# Swiss Market Practice Guidelines EBICS

## EBICS 3.0

### Empfehlungen für die Umsetzung des EBICS-Standards

Version 1.1, gültig ab 15 November 2021

# Revisionsnachweis

Nachfolgend werden alle in diesem Dokument durchgeführten Änderungen mit Versionsangabe, Änderungsdatum, kurzer Änderungsbeschreibung und dem Gültig ab-Datum aufgelistet.

| Version | Datum | Änderungsbeschreibung | Gültig ab: |
|---|---|---|---|
| 1.1 | 29.10.2021 | Überarbeitung des Kapitels 6.1 «Initialisierung mit Schlüsselpaaren» bezüglich X.509-Zertifikaten | 15.11.2021 |
| 1.0 | 01.06.2020 | Erstausgabe | 15.11.2021 |

*Tabelle 1: Revisionsnachweis*

Die aktuellste Version dieses Dokuments kann von der Internetseite von SIX Interbank Clearing an der Adresse www.ebics.ch werden.

Bitte richten Sie sämtliche Anregungen, Korrekturen und Verbesserungsvorschläge zu diesem Dokument ausschliesslich an:

**SIX Interbank Clearing AG**
Hardturmstrasse 201
CH-8005 Zürich
E-Mail: billing-payments.pm@six-group.com
www.six-group.com

# Allgemeine Hinweise

SIX Interbank Clearing behält sich vor, dieses Dokument bei Bedarf jederzeit ohne vorherige Benachrichtigung zu ändern.



Das Dokument ist mit grösster Sorgfalt erstellt worden, doch können Fehler und Ungenauigkeiten nicht vollständig ausgeschlossen werden. SIX Interbank Clearing kann für Fehler in diesem Dokument und deren Folgen weder eine juristische Verantwortung noch irgendwelche Haftung übernehmen.

Aus Gründen der besseren Lesbarkeit wird, wo immer möglich, auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen sind als geschlechtsneutral zu betrachten.

Sollten Sie allfällige Fehler in diesem Dokument feststellen oder Verbesserungs-vorschläge haben, sind wir Ihnen dankbar für Ihre Rückmeldung per E-Mail an **billing-payments.pm@six-group.com**.

# Inhaltsverzeichnis

# Tabellenverzeichnis



# Abbildungsverzeichnis

# 1 Einleitung

Im Auftrag des PaCoS (Payments Committee Switzerland) erarbeitet die EBICS-Arbeitsgruppe die Schweizer Empfehlungen für die Umsetzung des EBICS-Standards für den Finanzplatz Schweiz. Es handelt sich hierbei um eine Dokumentation der von den Finanzinstituten für den Finanzplatz Schweiz genutzten EBICS Konfigurations-Einstellungen und Parametern. Das Dokument soll Softwarepartner und Nutzer eine Hilfestellung bieten und gibt diesbezüglich Empfehlungen im Sinne einer «Best Practice». Der Einsatz von EBICS ist für die Institute in der Schweiz optional.

Mit dem EBICS-Standard ist im europäischen Raum ein Industrie-Standard für die Finanzwirtschaft entstanden, der sich auch branchenübergreifend etabliert hat. In Deutschland ist die Unterstützung dieses Standards für Finanzinstitute seit Januar 2008 verpflichtend.

Durch die deutsch-französische EBICS-Gesellschaft, die im Juni 2010 gegründet wurde, findet dieser Standard in der Version ab 2.4 eine weitere Verbreitung durch die gemeinsame Anwendung in Deutschland und Frankreich. Insbesondere die Erstellung gemeinsamer Implementation Guidelines führt zu einer stärkeren Verbreitung des Standards.

## 1.1 Zweck des Dokuments und Zielgruppe

Das vorliegende Dokument dient als Ergänzung zu den von der EBICS-Gesellschaft veröffentlichten Dokumenten (siehe Referenzen [1] – [5]) und richtet sich primär an Softwareentwickler und Systemadministratoren.

Es soll die spezifischen Konventionen des Schweizer Finanzplatzes bei der Verwendung von EBICS dokumentieren.

