

**Anlage
zu den
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-Anbindung)

gültig ab 19. November 2017

SRZ-Anbindung

Inhaltsverzeichnis

1	Zulassung zum Produktionsbetrieb	4
2	Sicherungsverfahren	5
2.1	Elektronische Unterschriften.....	5
2.2	Authentifikationssignatur.....	5
2.3	Verschlüsselung	6
3	Initialisierung der EBICS-Anbindung	7
3.1	Einrichtung der Kommunikationsverbindung	7
3.2	Initialisierung der Schlüssel	7
3.2.1	Neuinitialisierung der Teilnehmerschlüssel	7
3.2.2	Initialisierung der bankseitigen Schlüssel	9
4	Delta-Vorgaben zur Verwendung von EBICS	10
4.1	Grundlagen und Überblick	10
4.1.1	Verwendete Version der Spezifikation für die EBICS-Anbindung und Grobüberblick über das Delta	10
4.2	Festlegungen	10
4.2.1	Unterschriftsklasse	10
4.2.2	Vorabprüfung	11
4.2.3	Ablauf der Autorisierung	11
4.2.4	SRZ-Kundenprotokoll	12
4.2.5	Verwendung von XML-Containern.....	13
4.2.6	Auftragsarten für das SRZ-Verfahren	13
5	Änderung der Teilnehmerschlüssel mit automatischer Freischaltung	16
6	Regelmäßige Änderung des öffentlichen Bankschlüssels	17
7	Sperrung der Teilnehmerschlüssel	18
8	Testanforderungen	19
8.1	Grundsätzliches	19
8.2	Testszenarien	20
8.2.1	Initialisierung der EBICS-Anbindung	20
8.2.2	Download Transaktionen	20
8.2.3	Datenaustausch über die EBICS-Anbindung.....	20
9	Delta-Vorgaben zum SEPA-Zahlungsverkehr	21

SRZ-Anbindung

9.1	Grundlagen und Überblick	21
9.1.1	Verwendung von SEPA-Datenformaten im SRZ-Verfahren	21
9.1.2	Verwendete Version der Anlage 3 des DFÜ-Abkommens und Grobüberblick über das Delta	22
9.2	Festlegungen	22
9.2.1	Verwendung des XML-Containers	22
9.2.2	Beschränkung auf einen Sammler pro ISO-Nachricht	23
9.2.3	Verpflichtende Einstellung des Hashwertes in den XML-Container	24
9.2.4	Hinterlegung der Kennung des SRZ	25
9.2.5	Besonderheiten bei der Belegung und Einlieferung von SEPA-Überweisungen bei der Deutschen Bundesbank	27
9.2.6	Besonderheiten bei der Belegung und Einlieferung von SEPA-Lastschriften bei der Deutschen Bundesbank	28
9.3	Beispiel	29
9.4	Kontrollmaßnahmen	34
10	Delta-Vorgaben für SCC-Karteneinzüge	35
10.1	Grundlagen und Überblick	35
10.1.1	Verwendung von SCC-Datenformaten im SRZ-Verfahren	35
10.1.2	Grundlegende Festlegungen zu den Vorgaben	35
10.2	Festlegungen zum XML-Container	36
10.3	Besonderheiten bei der Belegung und Einlieferung von SCC-Karteneinzügen bei der Deutschen Bundesbank	39
10.4	Kontrollmaßnahmen	40

SRZ-Anbindung

1 Zulassung zum Produktionsbetrieb

Für die EBICS-Kommunikation ist zunächst vom SRZ ein Zulassungs- und Conformancetest zu durchlaufen (nähere Einzelheiten s. Nummer 8 „Testanforderungen“).

Die Zulassung zum Produktionsbetrieb für die EBICS-Kommunikation ist vom SRZ mit dem Vordruck 4755 „Antrag auf EBICS-Kommunikation Service-Rechenzentrum (SRZ)“ beim Kundenbetreuungsservice zu beantragen.

SRZ-Anbindung

2 Sicherungsverfahren

Das SRZ benennt der Deutschen Bundesbank im Rahmen der Antragsstellung die EBICS-Teilnehmer.

Folgende Sicherungsverfahren werden in der EBICS-Anbindung eingesetzt:

- Transport-Unterschrift
- Authentifikationssignatur
- Verschlüsselung

Für jedes 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 2 beschriebenen Verfahren mitzuteilen. Die öffentlichen Bankschlüssel sind gemäß dem in Nummer 2 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

Zur Übertragung der Zahlungsaufträge an das Banksystem steht den EBICS-Teilnehmern ausschließlich die Transportunterschrift (Typ „T“) im Rahmen der Elektronischen Unterschrift (EU) zur Verfügung.

Mit dem vom SRZ verwendeten Programm können verschiedene Nachrichten (z. B. SEPA-Überweisungen, Aufträge für Initialisierung, Protokollabruf etc.) erstellt werden. Die Deutsche Bundesbank teilt dem SRZ im Rahmen der Zulassung mit, welche EBICS-Auftragsarten genutzt werden können.

2.2 Authentifikationssignatur

Die Authentifikationssignatur wird über die einzelnen EBICS-Nachricht einschließlich Steuerungs- und Anmeldedaten und die darin enthaltene T-Unterschrift gebildet. Mit Ausnahme einiger in der Spezifikation für die EBICS-Anbindung definierten systembedingten Auftragsarten wird die Authentifikationssignatur bei jedem Transaktionsschritt sowohl vom SRZ- als auch vom Banksystem geleistet. Das SRZ 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

SRZ-Anbindung

gespeicherten öffentlichen Schlüssel der Deutschen Bundesbank gemäß den Vorgaben der Spezifikation für die EBICS-Anbindung prüft.

2.3 Verschlüsselung

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

Darüber hinaus ist auf den externen Übertragungstrecken zwischen SRZ- und Banksystem zusätzlich eine Transportverschlüsselung vorzunehmen. Das SRZ muss gewährleisten, dass eine Software eingesetzt wird, die Aktualität und Authentizität der hierfür eingesetzten Serverzertifikate der Deutschen Bundesbank gemäß den Vorgaben der Spezifikation für die EBICS-Anbindung überprüft.

SRZ-Anbindung

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 SRZ mitgeteilt.

Die Deutsche Bundesbank teilt den vom SRZ 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 2.5 sowie Schemaversion H004)
- Kunden-ID
- EBICS-Teilnehmer-ID
- Weitere spezifische Angaben zu Kunden- und EBICS-Teilnehmerberechtigungen

Für die dem SRZ zugeordneten EBICS-Teilnehmer vergibt die Deutsche Bundesbank jeweils eine EBICS-Teilnehmer-ID, die den EBICS-Teilnehmer eindeutig identifiziert.

3.2 Initialisierung der Schlüssel

3.2.1 Neuinitialisierung der Teilnehmerschlüssel

Die vom EBICS-Teilnehmer eingesetzten Schlüsselpaare für 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 zugeordnet.
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 Sicherung eingesetzten privaten Schlüssel definiert jeder EBICS-Teilnehmer pro Schlüssel ein Passwort, das den Zugriff auf den jeweiligen privaten Schlüssel absichert.

SRZ-Anbindung

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 systembedingten Auftragsarten INI und HIA.
- Mit einem vom SRZ unterschriebenen Initialisierungsbrief an die Zentrale (Z 201-2).

Hierbei ist zu beachten, dass bei der elektronischen Einreichung der 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 SRZ 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
- T-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

SRZ-Anbindung

Die Deutsche Bundesbank prüft die Unterschrift des SRZ oder der gesondert ermächtigten Person auf dem Initialisierungsbrief mit dem auf dem SRZ-Unterschriftenblatt bzw. auf dem Vordruck 4755 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 systembedingten Auftragsart HPB ab.

Der Hashwert des öffentlichen Bankschlüssels wird dem SRZ 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. Das SRZ 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.

SRZ-Anbindung

4 Delta-Vorgaben zur Verwendung von EBICS

4.1 Grundlagen und Überblick

Bei der Verwendung von EBICS unter Einschaltung von SRZ gelten grundsätzlich die in der Spezifikation für die EBICS-Anbindung beschriebenen Regeln und Definitionen. Die jeweils aktuelle Version stellt die Deutsche Kreditwirtschaft (DK) im Internet unter www.ebics.de zur Verfügung. Darüber hinaus werden die nachstehenden, die Spezifikation für die EBICS-Anbindung einschränkenden, Festlegungen für das SRZ-Verfahren getroffen.

