist EBICS-konform gemäß Kapitel 10 der Spezifikation für die EBICS-Anbindung (HAC) bzw. Kapitel 4.2 der Common Integrative Implementation Guide to Supplement the EBICS Specification (PTK) aufgebaut.

Im Kundenprotokoll werden die im Kunde-Bank-Standard definierten Fehlercodes verwendet, so dass die Realisierung einer automatisierten Verarbeitung möglich ist (Fehlercodes für „HAC“ siehe Kapitel 10.3 der EBICS Spezifikation). Sollte ein Zahlungsdienstleister nicht zur Einreichung von Aufträgen für den im Tag `<SndgInst>` des Fileheaders genannten BIC berechtigt sein, wird der Auftrag mit dem auf den Teilnehmer bezogenen EBICS Fehlercode [27] "Keine Unterschriftsberechtigung" bei „PTK“ bzw. Fehlercode DS0H „NotAllowedAccount“ (keine Unterschriftsberechtigung) bei „HAC“ zurückgewiesen. Die Kundenprotokolle werden maximal 10 Geschäftstage zum Abruf bereitgehalten.

Ein empfangender Zahlungsdienstleister hat im Gegenzug für die von der Deutschen Bundesbank ausgelieferten Daten ein EBICS-Kundenprotokoll nach Maßgabe des DFÜ-Abkommens zu erstellen. Er hat ebenfalls sicherzustellen, dass für jeden Auftrag eine Dateianzeige im Kundenprotokoll erstellt wird. Die Dateianzeige soll sich an den Beschreibungen zum Aufbau der Dateianzeige im Kundenprotokoll der Deutschen Bundesbank orientieren (Tabelle 17 bis Tabelle 20).

Für die Auftragsarten der Tabellen 4 bis 7 erfolgt eine Dateianzeige im Kundenprotokoll.

Die Dateianzeige für die Auftragsarten QB1, QC1, QD5, QD6, QK1, QS1, QS2 und QS3 beinhaltet folgende Informationen des File Headers der Zahlung:

Beschreibung	Feld Name	XML-Element File Header
Zahlungsart	File Type	`FType`
11-stelliger BIC des Senders	Sending Institution	`SndgInst` [4]
Erstellungsdatum	File Date and Time	`FDtTm`
Anzahl der Zahlungssätze (Summe der Bulks)	Total Number of Bulks	Für `FType` = „CORE IDF“: `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` Für `FType` = „B2B IDF“: `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` Für `FType` = „SCC IDF“: `NumDDBlk + NumPCRBlk + NumREJBlk + NumRVSBlk + NumRFRBlk` Für `FType` = „ICF“: `NumCTBlk + NumRFRBlk + NumPCRBlk + NumROIBlk` Für `FType` = „BCF“: `NumCTBlk + NumPCRBlk + NumROIBlk + NumRFRBlk`
Dateireferenz des Senders	File Reference	FileRef

Tabelle 17: Aufbau Dateianzeige des Kundenprotokolls für Einreichungen in den SEPA-Clearer des EMZ und den Scheckabwicklungsdienst des EMZ

Beispiel Dateiinhalt QC1:

```
…
<AddtlInf>==========================================</AddtlInf>
<AddtlInf>ICF</AddtlInf>
<AddtlInf>BIC des Senders                    : BANKDEFF500</AddtlInf>
<AddtlInf>Erstellungsdatum                   :2012-04-03T10:11:35</AddtlInf>
<AddtlInf>Anzahl der Zahlungssaetze          :397</AddtlInf>
<AddtlInf>Dateireferenz des Senders          :1234567890123456</AddtlInf>
<AddtlInf>==========================================</AddtlInf>
</StsRsnInf>
…
```

Für die Auftragsart QG2 ist die Dateianzeige wie folgt aufgebaut:

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bankleitzahl	Leitzahl des Empfängers der Datei; Bei Einlieferungen BLZ der kontoführenden Bundesbankfiliale	A3

[4] Als Sending Institution wird hier der BIC des SEPA-Clearers eingestellt (in der Produktion MARKDEFF)

Beschreibung	Feld Name	Position
Kontonummer	Leitzahl des Absenders der Datei	Bei Einlieferungen von Zahlungsdienstleistern mit Bankleitzahl: A4. Bei Einlieferungen von Zahlungsdienstleister ohne Bankleitzahl: 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 18: Aufbau Dateianzeige des Kundenprotokolls Zahlungsaufträge in Euro im EÖ-Format

Für die Auftragsart QWT ist die Dateianzeige wie folgt aufgebaut:

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bankleitzahl	Leitzahl des Empfängers der Datei; Bei Einlieferungen BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei	Bei Einlieferungen von Zahlungsdienstleister mit Bankleitzahl: A4 Bei Einlieferungen von Zahlungsdienstleister ohne Bankleitzahl: 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 19: Aufbau Dateianzeige des Kundenprotokolls Zahlungsaufträge in Fremdwährung

Für die Auftragsart QMA ist die Dateianzeige wie folgt aufgebaut:

Beschreibung	Feld Name	Position
Zahlungsart	Dateikennzeichen/Dateityp	A2
Bankleitzahl	Leitzahl des Empfängers der Datei; Bei Einlieferungen BLZ der kontoführenden Bundesbankfiliale	A3
Kontonummer	Leitzahl des Absenders der Datei	Bei Einlieferungen von Zahlungsdienstleister mit Bankleitzahl: A4 Bei Einlieferungen von Zahlungsdienstleister ohne Bankleitzahl: A9
Einreicher	Bezeichnung des Absenders der Datei	A5
Erstellungsdatum	Datum Geschäftstag	A6
Dateinummer	Eindeutige Nummer der Datei	A7
Anzahl der Datensätze	Anzahl der Datensätze	E3

Tabelle 20: Aufbau Dateianzeige des Kundenprotokolls Umsatzanfragen

Die Protokolle sind für den Abruf durch die Deutsche Bundesbank mindestens 10 Geschäftstage bereitzuhalten.

Die Protokollierung des Schlüsselmanagements und der sonstigen systembedingten Auftragsarten hat den Vorgaben der EBICS-Spezifikation zu entsprechen. Diese Protokolle werden von der Deutschen Bundesbank 10 Geschäftstage vorgehalten und sind vom Zahlungsdienstleister ebenfalls 10 Geschäftstage bereit zu halten.

5.3 Back-Up-Verfahren

Das Back-Up-Verfahren für die EBICS-Kommunikation mit Zahlungsdienstleistern ist DFÜ nächster Geschäftstag.

6 Testanforderungen

Hinweise zum Testverfahren sind der „Anlage Test zu den Verfahrensregeln der Deutschen Bundesbank zur Kommunikation über EBICS mit Einlagenkreditinstituten und sonstigen Kontoinhabern mit Bankleitzahl“ zu entnehmen.