## 1.2 Abgrenzung

Dieses Dokument beschreibt die Anwendung des EBICS-Standards in der Schweiz.

Da der EBICS-Standard in einigen Punkten unterschiedliche Implementierungsmöglichkeiten vorsieht, hat sich der Finanzplatz Schweiz darauf verständigt, die Umsetzungsmöglichkeiten abzustimmen und einheitlich zu nutzen.

Das Dokument beschreibt nur diese abgestimmten Umsetzungsentscheide.

Finanzinstitute können darüber hinaus weitere im Standard vorgesehene Varianten unterstützen, welche in eigenen Dokumenten eines Finanzinstituts geregelt werden.

## 1.3 Referenzdokumente

| Ref | Dokument | Titel | Quelle |
|---|---|---|---|
| | Basisdokumente | | |
| [1] | 2017-03-29-EBICS_V_3.0-FinalVersion.pdf | Specification EBICS | EBICS |
| [2] | 2017-03-29-EBICS Common IG basierend EBICS 3.0.pdf | Common Implementation Guide EBICS 3.0 | EBICS |
| [3] | EBICS 3.0 schema H005FinalVersion07-08-2017.zip | EBICS 3.0-Schemadateien (.xsd) mit Typen, Auftragsarten, Datenstrukturen und Funktionen | EBICS |
| [4] | 2017-03-29-EBICS Common IG basierend EBICS 3.0.pdf | Common Implementation Guide EBICS 3.0 | EBICS |
| [5] | Sicherheitskonzept EBICS | Auf Anfrage erhältlich bei info@ebics.de | EBICS |
| | Zusatzdokumente | | |
| [6] | EBICS Version 3.0 FinalDE-29-03-2017.pdf | Anlage 1 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäss DFÜ-Abkommen<br>«Spezifikation für die EBICS-Anbindung» Version 3.0 | DK |
| [7] | EBICS_Anhang_TransportLayer SecurityDE-29-03-2017.pdf | EBICS Anhang “Transport Layer Security” | DK |
| [8] | 2019-07-04-Mapping_EBICS-BTF-AA-Sortiert_wie_Anlage_3_zzgl_SonstigerThemen.pdf | Mapping_EBICS-BTF-AA (Deutschland) | DK |
| [9] | 20180808113947EBICS3.0 aide a la migration V1.1.pdf | Mapping_EBICS-BTF-FileFormat-Parameter (Frankreich) | CFONB |
| [10] | EBICS_BTF_Parameter_CH.pdf | BTF Parameter CH | SIX |

*Tabelle 2: Referenzdokumente*

## 1.4 Links zu entsprechenden Internetseiten

| Organisation | Link |
|---|---|
| CFONB | www.cfonb.org |
| DK (ZKA) | www.ebics.de (deutsch) |
| EBICS | www.ebics.org (englisch) |
| SIX (SIX Interbank Clearing) | www.iso-payments.ch<br>www.paymentstandards.ch<br>www.ebics.ch |

*Tabelle 3: Links zu Internetseiten*

# 2 EBICS-Anwendung für den Finanzplatz Schweiz

## 2.1 EBICS-Grundlagen

Die EBICS-Grundlagen sind ausführlich auf der Webseite der EBICS-Gesellschaft dokumentiert.

## 2.2 Anwendbare EBICS-Spezifikation

Dieses Dokument berücksichtigt die EBICS-Spezifikation in der Version 3.0 [1].

Ab November 2021 werden die Schweizer Finanzinstitute, welche EBICS anbieten, serverseitig die Version 3.0 unterstützen.

**Hinweis:**

Für den Einsatz von Version 3.0 ist eine Abstimmung mit dem jeweiligen Finanzinstitut erforderlich.

Bereits existierende Implementierungen in der Schweiz beruhen auf der EBICS-Spezifikation Version 2.5 und können unverändert von den Finanzinstituten angeboten werden. Es wird jedoch empfohlen, neue Kundenanbindungen auf Basis der Spezifikationen dieses Dokuments zu implementieren.