4.1.1 Verwendete Version der Spezifikation für die EBICS-Anbindung und Grobüberblick über das Delta

Diese Delta-Vorgaben nehmen Bezug auf die Spezifikation für die EBICS-Anbindung **Version 2.5 und die zugehörigen EBICS-Schemata H004/S001**.

Daraus ergeben sich im Grobüberblick folgende Festlegungen für das SRZ-Verfahren:

Festlegungen hinsichtlich Kapitel in EBICS 2.5	Siehe Nummer in Delta-Vorgaben	Beschreibung
3.5.1	4.2.1	SRZ wird grundsätzlich nur die Unterschriftsklasse „T“ zugeordnet.
3.6, 5.3	4.2.2	Die Vorabprüfung ist nicht vorgesehen.
3.12	4.2.3	Modifikationen zum Ablauf der Autorisierung im EBICS-Verfahren
10	4.2.4	EBICS-Kundenprotokoll (HAC): Die Spezifikation des Kundenprotokolls PTK, das nur in Deutschland verwendet wird, wird durch die Spezifikation eines XML-basierten Kundenprotokolls (HAC) ergänzt.
13	4.2.6	Die für das SRZ-Verfahren zulässigen Auftragsarten

4.2 Festlegungen

4.2.1 Unterschriftsklasse

Die Auftragsdaten der Sendeaufträge müssen vor dem Versand signiert, d. h. mit einer Elektronischen Unterschrift (EU) versehen werden.

Vom SRZ eingereichte Sendeaufträge werden grundsätzlich mit einer Transport-Unterschrift (Unterschriftsklasse „T“) signiert. Zur nachträglichen elektronischen Autorisierung steht dem Kunden die Verteilte Elektronische Signatur (VEU; siehe Kapitel 8 der Spezifikation für die EBICS-Anbindung) zur Verfügung.

SRZ-Anbindung

Unterschriftsberechtigungen des Typs „T“ werden dem SRZ bzw. den EBICS-Teilnehmern des SRZ pauschal zugewiesen. Die vom SRZ eingesetzte Transportunterschrift dient ausschließlich zur Absicherung der Einreichung von Sendeauftragsdaten, die das SRZ im Auftrag seiner Kunden gemäß SRZ-Vereinbarung durchführt. Die Transportunterschrift ist in diesem Fall nur dem SRZ (Teilnehmer innerhalb des SRZ) zugeordnet.

4.2.2 Vorabprüfung

Die Vorabprüfung steht in der Abwicklung des Zahlungsverkehrs unter Einschaltung von SRZ nicht zur Verfügung. Daher entfallen für das SRZ-Verfahren die Kapitel 3.6 und 5.3 der Spezifikation für die EBICS-Anbindung.

4.2.3 Ablauf der Autorisierung

Die in Kapitel 3.12 (Ablauf der EBICS-Transaktionen) der Spezifikation für die EBICS-Anbindung beschriebenen Varianten der Autorisierung sind für das SRZ-Verfahren nur eingeschränkt gültig. Für die Autorisierung der Auftragsdaten im SRZ-Verfahren gelten folgende Bestimmungen:

Die Einreichung der Nutzdaten (Auftragsdaten) der Mandanten (Sammeldatei) erfolgt zusammen mit einer Transport-EU (Unterschriftsklasse „T“) durch einen Sendeauftrag des SRZ mit den Auftragsattributen „DZHNN“.

Die Deutsche Bundesbank prüft die Transport-EU des SRZ unmittelbar nach Empfang der Auftragsdaten.

Bei negativem Prüfergebnis wird die gesamte Datei mit den Auftragsdaten von der Deutschen Bundesbank abgelehnt und unmittelbar das negative Prüfergebnis in das für das SRZ bestimmte Kundenprotokoll gemäß der Spezifikation für die EBICS-Anbindung protokolliert. Das SRZ ist verpflichtet, sich durch zeitnahes Abholen des Kundenprotokolls vom Status der Bearbeitung der eingereichten Auftragsdaten zu informieren. Eine Konto- und/oder Limitprüfung erfolgt im Rahmen der Prüfung der Transport-EU (Unterschriftsklasse „T“) des SRZ nicht.

Bei positivem Prüfergebnis wird die gesamte Datei mit den Auftragsdaten von der Deutschen Bundesbank der Weiterverarbeitung zugeführt und unmittelbar das positive Prüfergebnis in das für das SRZ bestimmte Kundenprotokoll gemäß der Spezifikation für die EBICS-Anbindung protokolliert. Das SRZ ist verpflichtet, sich durch zeitnahes Abholen des Kundenprotokolls vom Status der erfolgreichen Dateiübertragung und der Prüfung der Transportunterschrift der eingereichten Auftragsdaten zu informieren.

SRZ-Anbindung

Durch die positive Prüfung der Transport-EU des SRZ ist keine Autorisierung der Auftragsdaten der Mandanten erfolgt. Eine Autorisierung durch die berechtigten Kunden der Deutschen Bundesbank (Mandanten des SRZ) erfolgt gemäß gesonderter Vereinbarung entweder durch Elektronische Unterschrift(en) oder durch Pauschalautorisierung.

Die Einreichung der noch ausstehenden bankfachlichen EU(s) erfolgt unmittelbar durch den (unterschriftsberechtigten) Kunden der Deutschen Bundesbank, d. h. durch dessen unterschiftsberechtigte EBICS-Teilnehmer mit Hilfe der Auftragsart HVE gemäß der Spezifikation für die EBICS-Anbindung.

Jede logische Datei (Sammler) bezieht sich auf genau eine Kontoverbindung. Die Autorisierung wird entsprechend der jeweiligen Kundenvereinbarungen je Kontoverbindung auf den Systemen der Deutschen Bundesbank hinterlegt. Die Bereitstellung der Auftragsdaten für die elektronische Signatur (Einstellung in VEU) wird im jeweiligen Kundenprotokoll des betreffenden Kunden eingetragen.

4.2.4 SRZ-Kundenprotokoll

Für die Protokollierung von Einreichungen (vgl. Spezifikation für die EBICS-Anbindung, Kapitel 10) gilt folgende Besonderheit:

Pro im Container enthaltener logischer Datei wird immer der Hashwert im SRZ-Kundenprotokoll ausgegeben. Die anderen Kundenprotokollvarianten des Kapitels 10 gelten somit nicht.

Das SRZ-Kundenprotokoll wird in Form des maschinenlesbaren XML-Formats mittels der Auftragsart HAC (Abholen Kundenprotokoll) bereitgestellt.¹

Die Deutsche Bundesbank dokumentiert in SRZ-Kundenprotokollen die folgenden Vorgänge:

- Übertragung der Auftragsdaten an das Banksystem (EBICS-Kommunikationsrechner)
- Ergebnis einer jeden Unterschriftenprüfung von Aufträgen des SRZ an das Banksystem
- Fehler bei der Dekomprimierung
- Gültigkeitsdauer der genutzten Schemaversion einer eingereichten pain-Nachricht
- Prüfung der Hashwerte des öffentlichen bankfachlichen Schlüssels bei erstmaliger Verwendung eines vorhergehenden öffentlichen Bankschlüssels

¹ Die Auftragsart HAC ist vorzugsweise zu verwenden. Auf Basis bilateraler Vereinbarung kann alternativ oder ergänzend das Kundenprotokoll im bisherigen Textformat mittels der Auftragsart PTK (vgl. Kapitel 4.2 des EBICS Implementation Guides vom 16. Mai 2011, basierend auf Version 2.5 der EBICS-Spezifikation) bereitgestellt werden.

SRZ-Anbindung

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

4.2.5 Verwendung von XML-Containern

Es ist immer ein XML-Container zu verwenden (mit 1 bis n pain-Nachrichten), dies wird in Nummer 9 (Delta-Vorgaben für SRZ zum SEPA-Zahlungsverkehr) bzw. Nummer 10 dieser Anlage (Delta-Vorgaben für SRZ für SCC-Karteneinzüge) beschrieben.

Im SRZ-Verfahren enthält eine pain-Nachricht genau einen Sammler (PmtInf-Block, Details siehe Nummern 9 und 10) mit maximal 100.000 Transaktionen.

Selektionskriterium für eine Weiterleitung der einzelnen pain-Nachricht nach Auflösung des Containers ist der BIC bzw. die IBAN des Auftraggeberkontos (kommt pro pain-Nachricht nur einmal vor, da nur ein Sammler erlaubt). Um eine Möglichkeit zur Überprüfung der unveränderten Weitergabe der pain-Nachricht zu haben, ist die Verwendung des im XML-Container vorgesehenen optionalen Hashwertes im SRZ-Verfahren verpflichtend.

