EBICS

Empfehlungen für die Umsetzung des EBICS-Standards
für den Finanzplatz Schweiz

«Swiss Market Practice Guidelines EBICS»

Version 1.3 – 20.12.2019

Allgemeiner Hinweis

Anregungen und Fragen zu diesem Dokument können an das jeweilige Finanzinstitut oder an SIX unter folgender Adresse gerichtet werden: billing-payments.pm@six-group.com.

Änderungskontrolle

Alle durchgeführten Änderungen an diesem Dokument werden in einem Revisionsnachweis mit Versionsangabe, Änderungsdatum, einer kurzen Änderungsbeschreibung und dem Gültig ab-Datum aufgelistet.

Revisionsnachweis

Version	*Datum*	*Kommentar*	*Gültig ab:*
1.3	20.12.2019	Kapitel 1.1: Adresse richtiggestellt. Kapitel 1.4: Referenzdokumente aktualisiert. Kapitel 1.5: Links aktualisiert. Kapitel 2.2: Hinweis zu TLS-Version hinzugefügt. Kapitel 2.5.3: Neue Auftragsarten für externe Sammelbuchungsauflösung (QR-Rechnung) mittels camt.054 hinzugefügt. Kapitel 2.5.4 und 2.5.5: Neu hinzugefügt.	01.01.2020
1.2	28.11.2017	Anpassung in Kapitel 2.5.1, Auftragsarten CH-DD COR1/B2B Hinweis zu Auslieferung von Meldungen in ZIP-Container in Kapitel 2.5.2 und 2.5.3 hinzugefügt	01.01.2018
1.1	16.12.2016	Anpassungen in Kapitel 2, 3 und 4	01.01.2017
1.0	10.04.2015	Erstausgabe	01.01.2016

Inhaltsverzeichnis

1 Einleitung

Im Auftrag des PaCoS (Payments Committee Switzerland) erarbeitete eine Arbeitsgruppe die Schweizer Empfehlungen für die Umsetzung des EBICS-Standards für den Finanzplatz Schweiz. Es handelt sich hierbei um unter den Finanzinstituten abgestimmte Empfehlungen. Der Einsatz von EBICS ist für die Institute in der Schweiz nicht verpflichtend.

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 Änderungskontrolle

Dieses Dokument untersteht der Änderungshoheit der

SIX Interbank Clearing AG
Hardturmstrasse 201
CH-8021 Zürich

und widerspiegelt die Empfehlung der Schweizer Finanzinstitute. Zukünftige Änderungen und Erweiterungen erfolgen durch SIX Interbank Clearing.

Die aktuellste Version dieses Dokuments kann von der Internetseite von SIX Interbank Clearing an der folgenden Adresse heruntergeladen werden:

http://www.ebics.ch

1.2 Zweck des Dokuments und Zielgruppe

Das vorliegende Dokument dient als Ergänzung zu den von der EBICS-Gesellschaft veröffentlichten Dokumenten (siehe Referenzen [1] - [4]) und richtet sich primär an Softwareentwickler und Systemadministratoren.

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

1.3 Abgrenzung

Dieses Dokument beschreibt die Anwendung des EBICS-Standards in der Schweiz. Grundlage bildet dabei die EBICS-Spezifikation [1] basierend auf Version 2.5 der deutsch-französischen EBICS-Implementations-Richtlinien.

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.

1.4 Referenzdokumente

Ref	Dokument	Titel	Quelle
	Basisdokumente		
[1]	EBICS-Version_2.5_Final DE-16-05-2011.pdf	Anlage 1 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäss DFÜ-Abkommen «Spezifikation für die EBICS-Anbindung» Version 2.5	DK (ZKA)
[2]	EBICS Anhang2 Auftragsarten-FileFormatParameter-30-07-2018-oAE.pdf	Auftragsarten – Anhang 2 der EBICS-Spezifikation	DK (ZKA)
[3]	EBICS_Common_IG_basiert_auf_EBICS_2.5.pdf	Common Implementation Guide EBICS 2.5	DK (ZKA)
[4]	ebics_xml_schema12-07-2011.zip	EBICS-Schemadateien (.xsd) mit Typen, Auftragsarten, Datenstrukturen und Funktionen	EBICS
	Zusatzdokumente		
[5]	Sicherheitskonzept EBICS	Auf Anfrage erhältlich bei info@ebics.de	EBICS
[6]	EBA-Leitlinien zur Sicherheit von Internetzahlungen	Final Guidelines on the Security of Internet Payments	EBA
[7]	EU Richtlinien betr. Sicherheit für elektronisch initiierten Zahlungen	Payment Service Directive 2	EU