### 2.2.1 EBICS Timeline

Mit der Einführung von EBICS 3.0 läuft die verpflichtende Unterstützung der EBICS Version 2.4 aus und ist ab diesem Zeitpunkt keine offiziell vom Finanzplatz unterstützte Version mehr.

Die Version 2.5, auf der die überwiegende Anzahl der aktuellen EBICS Angebote der Finanzinstitute in der Schweiz beruht, wird vom Finanzplatz noch weitere 3 Jahre (bis Ende 2024) offiziell unterstützt.

**Hinweis:**

Für die Unterstützung der ISO 20022 Schema-Migration auf die Version 2019 ist die Verwendung von EBICS 3.0 erforderlich.

# 3 Sicherheit

## 3.1 Sicherheitsaspekte gemäss EBICS-Sicherheitskonzept

Das Protokoll ermöglicht bei korrekter Umsetzung die End-to-End-Sicherheit im Sinne eines sicheren Transportkanals.

Für die Gewährleistung der Sicherheit werden im EBICS-Sicherheitskonzept gewisse Bedingungen bei den Endpunkten – Finanzinstitut und Kunde – vorausgesetzt.

Für die Implementierung dieser Punkte sind sowohl das Finanzinstitut, der Softwarehersteller, der das EBICS-Protokoll in seiner Lösung abgebildet hat und der Kunde verantwortlich.

Für einen Einsatz auf dem Finanzplatz Schweiz sind die nachfolgenden Punkte aus dem EBICS-Sicherheitskonzept betreffend Kundensystem zwischen den jeweiligen Parteien vor einem Einsatz vertraglich zu regeln.

**In der Verantwortung des Kunden liegen:**

- Die internen Kommunikationswege für unverschlüsselte bankfachliche Nutzdaten und unverschlüsselte EUs sind gegen Abhören und Manipulation geschützt.
- Die internen Kommunikationswege für EBICS-Nachrichten sind gegen Abhören und Manipulation gesichert.
- Der Schutz der Kundensoftware und der internen Kommunikationswege liegt in der alleinigen Verantwortung des Kunden und ist kundenindividuell gelöst.

**In der Verantwortung des Softwareherstellers liegen:**

- Die privaten Teilnehmerschlüssel sind gegen unautorisiertes Auslesen und Verändern geschützt.
- Die öffentlichen Schlüssel der Bank sind gegen unautorisiertes Verändern geschützt.
- Die geheimen symmetrischen Schlüssel sind gegen unautorisiertes Auslesen und Verändern geschützt.
- Das Zertifikat, das als Vertrauensanker bei der Prüfung des TLS-Zertifikats des Finanzinstituts verwendet wird, ist gegen unautorisiertes Verändern geschützt.
- Die Kundensoftware ist gegen Manipulationen gesichert, die den Teilnehmer über den Ablauf von EBICS-Transaktionen täuschen könnten.

**In der Verantwortung des Finanzinstituts liegt:**

- Richtlinien für die sichere Speicherung der privaten/öffentlichen Schlüssel sind Bestandteil der Kundenbedingungen der Finanzinstitute.

## 3.2 TLS-Version und Cypher

Es ist zu berücksichtigen, dass zur sicheren Dateiübertragung mindestens die TLS-Version 1.2 verpflichtend zu verwenden ist [7].

## 3.3 Elektronische Unterschrift (EU)

In der Schweiz erfolgt die Freigabe von Aufträgen, die über eine Direkt-Einlieferungsschnittstelle übermittelt wurden, in der Regel mittels Einzelunterschrift, wobei diese in der Mehrzahl eine Firma repräsentiert und nicht eine Einzelperson. Dieses Vorgehen basiert darauf, dass solche Aufträge aus einer gesicherten Umgebung des Kunden übermittelt werden, ein möglichst hoher Automationsgrad angestrebt wird und die personenbezogenen Unterschriften im Vorfeld der Übermittlung von einer Kundensoftware geprüft worden sind (z.B. im ERP-System des Kunden).