4.2.6 Auftragsarten für das SRZ-Verfahren

Für das SRZ-Verfahren gelten die nachfolgend beschriebenen Auftragsarten.

4.2.6.1 SEPA-Format

Für SRZ gelten folgende Auftragsartenkennungen gemäß EBICS Anhang 2 mit den in Nummer 9 dieser Anlage angegebenen Formatspezifikationen:

Kennung	Text	Format
CCS (Customer Credit Trans- fer SRZ)	Senden von SEPA-Überweisungen in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.001.001.03 auf Grundlage der Version 3.1 (pain.001.001.03_GBIC_2) u. 3.0 (pain.001.001.03_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.001.003.03

SRZ-Anbindung

Kennung	Text	Format
CDS (Customer Direct Debit SRZ)	Senden von SEPA-Basis-Lastschriften (CORE) in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.008.001.02 auf Grundlage der Version 3.1 (pain.008.001.02_GBIC_2) u. 3.0 (pain.008.001.02_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.008.003.02
C2S (Customer B2B Direct Debit SRZ)	Senden von SEPA-Firmen-Lastschriften (B2B) in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.008.001.02 auf Grundlage der Version 3.1 (pain.008.001.02_GBIC_2) u. 3.0 (pain.008.001.02_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.008.003.02

Die vom SRZ eingereichte Sammeldatei wird nach Kunden aufgesplittet und unter Verwendung der folgenden Auftragsarten in das EBICS-System der Deutschen Bundesbank eingestellt.

EBICS-Auftragsart verwendet vom SRZ	Auftragsart zur Einstellung in die VEU
CCS	CCX (EBICS-interne Abbildung von über CCS eingereichten SEPA-Überweisungen bei Nutzung der VEU im SRZ-Verfahren)
CDS	CDX (EBICS-interne Abbildung von über CDS eingereichten SEPA-Basis-Lastschriften (CORE) bei Nutzung der VEU im SRZ-Verfahren)
C2S	C2X (EBICS-interne Abbildung von über C2S eingereichten SEPA-Firmen-Lastschriften bei Nutzung der VEU im SRZ-Verfahren)

Daneben nimmt die Deutsche Bundesbank vom SRZ pauschalautorisierte SEPA-Basislastschriften mit folgenden Auftragsartenkennungen entgegen:

SRZ-Anbindung

Kennung	Text	Format
XDS (bbk- spezifische Direct Debit SRZ)	Senden von vom Kunden pauschalautorisierten SEPA-Basis-Lastschriften (CORE) in einem Container durch SRZ	XML-Container container.nnn.001.02 mit 1-n pain.008.001.02 auf Grundlage der Version 3.1 (pain.008.001.02_GBIC_2) u. 3.0 (pain.008.001.02_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.008.003.02

4.2.6.2 SCC-Karteneinzüge

Für SRZ gelten folgende Auftragsartenkennungen gemäß EBICS Anhang 2 mit der in Nummer 10 dieser Anlage angegebenen Formatspezifikation:

Kennung	Text	Format
CK8 (Upload SEPA Cards Clearing Collection)	Senden von vom Kunden pauschal- autorisierten SCC-Karteneinzügen in einem Container durch SRZ	XML-Container scc.nnn.002.04 mit 1-n pain.008.002.04

SRZ-Anbindung

5 Änderung der Teilnehmerschlüssel mit automatischer Freischaltung

Wenn die vom EBICS-Teilnehmer eingesetzten 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.

Wenn die Transport-Unterschrift nicht erfolgreich geprüft werden konnte, wird wie unter Abschnitt VI Nummer 2. Absatz (2) der SRZ-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.

SRZ-Anbindung

6 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 4755 „Antrag auf EBICS-Kommunikation Service-Rechenzentrum (SRZ)“ 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 Auftragsart HPB abzuholen.

Bei stichtagsbezogener Einführung eines neuen öffentlichen Bankschlüssels wird der neue und der vorhergehende Bankschlüssel auf drei Monate befristet parallel unterstützt.

Bei jeder Aufnahme der Kommunikation 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.

SRZ-Anbindung

7 Sperrung der Teilnehmerschlüssel

Soweit der EBICS-Teilnehmer über gültige Sicherungsmedien verfügt, kann er seinen DFÜ-Zugang via EBICS sperren. Hierbei wird durch Senden einer Nachricht mit der 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 für das SRZ zeichnungsberechtigten Personen zu bestätigen.

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

SRZ-Anbindung

8 Testanforderungen

8.1 Grundsätzliches

Vor Verfahrensaufnahme ist durch einen erfolgreich absolvierten Zulassungs- und Conformance-Test 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 SRZ bietet sich bei diesem Test die Möglichkeit, die grundsätzlichen Verfahrensabläufe zu testen.

Es ist zu beachten, dass es sich bei den der Deutschen Bundesbank im Rahmen des Zulassungs- und Conformance-Tests übermittelten Testdaten um anonymisierte Echtdateien handeln soll, wobei das SRZ die Verantwortung für die Anonymisierung trägt. 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) 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).

SRZ-Anbindung

8.2 Testszzenarien

8.2.1 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 1: Test der Initialisierung der EBICS-Anbindung

8.2.2 Download Transaktionen

Testfall	Auftrag	Beschreibung
Test EBICS/D02	HAC	Abholung Kundenprotokolle im XML-Format nach Initialisierung

Tabelle 2: Test des Download von Transaktionen

8.2.3 Datenaustausch über die EBICS-Anbindung

Im Testschritt „Datenaustausch“ ist der erfolgreiche Datenaustausch über EBICS mittels XML-Container zu testen.

Basis für den Datenaustausch sind die unter den Nummer 9.2.1 und 10.2 beschriebenen Datenformate. Die individuell notwendigen Test-Stammdaten werden vom Kundentestzentrum mit den EBICS-Testteilnehmern abgestimmt.

SRZ-Anbindung

9 Delta-Vorgaben zum SEPA-Zahlungsverkehr

Die Standards für den SEPA-Zahlungsverkehr sind in Kapitel 2 (SEPA-Zahlungsverkehr) und Kapitel 9 (Container-Formate) der **Anlage 3 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen der Deutschen Kreditwirtschaft (Spezifikation der Datenformate)** spezifiziert. Die Version 3.1 der Anlage 3 des DFÜ-Abkommens (gültig ab 19.11.2017) ist auf der Internetseite www.ebics.de veröffentlicht. Es gelten folgende Abweichungen.

9.1 Grundlagen und Überblick

9.1.1 Verwendung von SEPA-Datenformaten im SRZ-Verfahren

Die SEPA-Datenformate basieren auf dem Standard ISO 20022 zur Definition von XML-basierten Nachrichten im Austausch zwischen Kunden und Zahlungsdienstleistern (ZDL). Durch den European Payments Council (EPC) wurden mittels der EPC Implementation Guidelines Belegungsrichtlinien für die ISO 20022-Formate festgelegt.

Diese Vorgaben für die zwischen Kunde und ZDL zu nutzenden SEPA-Datenformate wurden in eine konkrete Spezifikation überführt, welche Bestandteil des DFÜ-Abkommens (Anlage 3 des DFÜ-Abkommens, Kapitel 2) ist. Darüber hinaus ist in Kapitel 9 der Anlage 3 des DFÜ-Abkommens die optionale Bündelung mehrerer ISO-Nachrichten in einem XML-Container beschrieben.

Ziel dieser Delta-Vorgaben ist die Beschreibung der Besonderheiten, welche vom SRZ bei der Erstellung von Zahlungsdateien im SEPA-Datenformat zu berücksichtigen sind. Dabei wird nur auf die Abweichungen zur Spezifikation in der Anlage 3 des DFÜ-Abkommens, Kapitel 2 und 9, eingegangen. Die Abweichungen beschränken sich auf spezielle Belegungsvorgaben für einzelne Datenelemente sowie einer Einschränkung bei den möglichen Kardinalitäten. Somit genügt jede von SRZ zu erstellenden SEPA-Zahlungsdateien den allgemeinen Vorgaben der Anlage 3 des DFÜ-Abkommens, anders ausgedrückt: SEPA-Aufträge von SRZ bilden eine Untermenge (subset) der SEPA-Aufträge von Kunden im Allgemeinen. Insbesondere werden keine neuen, speziellen XML-Schemata für das SRZ-Verfahren definiert.

SRZ-Anbindung

9.1.2 Verwendete Version der Anlage 3 des DFÜ-Abkommens und Grobüberblick über das Delta

Diese Delta-Vorgaben nehmen Bezug auf die Anlage 3, Version 3.1, des DFÜ-Abkommens, deren Kapitel 2 und 9 in Nummer 9 dieser Anlage enthalten sind.