Tabelle 1: Referenzdokumente

1.5 Links zu entsprechenden Internetseiten

Organisation	Link
DK (ZKA)	www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/electronic-banking/dfue-verfahren-ebics.html
EBICS	www.ebics.de (deutsch) www.ebics.org (englisch)
SIX	www.iso-payments.ch www.sepa.ch www.six-group.com/interbank-clearing
European Banking Authority (EBA)	www.eba.europa.eu/-/eba-issues-guidelines-to-strengthen-requirements-for-the-security-of-internet-payments-across-the-eu
European Union (EU)	http://ec.europa.eu/finance/payments/framework/index_de.htm

Tabelle 2: 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 beruht auf der EBICS-Spezifikation [1] Version 2.5 und ist bankseitig für Implementierungen ab Januar 2017 gültig.

Bereits existierende Implementierungen in der Schweiz beruhen jedoch auf der EBICS-Spezifikation Version 2.4 und können, speziell in Bezug auf die unten angeführten Punkte, unverändert von den Finanzinstituten angeboten werden. Es wird jedoch empfohlen, neue Kundenanbindungen auf Basis der Spezifikationen dieses Dokuments zu implementieren.

Es ist zu berücksichtigen, dass zur sicheren Dateiübertragung im Internet ab 2020 mindestens die TLS-Version 1.2 verpflichtend zu verwenden ist.

2.3 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. Dieser Ansatz wird von den Schweizer Finanzinstituten ab 2017 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.

2.4 Schlüssel-Management

Folgende Ausprägungen bezüglich EU-Verfahren und Schlüssellänge werden in der Schweiz unterstützt (die Version «H004» 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 EU-Verfahren und Schlüssellängen sind mit diesem abzustimmen.

2.5 Bankfachliche Auftragsarten

Zur Kennzeichnung der bankfachlichen Auftragsarten werden in der Schweiz Auftragsarten-Codes verwendet.

Abhängig vom jeweiligen Angebot des Finanzinstituts stehen dafür die im Anhang 2 zur EBICS 2.5 Spezifikation aufgeführten Codes zur Verfügung.

Darüber hinaus werden zur Kennzeichnung der CH-spezifischen Auftragsarten von den Schweizer Finanzinstituten entsprechende Codes zur Verfügung gestellt.

Diese Auftragsarten-Codes verwenden als ersten Buchstabe X bzw. Y (für Uploads zum Finanzinstitut) oder Z (für Downloads vom Finanzinstitut).

Die Schweizer Finanzinstitute stellen jeweils Listen mit den von ihnen unterstützen Auftragsarten und den entsprechenden Codes zur Verfügung.

2.5.1 Codes für die Einlieferung von ISO-20022-Meldungen an CH-Finanzinstitute

Die nachfolgende Tabelle gibt die in der Schweiz verwendeten Codes zur Kennzeichnung der bankfachlichen Auftragsarten für die Einlieferung an die CH-Finanzinstitute an:

Geschäftsart	CH-Zahlungsart	EBICS 2.5 Auftragsarten-Code	Meldungstyp
Gemischte Einlieferung innerhalb einer Meldung, alle Zahlungsarten	Alle	XE2	pain.001.001.03.ch.02
Zahlungen im Inland in CHF und EUR	01 - 04	YE1	pain.001.001.03.ch.02
SEPA-Überweisung	5	YE5	pain.001.001.03.ch.02
Zahlungen im Ausland, alle Währungen	6	YE6	pain.001.001.03.ch.02
CHF-Zahlungsanweisung im Inland	7	YE7	pain.001.001.03.ch.02
Bankcheck/Postcash im In- und Ausland in allen Währungen	8	YE8	pain.001.001.03.ch.02

Geschäftsart	CH-Zahlungs-art	EBICS 2.5 Auftrags-arten-Code	Meldungstyp
Customer Direct Debit Initiation für Schweizer Lastschriften mit Widerspruch für das Verfahren LSV+ der Banken	CH-TA	XL3	pain.008.001.02.ch.03
Customer Direct Debit Initiation für Schweizer Lastschriften ohne Widerspruch für das Verfahren BDD der Banken	CH-TA	XL4	pain.008.001.02.ch.03
Customer Direct Debit Initiation für Schweizer Basis-Lastschriftverfahren (COR1) – Verfahren der PostFinance	CH-DD	XL5	pain.008.001.02.ch.03
Customer Direct Debit Initiation für Schweizer Firmen-Lastschriftverfahren (B2B) – Verfahren der PostFinance	CH-DD	XL6	pain.008.001.02.ch.03
SEPA Zahlungsverkehr Direct Debit Initiation, CORE	SDD CORE	XE3	pain.008.001.02.chsdd.02
SEPA Zahlungsverkehr Direct Debit Initiation, B2B	SDD B2B	XE4	pain.008.001.02.chsdd.02

Tabelle 3: Codes für die Einlieferung von ISO-20022-Meldungen

Hinweis: Die Meldungstypen aus der obigen Tabelle können entweder mit dem ISO-Namespace oder dem CH-Namespace eingeliefert werden.