In der Praxis kommen auch Mischformen zum Einsatz, bei denen z.B. eine personenbezogene Unterschrift zum Zuge kommt oder eine verteilte Freigabe über die Weblösung des Instituts erfolgt (teilweise auch noch mittels schriftlicher Freigabe oder via Fax). Dieser Ansatz wird von den Schweizer Finanzinstituten durch die Unterstützung der VEU (Verteilte Elektronische Unterschrift) serverseitig unterstützt.

Die Nutzungsmöglichkeit der VEU hängt von der vertraglichen Regelung zwischen Kunde und Finanzinstitut sowie dem Angebot des Finanzinstituts ab.

## 3.4 Schlüssel-Management

Folgende Ausprägungen bezüglich EU-Verfahren und Schlüssellänge werden in der Schweiz unterstützt (die Version «H005» des EBICS-Protokolls sieht die Verwendung der folgenden Verfahren vor):

- «X002» für die Authentifikationssignatur
- «A005» oder «A006» für die EU
- «E002» für die Verschlüsselung
- Schlüssel-Länge: 2048 Bit

Die jeweils vom Finanzinstitut angeboten elektronische Unterschrifts-Verfahren und Schlüssellängen sind mit diesem abzustimmen.

# 4 Auftragsarten

In EBICS 3.0 wird zwischen administrativen und (bank-)fachlichen Auftragsarten unterschieden.

Während die administrativen Auftragsarten in allen EBICS Versionen (2.x und 3.x) und Varianten (DE, FR) einheitliche Auftragsarten-Codes aufweisen, ist die Systematik zur Kennzeichnung der fachlichen Auftragsarten abhängig von der eingesetzten EBICS-Version bzw. Variante.

Mit der Einführung der EBICS Version 3 wurde jedoch die länder-spezifische Systematik zur Kennzeichnung von fachlichen Auftragsarten vereinheitlicht (BTF Codierung).

## 4.1 Administrative Auftragsarten

Die administrativen Auftragsarten dienen u. a. der Administration des EBICS-Kanals und umfassen Aufgaben wie Abholen des Übertragungsprotokolls, Schlüsselaustausch oder dem Abruf der vom Server unterstützen BTF-Parameter.

Die administrativen Auftragsarten sind im EBICS Standard [1], [2] abschliessend dokumentiert.

## 4.2 Bankfachliche Auftragsarten

Für das Senden von bankfachlichen Dateien zum Finanzinstitut bzw. für die Abholung bankfachlicher Dateien vom Finanzinstitut stehen die folgenden Auftragsarten zur Verfügung:

- BTU (Upload zum Finanzinstitut) und
- BTD (Download vom Finanzinstitut)

### 4.2.1 Attribut «fileName»

Neben der Spezifikation der fachlichen Eigenschaften der Datei über die BTF-Parameter des angesprochenen EBICS Services kann ausschliesslich bei der Auftragsart **BTU** optional noch der lokale Dateiname am Kundensystem angegeben werden.

Diese Angabe kann Fehlersuche und Support erleichtern.

### 4.2.2 EBICS Service

Das vom Client angeforderte EBICS Service wird über die entsprechenden BTF-Parameter spezifiziert.

Der generelle Aufbau und die Funktionsweise der BTF-Parameter wird im Kapitel 5 BTF Parameter erklärt.

### 4.2.3 SignatureFlag

Wird das SignatureFlag verwendet, prüft der EBICS Server ob die übertragene Datei vom Sender vollständig mit der erforderlichen Kombination von elektronischen Signaturen geliefert wurde.

Bei Fehlen des Signatur-Flags muss die Datei für die Weiterverarbeitung durch das Finanzinstitut vom Kunden ausserhalb des EBICS-Kanals freigegeben werden (z.B. E-Banking).

#### 4.2.3.1 Attribut «requestEDS»

Bei Verwendung des optionalen Attributs requestEDS werden Dateien mit unvollständig vorliegenden elektronischen Signaturen vom Server nicht zurückgewiesen sondern in die Warteschlange für die verteilte elektronische Unterschrift eingestellt.