Es ergeben sich im Grobüberblick folgende Festlegungen für das SEPA-Datenformat im SRZ-Verfahren:

Festlegungen hinsichtlich Kapitel in Anlage 3 des DFÜ-Abkommens	Siehe Nummer in Delta-Vorgaben	Beschreibung
2.2.1, 2.2.2, 9.1	9.2.1	Auflieferung von SRZ-Aufträgen ausschließlich unter Verwendung des XML-Containers.
2.2.1.2 und 2.2.2.2	9.2.2	Beschränkung auf 1 Sammler, d. h. 1 PaymentInformation-Block je pain-Nachricht.
9.1.3	9.2.3	Verpflichtende Einstellung des Hashwertes der pain-Nachricht durch das SRZ in den XML-Container um Originalität des Auftrages überprüfen zu können.
2.2.1.4 und 2.2.2.4	9.2.4	Name und Kennung des SRZ werden in der Datenelementgruppe <InitiatingParty> hinterlegt.

9.2 Festlegungen

9.2.1 Verwendung des XML-Containers

Ein SRZ reicht in der Regel Zahlungsaufträge für verschiedene Mandanten des SRZ ein. Diese Mandanten unterhalten jeweils ein oder mehrere Girokonten bei der Deutschen Bundesbank.

Vor diesem Hintergrund ist es erforderlich, dass in einer pain-Nachricht nur Aufträge für eine Kontoverbindung enthalten sind, damit die einzelnen vom SRZ eingereichten pain-Nachrichten nur Aufträge eines Kunden (= Mandanten des SRZ) enthalten und unverändert der Deutschen Bundesbank zur Verfügung gestellt werden können.

Hieraus resultiert zum einen, dass je pain-Nachricht nur ein Sammler – d. h. nur ein Payment Information-Block enthalten ist (siehe Nummer 9.2.2 dieser Anlage) – und zum anderen bedeutet dies, dass dem SRZ die Möglichkeit geboten werden muss, mehrere pain-Nachrichten gesammelt zu übermitteln. Hierzu ist die in der Anlage 3 des DFÜ-Abkommens in Kapitel 9 spezifizierte XML-Containerstruktur mit folgenden EBICS-Auftragsarten zu verwenden.

SRZ-Anbindung

EBICS-Auftragsart	Text	Format
CCS (Customer Credit Transfer SRZ)	Senden von SEPA-Überweisungen in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.001.001.03 auf Grundlage der Version 3.1 (pain.001.001.03_GBIC_2) u. 3.0 (pain.001.001.03_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.001.003.03
CDS (Customer Direct Debit SRZ)	Senden von SEPA-Basis-Lastschriften (CORE) in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.008.001.02 auf Grundlage der Version 3.1 (pain.008.001.02_GBIC_2) u. 3.0 (pain.008.001.02_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.008.003.02
C2S (Customer B2B Direct Debit SRZ)	Senden von SEPA-Firmen-Lastschriften in einem Container durch SRZ zwecks Autorisierung mittels VEU durch Kunden	XML-Container container.nnn.001.02 mit 1-n pain.008.001.02 auf Grundlage der Version 3.1 (pain.008.001.02_GBIC_2) u. 3.0 (pain.008.001.02_GBIC_1 – gültig bis 16. Nov. 2018) der Anlage 3 DFÜ-Abkommen oder XML-Container container.nnn.003.02 mit 1-n Vorgängerversion pain.008.003.02

9.2.2 Beschränkung auf einen Sammler pro ISO-Nachricht

Wie bereits in Nummer 9.2.1 beschrieben, darf jede pain-Nachricht nur 1 Sammler – sprich PaymentInformation-Block – enthalten. Der Sammler muss mind. eine und darf bei der Deutschen Bundesbank maximal 100.000 Transaktionen enthalten.

SRZ-Anbindung

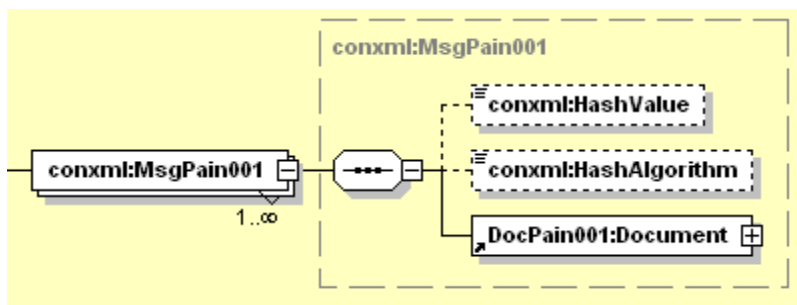
Abweichende Regel in Abschnitt 2.2.1.2 und 2.2.2.2 der Anlage 3 des DFÜ-Abkommens

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
GroupHeader	<GrpHdr>	[1..1]	siehe Anlage 3, Kapitel 2.2.1.3	-	-
PaymentInformation	<PmtInf>	[1..1]	siehe Anlage 3, Kapitel 2.2.1.6	-	Diese Datenelementgruppe darf nur 1x vorkommen.

9.2.3 Verpflichtende Einstellung des Hashwertes in den XML-Container

Um eine Möglichkeit zur Überprüfung der unveränderten Weitergabe der pain-Nachricht zu haben, ist die Verwendung des im XML-Container vorgesehenen optionalen Hashwertes im SRZ-Verfahren verpflichtend.

Abweichende Belegungsregeln in Abschnitt 9.1.3.3 der Anlage 3 des DFÜ-Abkommens



Diese Datenelementgruppe muss wie folgt durch das SRZ belegt werden:

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
HashValue	<HashValue>	[1..1]	Hashwert	conxml:HashSHA256	Zurzeit muss der Hashwert mit SHA 256 berechnet werden. Ggf. werden später weitere Hashverfahren zugelassen, dann ist der in diesem Feld eingetragene Hashwert mit dem Verfahren wie in <HashAlgorithm> errechnet worden. Im Rahmen des SRZ-Verfahrens ist die Angabe des Hashwertes verpflichtend.
HashAlgorithm	<HashAlgorithm>	[0..1]	verwendeter Hash-Algorithmus	conxml:HashAlgorithm	Zurzeit ist der Wert fix mit SHA256 zu belegen. Ggf. werden zu einem späteren Zeitpunkt weitere Hashverfahren zugelassen.

SRZ-Anbindung

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
Document	<Document>	[1..1]	siehe Anlage 3, Kapitel 2.2.1.1, 2.2.2.1, 2.2.3.1		Das Element entstammt nicht dem Container-Namensraum, sondern dem Namensraum der XML pain-Nachricht. Um zu vermeiden, dass jedes Element unterhalb von Document mit einem Präfix versehen werden muss, hat die Angabe des Namensraums im Document-Tag (siehe Beispiel) zu erfolgen.

Beispiel

```

<MsgPain001>
  <HashValue>D7A8FBB307D7809469CA9ABC0082E4F8D5651E46D3CDB762D02D0BF37C9E592
  </HashValue>
  <HashAlgorithm>SHA256</HashAlgorithm>
  <Document xmlns="urn:iso:std:iso:2002:tech:xsd:pain.001.001.03">
    <CstmrCdtTrfInitn>
      <!-- Inhalt der ersten pain-Nachricht -->
    </CstmrCdtTrfInitn>
  </Document>
</MsgPain001>

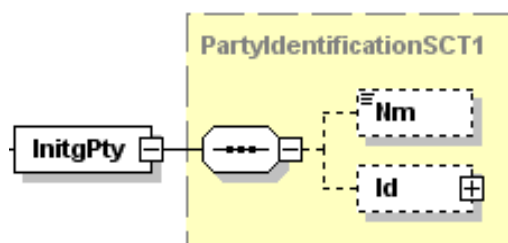
```

Für die Datenelementgruppe <MsgPain008> gelten dieselben Belegungsregeln wie für die Datenelementgruppe <MsgPain001>.

9.2.4 Hinterlegung der Kennung des SRZ

Die Initiating Party ist mit dem Namen und der Kennung des SRZ zu belegen.