**Hinweis:**

Für die Nutzung der verteilten elektronischen Unterschrift muss eine entsprechende vertragliche Vereinbarung mit dem Finanzinstitut vorliegen.

### 4.2.4 DateRange

Durch Angabe eines Datumsbereichs kann ausschliesslich bei der Auftragsart BTD die Anforderung für die Abholung von Dateien vom Finanzinstitut zeitlich (Erstellungsdatum, Kontoauszugs-Datum) eingeschränkt werden.

Hinweis: Diese Funktion wird nicht von allen Finanzinstituten unterstützt.

# 5 BTF Parameter

Durch die Angabe von BTF Parametern wird in EBICS 3.0 die fachliche Ausprägung einer Datei und der gewünschte EBICS Service spezifiziert.

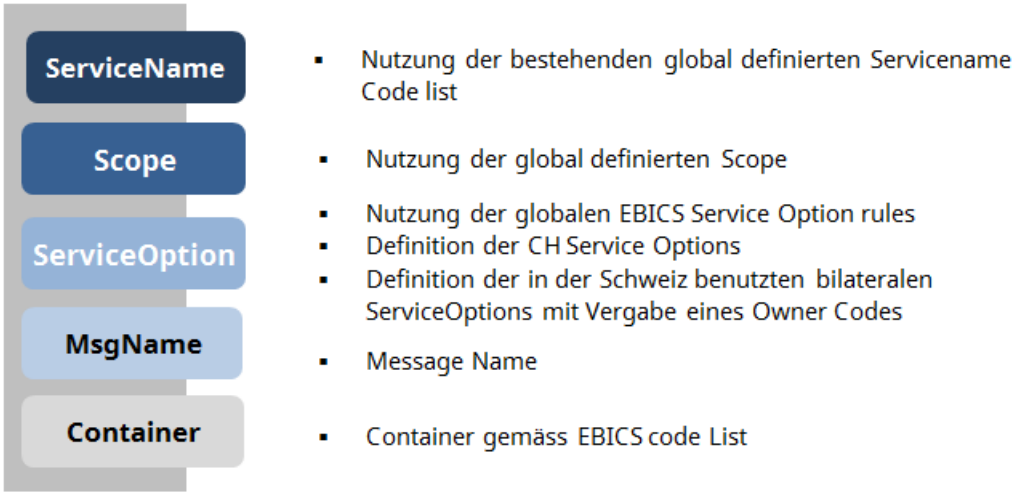


*Abbildung 1: BTF Parametern*

Neben dem Namen des Services und der Meldungs-Bezeichnung (Meldungs-Standard) ist immer auch der sog. Scope (= der Herausgeber des für die Meldung verwendeten fachlichen Regelwerks) anzugeben.

Weitere optionale Parameter können angegeben werden für eine fein-granulare Kennzeichnung der zu übertragenden Datei.

Die BTF Parameter werden sowohl für die Spezifikation von Dateien für die Übertragung zum Finanzinstitut als auch das Abholen vom Finanzinstitut und in administrativen Auftragsarten verwendet.

Die in CH und LI aktuell verwendeten EBICS BTF Parameter institutsabhängig) finden sich im Dokument BTF Parameter CH [10].

## 5.1 ServiceName

Der Parameter ServiceName ist der zentrale Parameter innerhalb von BTF. Er kennzeichnet über eine standardisierte Codeliste den entsprechenden EBICS Service des Finanzinstituts.

Zu den Services zählen bankfachliche Leistungen wie z.B. die Einlieferung von Zahlungsaufträgen oder die Bereitstellung von Kontoauszügen und Reports.

Diese Services können mit Meldungen in unterschiedlichen Meldungsstandards, Versionen und nach unterschiedlichen Regelwerken genutzt werden.

Die zur Verfügung stehenden Codes für ServiceName sind im EBICS Standard festgelegt und garantieren somit eine konsistente, marktübergreifende Bezeichnung.