Abweichende Belegungsregeln in Abschnitt 2.2.1.4 und 2.2.2.4 der Anlage 3 des DFÜ-Abkommens

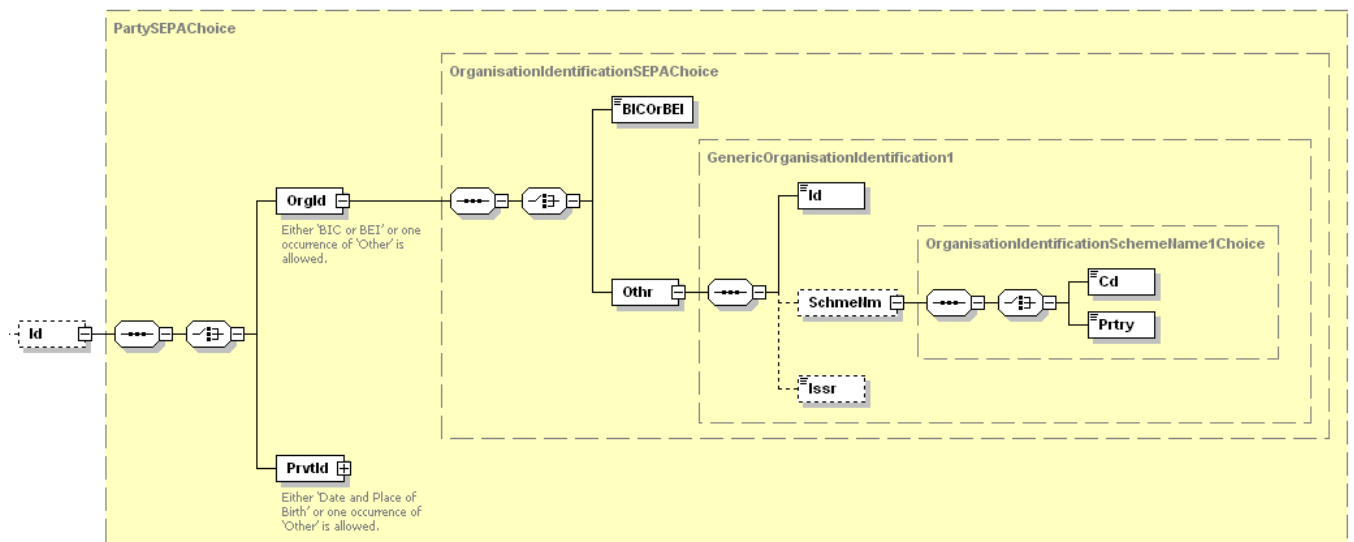


SRZ-Anbindung

Diese Datenelementgruppe muss wie folgt durch das SRZ belegt werden:

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
Name	<Nm>	[1..1]	Name	Max70Text	Muss mit der Bezeichnung des SRZ belegt werden
Identification	<Id>	[1..1]	siehe Anlage 3, Kapitel 2.2.1.5		Diese Datenelementgruppe muss belegt werden, Details s. nächste Tabelle

Abweichende Belegung der Identification der Initiating Party



Diese Datenelementgruppe muss wie folgt durch das SRZ belegt werden:

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
Organisatio- nidentification	<OrgId>	[1..1]	eindeutiger Identifikationscode einer Organisation	OrganisationIdentificationSEPAChoice	Es ist stets die Variante „Other“ zu belegen.
Other	<Othr>	[1..1]	Einheitliche und eindeutige Kennung, die einer Einrichtung zugeordnet ist.	GenericOrganisationIdentification1	
Identification	<Id>	[1..1]	Kennung Name oder Nummer zur Wiedererkennung einer Einheit	Max35Text	Muss in Abstimmung mit der Annahmestelle mit der 10-stelligen Kennung des SRZ belegt werden. Sofern die SRZ-Kennung

SRZ-Anbindung

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
					kürzer als 10-Stellen ist, ist die linksbündig eingestellte SRZ-Kennung bis auf 10 Stellen mit Leerzeichen aufzufüllen. Weitere Informationen können ab Position 11 eingestellt werden.
SchemeName	<SchmeNm>	[1..1]	Name des Schemas	Organisation-Identification-Scheme-Name1-Choice	
Proprietary	<Prty>	[1..1]	Name in Freitextform		Muss mit der Konstante SRZ belegt werden.
Issuer	<Issr>	[1..1]	Herausgeber der Kennung	Max35Text	Muss mit der Konstante DK belegt werden.

Beispiel

```

<InitgPty>
  <Nm>Name des SRZ</Nm>
  <Id>
    <OrgId>
      <Othr>
        <Id>DRTHG23425</Id>
        <!-- 10-stellige Kennung des SRZ -->
        <SchmeNm><Prtry>SRZ</Prtry></SchmeNm>
        <Issr>DK</Issr>
      </Othr>
    </OrgId>
  </Id>
</InitgPty>

```

9.2.5 Besonderheiten bei der Belegung und Einlieferung von SEPA-Überweisungen bei der Deutschen Bundesbank

Für die Belegung und Einlieferung der SEPA-Überweisung bei der Deutschen Bundesbank gelten die nachfolgenden Vorgaben der „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)“ nebst der dazugehörigen Anlage „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SEPA-Überweisungen“ (Technische Spezifikation SCT/sonstige Kontoinhaber ohne BLZ)“ entsprechend:

SRZ-Anbindung

	Verfahrensregeln SEPA-Überweisungen für sonstige Konto- inhaber ohne BLZ	Technische Spezifikation SCT/ sonstige Konto- inhaber ohne BLZ
Auftraggeberermittlung Belegung der Elemente <ul style="list-style-type: none"> • 'Debtor Account' <DbtrAcct><Id><IBAN> • 'Debtor Agent' <ul style="list-style-type: none"> - <DbtrAgt><FinInstnId><BIC> - <DbtrAgt><FinInstnId><Othr><Id> 		2.2.4
Angabe eines abweichenden Belastungskontos Belegung des Elements Ultimate Debtor <UltmtDbtr><Id><Orgld><Othr><Id> auf Sammler- /Transaktionsebene <i>Hinweis: Ein angegebenes abweichendes Belastungskonto hat keine Auswirkungen auf die fachliche Kontoprüfung in EBICS. Hierfür ist einzig die Angabe der IBAN im Debtor ausschlag- gebend.</i>		2.2.5
Gewünschtes Ausführungsdatum (Requested Execution Date) Belegung des Elements 'Requested Execution Date' <ReqdExctnDt>	4.1.1	2.2.7
Gewünschter Ausführungszeitpunkt Belegung des Elements 'Instruction Priority' <InstrPrty>	4.1.1 (4) i. V. m. 4.1.3 (4)	
Angabe des BIC des Zahlungsdienstleisters des Zah- lungsempfängers Belegung des Elements <CdtrAgt><FinInstnId><BIC>		2.2.8
Einlieferungsfrist <ul style="list-style-type: none"> • SEPA-Überweisungen • SEPA-Terminüberweisungen 	4.1.3 (3) 4.1.3 (4)	

Hinweis: Die Belegung der oben angegebenen Elemente sollte in Absprache mit dem Kunden erfolgen. Zudem sollte die Übertragung der Auftragsdaten über EBICS so rechtzeitig erfolgen, dass der Kunde die Auftragsdaten vor den von der Deutschen Bundesbank für das Zahlungsverfahren festgelegten Annahmeschlusszeiten mittels Verteilter Elektronischer Unterschrift (VEU) autorisieren kann.

9.2.6 Besonderheiten bei der Belegung und Einlieferung von SEPA-Lastschriften bei der Deutschen Bundesbank

Für die Belegung und Einlieferung von SEPA-Lastschriften gelten die nachfolgenden Vorgaben der „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)“ nebst der dazugehörigen Anlage „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SEPA-Lastschriften“ (Technische Spezifikation SDD/sonstige Kontoinhaber ohne BLZ)“ entsprechend:

SRZ-Anbindung

	Verfahrensregeln SEPA-Lastschriften für sonstige Konto- inhaber ohne BLZ	Technische Spezifikation SDD/ sonstige Konto- inhaber ohne BLZ
Auftraggeberermittlung Belegung der Elemente <ul style="list-style-type: none"> • 'Creditor Account' <CdrAcct><Id><IBAN> • 'Creditor Agent' <ul style="list-style-type: none"> - <CdrAgt><FinInstnId><BIC> - <CdrAgt><FinInstnId><Othr><Id> 		2.2.4
Angabe eines abweichenden Gutschriftskontos Belegung des Elemente Ultimate Debtor <UltmtCdr><Id><OrgId><Othr><Id> auf Sammler- /Transaktionsebene <i>Hinweis: Ein angegebenes abweichendes Gutschriftskonto hat keine Auswirkungen auf die fachliche Kontoprüfung in EBICS. Hierfür ist einzig die Angabe der IBAN im Creditor aus- schlaggebend.</i>		2.2.5
Gewünschtes Fälligkeitsdatum (Requested Collection Date) Belegung des Elements 'Requested Collection Date' <ReqdColltnDt>	4.1.1	2.2.7
Angabe des BIC des Zahlungsdienstleisters des Zahlers Belegung des Elements <DbtrAgt><FinInstnId><BIC>		2.2.8
Einlieferungsfenster SEPA-Lastschriften	4.1.3 (3)	

Hinweis: Die Belegung der oben angegebenen Elemente sollte in Absprache mit dem Kunden erfolgen. Zudem sollte die Übertragung der Auftragsdaten über EBICS so rechtzeitig erfolgen, dass der Kunde die Auftragsdaten vor den von der Deutschen Bundesbank für das Zahlungsverfahren festgelegten Annahmeschlusszeiten mittels Verteilter Elektronischer Unterschrift (VEU) autorisieren kann.

9.3 Beispiel

```
<?xml version="1.0" encoding="UTF-8"?>
<conxml xmlns="urn:conxml:xsd:container.nnn.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:conxml:xsd:container.nnn.001.02 contain-
ner.nnn.001.02.xsd">
<ContainerId>
  <SenderId>Kunden-ID des SRZ</SenderId>
  <IdType>EBIC</IdType>
  <TimeStamp>115500000</TimeStamp>
</ContainerId>
<CreDtTm>2016-11-22T11:55:00.000Z</CreDtTm>

<MsgPain001>
<!-- Dieser Block kann beliebig wiederholt werden. Jeder Block enthält
genau einen Sammelauftrag, d.h. genau einen PmtInf-Block.
```

SRZ-Anbindung

Verschiedene Blöcke können aus Sammelaufträgen für 1 oder mehrere Mandanten des SRZ bestehen.

Die verschiedenen Blöcke können Aufträge für 1 oder mehrere ZDL enthalten -->

```
<HashValue>D7A8FBB307D7809469CA9ABC0082E4F8D5651E46D3CDB762D02D0BF37C9E592</HashValue>
  <!-- Wert ist nicht korrekt -->
  <HashAlgorithm>SHA256</HashAlgorithm>
  <!-- Der Hashwert wird über die gesamte enthaltene pain-Nachricht --!>
  <!-- einschließlich des öffnenden und schließenden --!>
  <!-- <Document>-Tag gebildet. Das Dokument wird entsprechend Canonical--!>
  <!--XML, Version 1.0 (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) --!>
  <!-- kanonisiert. Als Hash-Algorithmus wird SHA-256 verwendet. --!>
  <!-- Der Hashwert wird hexadezimal in das <HashValue>-Tag eingetragen,--!>
  <!--für die hexadezimalen Ziffern A bis F werden Großbuchstaben --!>
  <!--verwendet. Bei der Verwendung des XML-Containers im Rahmen des --!>
  <!--SRZ-Verfahrens ist die Angabe des Hashwertes verpflichtend. -->
  <Document xmlns="urn:iso:std:iso:2002:tech:xsd:pain.001.001.03">
    <CstmrCdtTrfInitn>
      <GrpHdr>
        <MsgId>Message-ID-4711</MsgId>
        <CreDtTm>2016-11-22T11:54:00.000Z</CreDtTm>
        <NbOfTxes>2</NbOfTxes>
        <InitgPty>
          <Nm>Name des SRZ</Nm>
          <Id>
            <OrgId>
              <Othr>
                <Id>DRTHG23425</Id> <!-- 10-stellige Kennung des SRZ-->
                <SchmeNm><Prtry>SRZ</Prtry></SchmeNm>
                <Issr>DK</Issr>
              </Othr>
            </OrgId>
          </Id>
        </InitgPty>
      </GrpHdr>
      <PmtInf>
        <!-- Im SRZ-Fall ist nur 1 Wiederholung des PmtInf-Blockes zulässig -->
        <PmtInfId>Payment-Information-ID-4710</PmtInfId>
        <PmtMtd>TRF</PmtMtd>
        <PmtTpInf>
          <SvcLvl>
            <Cd>SEPA</Cd>
          </SvcLvl>
        </PmtTpInf>
        <ReqdExctnDt>2016-11-25</ReqdExctnDt>
        <Dbtr>
          <Nm>Debtor Name</Nm>
        </Dbtr>
        <DbtrAcct>
          <Id>
            <IBAN>DE44390500002645625322</IBAN>
          </Id>
        </DbtrAcct>
        <DbtrAgt>
          <FinInstnId>
```

SRZ-Anbindung

```
<BIC>AACSDE33XXX</BIC>
<!-- Mandant 1 des SRZ hat Kontoverbindung bei der Spk. Aachen -->
</FinInstnId>
</DbtrAgt>
<ChrgBr>SLEV</ChrgBr>
<CdtTrfTxInf>
  <PmtId>
    <InstrId>SRZID4711</InstrId>
    <EndToEndId>Mandant-ID 1234</EndToEndId>
  </PmtId>
  <Amt>
    <InstdAmt Ccy="EUR">6543.14</InstdAmt>
  </Amt>
  <CdtrAgt>
    <FinInstnId>
      <BIC>SPUEDE2UXXX</BIC>
    </FinInstnId>
  </CdtrAgt>
  <Cdtr>
    <Nm>Creditor Name</Nm>
  </Cdtr>
  <CdtrAcct>
    <Id>
      <IBAN>DE21500500009876543210</IBAN>
    </Id>
  </CdtrAcct>
  <RmtInf>
    <Ustrd>Unstructured Remittance Information</Ustrd>
  </RmtInf>
</CdtTrfTxInf>
<CdtTrfTxInf>
  <PmtId>
    <InstrId>SRZID4712</InstrId>
    <EndToEndId>Originator- ID 1235</EndToEndId>
  </PmtId>
  <Amt>
    <InstdAmt Ccy="EUR">112.72</InstdAmt>
  </Amt>
  <CdtrAgt>
    <FinInstnId>
      <BIC>SPUEDE2UXXX</BIC>
    </FinInstnId>
  </CdtrAgt>
  <Cdtr>
    <Nm>Other Creditor Name</Nm>
  </Cdtr>
  <CdtrAcct>
    <Id>
      <IBAN>DE21500500001234567897</IBAN>
    </Id>
  </CdtrAcct>
  <RmtInf>
    <Ustrd>Unstructured Remittance Information</Ustrd>
  </RmtInf>
</CdtTrfTxInf>
</PmtInf>
</CstmrCdtTrfInitn>
</Document>
```

SRZ-Anbindung

```
</MsgPain001>

<MsgPain001>
  <HashVal-
Val-
ue>D7A8FBB307D7809469CA9ABC0082E4F8D5651E46D3CDB762D02D0BF37C9E592</HashVa
lue>
    <!-- Wert ist nicht korrekt -->
    <HashAlgorithm>SHA256</HashAlgorithm>
<!-- Die Angabe des Hashwertes ist im SRZ-Verfahren verpflichtend. -->
    <Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.03">
      <CstmrCdtTrfInitn>
        <GrpHdr>
          <MsgId>Message-ID-4711</MsgId>
          <CreDtTm>2016-11-22T11:54:10.000Z</CreDtTm>
          <NbOfTxes>2</NbOfTxes>
          <InitgPty>
            <Nm>Name des SRZ</Nm>
            <Id>
              <OrgId>
<Othr>
          <Id>DRTHG23425</Id>          <!-- 10-stellige Kennung desSRZ -->
          <SchmeNm><Prtry>SRZ</Prtry></SchmeNm>
            <Issr>DK</Issr>
          </Othr>
        </OrgId>
      </Id>
    </InitgPty>
  </GrpHdr>
  <PmtInf>
<!-- Im SRZ-Fall ist nur 1 Wiederholung des PmtInf-Blockes zulässig -->
    <PmtInfId>Payment-Information-ID-4711</PmtInfId>
    <PmtMtd>TRF</PmtMtd>
    <PmtTpInf>
      <SvcLvl>
        <Cd>SEPA</Cd>
      </SvcLvl>
    </PmtTpInf>
    <ReqdExctnDt>2016-11-25</ReqdExctnDt>
    <Dbtr>
      <Nm>Debtor Name</Nm>
    </Dbtr>
    <DbtrAcct>
      <Id>
        <IBAN>DE87200500001234567890</IBAN>
      </Id>
    </DbtrAcct>
    <DbtrAgt>
      <FinInstnId>
        <BIC>NOLADE2H</BIC>
<!-- Mandant 2 des SRZ hat Kontoverbindung bei der NORD/LB -->
      </FinInstnId>
    </DbtrAgt>
    <ChrgBr>SLEV</ChrgBr>
    <CdtTrfTxInf>
      <PmtId>
        <InstrId>SRZID4713</InstrId>
        <EndToEndId>Originator-ID 2234</EndToEndId>
```