## 5.2 Scope

Über den Parameter Scope wird das Regelwerk gekennzeichnet nach welcher eine Meldungsdatei erstellt wurde.

Da die Angabe des verwendeten Meldungsstandards i.A. nicht ausreichend genau ist für eine korrekte Verarbeitung der Meldungsdatei, muss der Parameter Scope immer geliefert werden.

Auch der Scope wird durch, im EBICS Standard definierte, Codes angegeben.

Die Codewerte sind entweder:

- 2-stellige ISO 3166 Landescodes (CH, DE, FR,...) oder
- 3-stellige EBICS definierte Issuer Codes für global gültige Regelwerke (GLB für SEPA und SWIFT FIN, CGI), sowie
- der Code BIL für bilateral vereinbarte Regeln.

Für den Zahlungsverkehr in CH und LI wird der Code CH (= SPS, Swiss Payments Standard) verwendet.

Der Scope beeinflusst weiters auch die Bezeichnungsstruktur der verfügbaren ServiceOptions.

## 5.3 ServiceOption

Über den optionalen Parameter ServiceOption können spezifische Sub-Varianten eines Services gekennzeichnet werden.

Der Aufbau der ServiceOption Codes ist vom verwendeten Scope abhängig.

ServiceOptions werden durch 3 bis 10-stellige ServiceOption Codes spezifiziert:

- ServiceOption Codes bei Scope = GLB sind fix 3-stellig und im EBICS Standard definiert.
- ServiceOption Codes bei Scope = ISO 3166 Landescode sind fix 4-stellig, bei CH immer mit X beginnend.

**Beispiel:**

XB2B - Lastschrifteinreichung, ohne Widerspruchsrecht, sortenrein

ServiceOption Codes bei Scope = BIL sind 5 bis 10-stellig.

In der Schweiz und Lichtenstein sind ServiceOption Codes immer 6 bis 10-stellig, beginnend mit dem Schweizer Issuer Code (siehe Kap. 5.3.1) und maximal 5 frei belegbaren Zeichen.

**Beispiel:**

CH001COR - PostFinance Lastschrifteinlieferung, nur COR1

### 5.3.1 Schweizer Issuer Code

Dieser Code wird in der Schweiz für die Kennzeichnung der bilateralen ServiceOptions verwendet.

Der Code besteht aus der Zeichenfolge «CH» und einer 3-stelligen Issuer-Nummer.

Die Issuer-Nummer 000 ist dabei für SPS-definierte Varianten reserviert, weitere Nummern werden mittels Antrag an die Adresse billing-payments.pm@six-group.com durch die PaCoS Arbeitsgruppe EBICS vergeben.

### 5.3.2 Standardwerte

Wird der Parameter ServiceOption bei Verwendung von Scope = «CH» nicht angegeben, so gelten die allgemeinen SPS Definitionen bzw. das institutsspezifische Standardangebot für den entsprechenden Service.

## 5.4 MsgName

MsgName enthält die technische Bezeichnung des Meldungstyps, z.B. pain.001 oder mt940, immer in Kleinbuchstaben.

### 5.4.1 Attribut «Version»

Das optionale Attribut «Version» muss in CH und LI immer dann geliefert werden, wenn das zu übertragende Dokument nicht der Schemaversion der aktuellen SPS Guidelines des Meldungstyps entspricht (nur für ISO 20022).

### 5.4.2 Attribut «Variant»

Das optionale Attribut «Variant» wird aktuell in CH und LI nicht verwendet.

### 5.4.3 Attribut «format»

Das optionale Attribut «format» kann bei Bedarf verwendet werden um Dokumente wie PDF oder nicht standardisierte Listen im CSV-, JSON- oder XML-Format zu kennzeichnen.

## 5.5 Container

Der optionale Parameter Container kennzeichnet Dateien, die als ZIP-Archiv oder eingebettet in einem XML-Container übertragen werden.

In CH und LI werden z.B. ISO 20022-Kontoauszüge und -Reports (camt.053, camt.054, camt.052) sowie PDF-Dokumente von den Finanzinstituten immer als ZIP-Dateien bereitgestellt.