SRZ-Anbindung

```
</PmtId>
<Amt>
  <InstdAmt Ccy="EUR">6543.14</InstdAmt>
</Amt>
<CdtrAgt>
  <FinInstnId>
    <BIC>SPUEDE2UXXX</BIC>
  </FinInstnId>
</CdtrAgt>
<Cdtr>
  <Nm>Creditor Name</Nm>
</Cdtr>
<CdtrAcct>
  <Id>
    <IBAN>DE21500500009876543210</IBAN>
  </Id>
</CdtrAcct>
<RmtInf>
  <Ustrd>Unstructured Remittance Information</Ustrd>
</RmtInf>
</CdtTrfTxInf>
<CdtTrfTxInf>
  <PmtId>
    <InstrId>SRZID4714</InstrId>
    <EndToEndId>Originator- ID 2235</EndToEndId>
  </PmtId>
  <Amt>
    <InstdAmt Ccy="EUR">112.72</InstdAmt>
  </Amt>
  <CdtrAgt>
    <FinInstnId>
      <BIC>SPUEDE2UXXX</BIC>
    </FinInstnId>
  </CdtrAgt>
  <Cdtr>
    <Nm>Other Creditor Name</Nm>
  </Cdtr>
  <CdtrAcct>
    <Id>
      <IBAN>DE21500500001234567897</IBAN>
    </Id>
  </CdtrAcct>
  <RmtInf>
    <Ustrd>Unstructured Remittance Information</Ustrd>
  </RmtInf>
</CdtTrfTxInf>
</PmtInf>
</CstmrCdtTrfInitn>
</Document>
</MsgPain001>

</conxml>
```

SRZ-Anbindung

9.4 Kontrollmaßnahmen

Die durch die SEPA-XML-Schemas der Deutschen Kreditwirtschaft in der jeweils geltenden Version vorgegebenen Strukturen werden durch das SRZ mit geeigneten Mitteln geprüft, z. B. durch den Einsatz von Parsern.

Darüber hinaus sind folgende Prüfungen durchzuführen:

- Ausführungsdatum, Fälligkeitsdatum: Die erforderlichen Annahmeschlusszeiten für die fristgemäße Ausführung der Aufträge müssen eingehalten werden.
- IBAN und ggf. Gläubiger-ID: Korrektheit von Prüfzahl und Länderkennzeichen sowie der länderspezifischen Länge
- BIC (sofern vorhanden): Existenz
- Betragssumme (Datenelement ControlSum) und Anzahl der Transaktionen (Datenelement NumberOfTransactions) ist korrekt
- Korrektheit des Hashwertes je pain-Nachricht aus dem XML-Container
- Die in das Datenelement InitiatingParty / Identification / OrganisationIdentification / Other / Identification eingestellte Kennung des SRZ muss der Deutschen Bundesbank bekannt sein.

SRZ-Anbindung

10 Delta-Vorgaben für SCC-Karteneinzüge

10.1 Grundlagen und Überblick

10.1.1 Verwendung von SCC-Datenformaten im SRZ-Verfahren

Die DK wickelt folgende aus ihren Kartenzahlungssystemen resultierenden Zahlungstransaktionen im XML-Format ab:

- Kartenzahlungen am POS im Rahmen des electronic cash-Systems (girocard-Karten sowie EAPS-Karten),
- Geldautomaten-Verfügungen für girocard-Karten und fremde Karten,
- Einzüge im Rahmen des GeldKarte-Systems,
- Laden von Mobilfunkkonten am Geldautomaten (POA), sowie
- Abwicklung von Kartenzahlungen über Cobrands zwischen Übergabestelle und Kartenherausgeber

Hierbei werden für die ISO 20022-Nachrichtentypen pain.008 (Einreichung) und pain.007 (Korrektur) die XML-Schemadateien gemäß SCC-Spezifikation in der Version 2.0 der Berlin Group genutzt, vgl. <http://www.berlin-group.org/iso20022-sepa-card-clearing>.

Ziel dieser Vorgaben ist die Beschreibung der Besonderheiten, welche von SRZ bei der Erstellung von Zahlungsdateien im SCC-Datenformat zu berücksichtigen sind. Dabei wird nur auf folgende Ergänzungen zu den DK-Spezifikationen eingegangen:

1. Einreichen von Umsätzen im SCC-Format, Ergänzung zum Technischen Anhang zum Vertrag über die Zulassung als Netzbetreiber im electronic cash-System der deutschen Kreditwirtschaft, 15.08.2016
2. Verrechnung der Verfügungsbeträge und Entgelte im SCC-Format, Anlage 7 zur Geldautomatenvereinbarung 2015, 15.03.2015
3. SEPA-Zahlungsverkehrsnachrichten für das Zahlungssystem GeldKarte, Belegungsrichtlinie Einreicherschnittstelle und Interbanken-Schnittstelle, Version 1.2 vom 09.09.2015

10.1.2 Grundlegende Festlegungen zu den Vorgaben

Um die bestehenden Abläufe im SRZ-Verfahren nutzen zu können, wird ein XML-Container zur Einreichung mehrerer pain.008-Nachrichten benötigt. Da das SCC-Format pain.008 auf separaten, von den SEPA-Zahlverfahren abweichenden XML-Schemadateien basiert, kann

SRZ-Anbindung

der bestehende XML-Container gemäß Kapitel 9 der Anlage 3 des DFÜ-Abkommens der DK nicht verwendet werden.

Deshalb ist ein spezieller XML-Container für die SCC-Formate zu verwenden, welcher in Nummer 10.2 beschrieben wird.

Nummer 10.4 enthält die Kontrollmaßnahmen, welche von einem SRZ vor Einreichung von SCC-Transaktionen durchzuführen sind.

10.2 Festlegungen zum XML-Container

Ein Netzbetreiber bzw. SRZ reicht in der Regel Zahlungsaufträge für verschiedene Händler (oder GA-Betreiber) ein. Diese Mandanten haben jeweils eine oder mehrere Kontoverbindungen, welche von einem oder mehreren ZDL geführt werden.

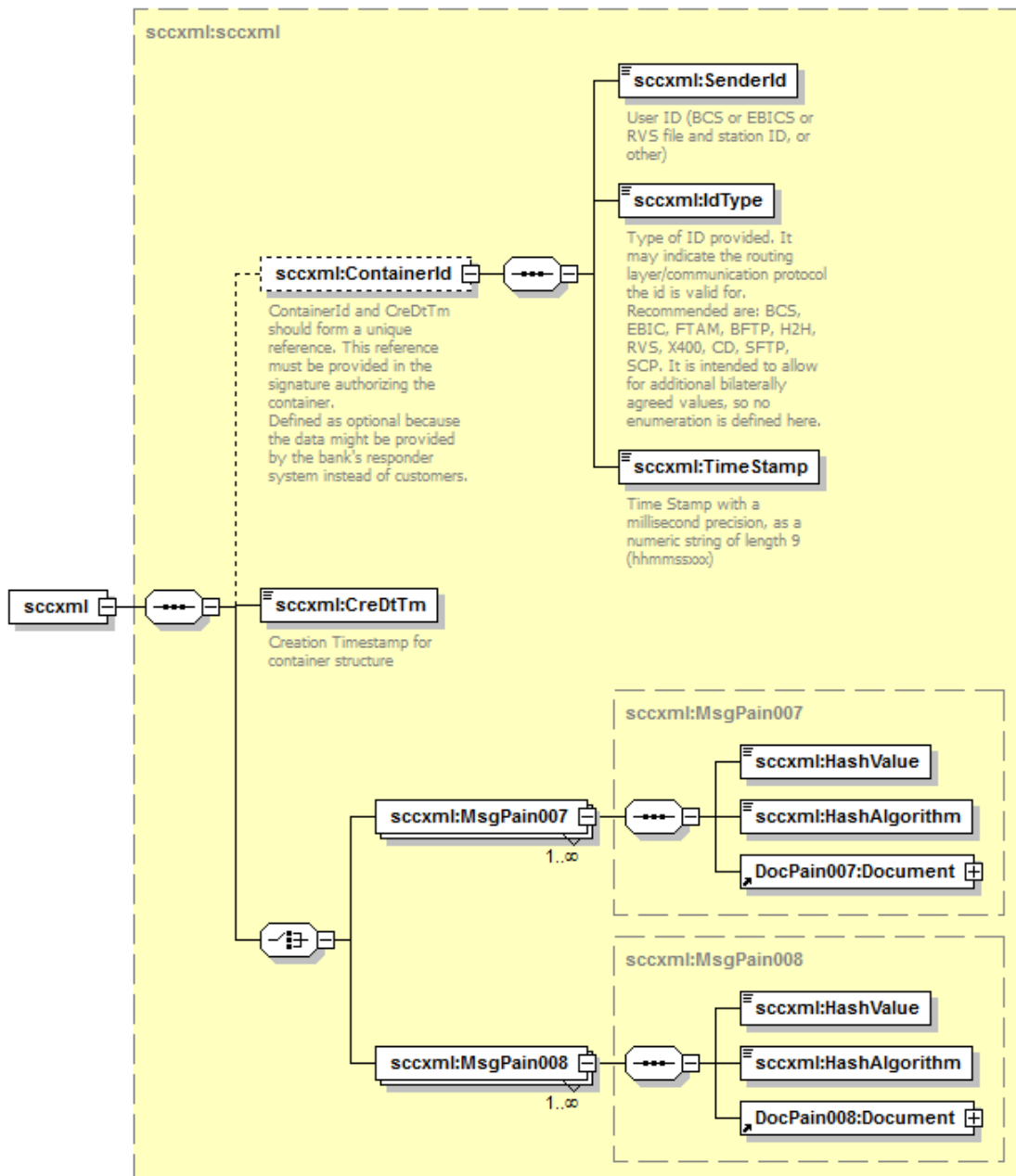
Vor diesem Hintergrund ist es erforderlich, dass in einer pain-Nachricht nur Aufträge für eine Kontoverbindung enthalten sind, damit die einzelnen vom SRZ eingereichten pain-Nachrichten nur Aufträge eines Kunden (= Mandanten des SRZ) enthalten und unverändert der Deutschen Bundesbank zur Verfügung gestellt werden können.

Hieraus resultiert zum einen, dass je pain-Nachricht nur ein Sammler – d. h. nur ein Payment Information-Block – enthalten ist.² Der Sammler muss mind. eine und darf maximal 100.000 Transaktionen enthalten. Zum anderen bedeutet dies, dass dem SRZ die Möglichkeit geboten werden muss, mehrere pain-Nachrichten gesammelt zu übermitteln. Hierzu ist die in der Anlage 3 des DFÜ-Abkommens in Kapitel 9 spezifizierte XML-Containerstruktur mit folgenden EBICS-Auftragsart zu verwenden.

EBICS-Auftragsart	Text	Format
CK8 (Upload SEPA Card Clearing Collection)	Senden von vom Kunden pauschalautorisierten SCC-Karteneinzügen in einem Container durch ein SRZ	XML-Container scc.nnn.002.04 mit pain.008.002.04

² Dies ist bereits unter Nummer 4.2.5 festgelegt worden.

SRZ-Anbindung



Definition

Container für SCC-Nachrichten

XML-Tag

<sccxml>

Kardinalität

[1..1]

SRZ-Anbindung

Regeln

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
ContainerId	<ContainerId>	[0..1]			
SenderId	<SenderId>	[1..1]	Identifikation des Absenders	Max22 Text	User-ID (z. B. EBICS)
IdentificationType	<IdType>	[1..1]	Art der Identifikation	Max4 Text	Art der gelieferten ID (z. B. EBICS)
TimeStamp	<TimeStamp>	[1..1]	Uhrzeit	DecimalTime	TimeStamp mit der Präzision einer Millisekunde, als numerischer String mit einer Länge von 9 (hhmmssxxx)
CreationDateTime	<CreDtTm>	[1..1]	Datum und Zeit der Erstellung des Containers.	ISODateTime	Erstellungszeitstempel für die Containerstruktur
MessagePain008	<MsgPain008>	[1..unbounded]			Auswahl des jeweiligen XML-Tag. Die maximale Anzahl soll 9.999.999 sein. Die Spezifikation „unbounded“ erfolgt aus technischen Gründen.
HashValue	<HashValue>	[1..1]	Hashwert	sccxml: Hash SHA256	Zurzeit muss der Hashwert mit SHA 256 berechnet werden. Die Berechnung des Hashwertes erfolgt gemäß Kap. 9.1.1 der Anlage 3 des DFÜ-Abkommens der DK. Im Rahmen des SRZ-Verfahrens ist die Angabe des Hashwertes verpflichtend.
HashAlgorithm	<HashAlgorithm>	[1..1]	verwendeter Hash-Algorithmus	sccxml: Hash Algorithm	Zurzeit ist der Wert fix mit SHA256 zu belegen. Ggf. werden zu einem späteren Zeitpunkt weitere Hashverfahren zugelassen.

SRZ-Anbindung

Name	XML-Tag	Kardinalität	Definition	Typ	Regeln
Document	<Document >	[1..1]	s. Dokumente referenziert in Kap. 1.1: a) Kap. 3.2 b) Kap. 3 c) Kap. 2.2.1		Das Element entstammt nicht dem Container-Namensraum, sondern dem Namensraum der SCC-Nachricht. Um zu vermeiden, dass jedes Element unterhalb von Document mit einem Präfix versehen werden muss, hat die Angabe des Namensraums im Document-Tag zu erfolgen.

10.3 Besonderheiten bei der Belegung und Einlieferung von SCC-Karteneinzügen bei der Deutschen Bundesbank

Für die Belegung und Einlieferung gelten die nachstehenden Vorgaben der „Verfahrensregeln der Deutschen Bundesbank für sonstige Kontoinhaber ohne Bankleitzahl zur Abwicklung von SCC-Karteneinzügen per Datenfernübertragung (DFÜ) (Verfahrensregeln SCC-Karteineinzüge/sonstige Kontoinhaber ohne BLZ)“ nebst der dazugehörigen Anlage „Technische Spezifikationen der Deutschen Bundesbank für die Abwicklung von SCC-Karteneinzügen“ (Technische Spezifikation SCC-Karteneinzüge/sonstige Kontoinhaber ohne BLZ)“ entsprechend:

	Verfahrensregeln SCC-Karteneinzüge für sonstige Kontoinhaber ohne BLZ	Technische Spezifikation SCC- Karteneinzüge / sonstige Kontoinhaber ohne BLZ
Auftraggeberermittlung Belegung der Elemente <ul style="list-style-type: none"> • 'Creditor Account' <CdtrAcct><Id><IBAN> • 'Creditor Agent' <ul style="list-style-type: none"> - <CdtrAgt><FinInstnId><BIC> - <CdtrAgt><FinInstnId><Othr><Id> 		2.2.4
Angabe eines abweichenden Gutschriftskontos Belegung des Elemente Ultimate Debtor <UltmtCdtr><Id><OrgId><Othr><Id> auf Sammler- /Transaktionsebene <i>Hinweis: Ein angegebenes abweichendes Gutschriftskonto hat keine Auswirkungen auf die fachliche Kontoprüfung in EBICS. Hierfür ist einzig die Angabe der IBAN im Creditor ausschlaggebend.</i>		2.2.5
Gewünschtes Fälligkeitsdatum (Requested Collection Date) Belegung des Elements 'Requested Collection Date' <Reqd-ColltnDt>	4.1.1	2.2.7
Einlieferungsfenster SCC-Karteneinzüge	4.1.3 (3)	

SRZ-Anbindung

Hinweis: Die Belegung der oben angegebenen Elemente sollte in Ansprache mit dem Kunden erfolgen.

10.4 Kontrollmaßnahmen

Die folgenden Plausibilitäts- und Feldinhaltsprüfungen sind vom SRZ durchzuführen:

- Die durch die XML-Schemas der DK bzw. Berlin Group vorgegebenen Strukturen werden mit geeigneten Mitteln geprüft, z. B. durch den Einsatz von Parsern.
- Fälligkeitsdatum (RequestedCollectionDate): Die erforderlichen Annahmeschlusszeiten für die fristgemäße Ausführung der Aufträge müssen eingehalten werden.
- IBAN und Gläubiger-ID: Korrektheit von Prüfzahl und Länderkennzeichen sowie der länderspezifischen Länge
- BIC (sofern vorhanden): Existenz
- Betragssumme (Datenelement ControlSum) und Anzahl der Transaktionen (Datenelement NumberOfTransactions) ist korrekt
- Korrektheit des Hashwertes je pain-Nachricht aus dem XML-Container
- Die in das Datenelement InitiatingParty / Identification / OrganisationIdentification / Other / Identification eingestellte Kennung des SRZ muss der Deutschen Bundesbank bekannt sein.