# 6 EBICS-Betrieb

## 6.1 Initialisierung mit Schlüsselpaaren

Die Initialisierung erfolgt in der Schweiz gemäss dem EBICS 3.0 Standard, welcher X.509 Zertifikate für die Registrierung neuer Schlüssel vorsieht.

Die Zertifikate dafür können entweder «Self-signed» oder von einer CA (Zertifizierungsstelle) ausgestellt sein. Nur das X.509 Format ist verpflichtend einzuhalten. Das Gültigkeitsdatum des Zertifikats wird immer überprüft, kann jedoch einen beliebigen gültigen Datumswert (Unbeschränkt = 9999-12-31) enthalten. Weitere Überprüfungen (z.B. CRL), wie sie für die Auftragsart H3K vorgesehen sind, werden nicht vorgenommen. Die Auftragsart H3K wird in der Schweiz nicht unterstützt.

Der Ablauf ist wie folgt:

1. Der Kunde unterschreibt die Vertragsunterlagen des Finanzinstituts.
2. Das Finanzinstitut sendet die EBICS-Zugangsdaten mit den Hash-Werten des Finanzinstituts an den Kunden.
3. Der Kunde führt mit seinem EBICS-System die Auftragsarten INI und HIA aus.
4. Der Kunde sendet den unterschriebenen Initialisierungsbrief mit seinen Hash-Werten an das Finanzinstitut.
5. Das Finanzinstitut vergleicht die Hash-Werte und führt eine Unterschriftenprüfung durch.
6. Das Finanzinstitut akzeptiert die Schlüssel und gibt den Vertrag technisch frei.
7. Der Kunde führt mit seinem EBICS-System die Auftragsart HPB aus und vergleicht die Hash-Werte des Finanzinstituts aus der Antwort auf HPB mit denen aus dem Brief mit den EBCIS-Zugangsdaten.
8. Der Kunde akzeptiert mit seinem EBICS-System die Schlüssel.

Nach dem erfolgreichen Durchlaufen aller Initialisierungs-Schritte kann der Kunde mit dem Finanzinstitut Daten austauschen.

**Hinweis:**

Für existierende Schlüssel, welche mit einer älteren EBICS Version erstellt wurden, ist eine Neu-Initialisierung mit X.509 Zertifikaten nur dann erforderlich, wenn die Länge der Schlüssel < 2048 bits ist.

Für diesen Fall wird empfohlen, vor der Migration auf EBICS 3.0 ein Update der bestehenden Schlüssel auf eine Schlüssellänge >= 2048 bits vorzunehmen.

## 6.2 Teilnehmer sperren

Die Schweizer Finanzinstitute unterstützen für die Sperrung eines EBICS-Benutzers die administrative Auftragsart SPR.

Zusätzlich kann ein EBICS-Benutzer auch auf manuelle Art (z.B. über Telefon oder andere Kommunikationsarten) gesperrt werden. Der Ablauf ist dabei wie folgt:

Das Ereignis, das zur Sperrung führt, trifft ein (z.B. aufgrund Kundentelefonat).

Das Finanzinstitut sperrt den Vertrag manuell.

Der Vertrag kann erst nach erneuter Initialisierung genutzt werden.

**Wichtig:**

Unabhängig von der Art der Benutzer-Sperrung (mittels Auftragsart SPR oder manuell) betrifft die Sperrung eines EBICS-Benutzers immer nur den Kommunikationskanal EBICS!

## 6.3 Kundenprotokoll

Sämtliche Aktionen und Ereignisse, die beim Senden, Abholen und Unterschreiben von Dateien auftreten, werden in EBICS aufgezeichnet und als maschinell auswertbares Protokoll im ISO 20022 Standard (pain.002) für den Kunden bereitgestellt.

Das Kundenprotokoll enthält alle Aktionen und Statusinformationen zu der PartnerID (Kunden-ID). Dieses Protokoll kann von berechtigten Benutzern mit der administrativen Auftragsart HAC abgeholt werden.