2.5.2 Codes für die Abholung von ISO-20022-Statusmeldungen von CH-Finanzinstituten

Die nachfolgende Tabelle gibt die in der Schweiz verwendeten Codes zur Kennzeichnung der bankfachlichen Auftragsarten für die Abholung von Statusmeldungen von den CH-Finanzinstituten an:

Geschäftsart	EBICS 2.5 Auftrags-arten-Code	Meldungstyp
Status Report gemischt Zahlung/Lastschrift/CHTA/SDD	Z01	pain.002.001.03.ch.02
Status Überweisungen (Antwort auf CH pain.001)	Z02	pain.002.001.03.ch.02
Status CH-Lastschriften (Antwort auf CH pain.008)	Z03	pain.002.001.03.ch.02
Status SEPA Lastschriftaufträge (Antwort auf CH pain.008 SDD)	Z04	pain.002.001.03.ch.02

Tabelle 4: Codes für die Abholung von ISO-20022-Statusmeldungen

Hinweis: Die Auslieferung der Meldungen erfolgt immer in einem ZIP-Container.

2.5.3 Codes für die Abholung von ISO-20022-Kontoauszügen und zugehörige Auflösung von Sammelbuchungen von CH-Finanzinstituten

Die nachfolgende Tabelle gibt die in der Schweiz verwendeten Codes zur Kennzeichnung der bankfachlichen Auftragsarten für die Abholung von Kontoauszugsmeldungen und zugehöriger Auflösung von Sammelbuchungen von den CH-Finanzinstituten an:

Geschäftsart	EBICS 2.5 Auftrags-arten-Code	Meldungstyp
Kontoauszug am Ende der Berichtsperiode	Z53	camt.053.001.04
Belastungs- bzw. Gutschriftsanzeige allgemein	ZS2	camt.054.001.04
Auflösung Sammelbuchungen (FI sammelt)	Z54	camt.054.001.04
Sonstige Auflösung Sammelbuchungen zu Kontoauszug camt.053 (FI sammelt)	ZS8	camt.054.001.04
Auflösung Sammelbuchungen QRR Zahlungen zu Kontoauszug camt.053 (FI sammelt)	ZQR	camt.054.001.04
Auflösung Sammelbuchungen ESR Zahlungen zu Kontoauszug camt.053 (FI sammelt)	ZE1	camt.054.001.04
Auflösung Sammelbuchungen SCOR Zahlungen zu Kontoauszug camt.053 (FI sammelt)	ZRF	camt.054.001.04
Auflösung Sammelbuchungen CH-Lastschriften zu Kontoauszug camt.053 (FI sammelt)	ZS3	camt.054.001.04
Auflösung Sammelbuchungen zu Kontoauszug camt.053 (Kunde sammelt)	ZS4	camt.054.001.04

Tabelle 5: Codes für die Abholung von ISO-20022-Kontoauszugsmeldungen

Hinweis: Die Auslieferung der Meldungen erfolgt immer in einem ZIP-Container.

2.5.4 Codes für die Abholung von ISO-20022-Saldenreports und zugehörige Auflösung von Sammelbuchungen von CH-Finanzinstituten

Einige Finanzinstitute stellen auch Saldenreports zu Intraday-Kontobewegungen zur Verfügung.

Die nachfolgende Tabelle gibt die in der Schweiz verwendeten Codes zur Kennzeichnung der bankfachlichen Auftragsarten für die Abholung von Saldenreportmeldungen von den CH-Finanzinstituten an:

Geschäftsart	EBICS 2.5 Auftrags-arten-Code	Meldungstyp
Saldenreport, Intraday-Kontobewegungen	Z52	camt.052.001.04
Auflösung Sammelbuchungen zu Saldenreport camt.052 (FI sammelt)	ZS5	camt.054.001.04
Auflösung Sammelbuchungen zu Saldenreport camt.052 (FI sammelt)	ZS9	camt.054.001.04
Auflösung Sammelbuchungen QRR Zahlungen zu Saldenreport camt.052 (FI sammelt)	ZQ2	camt.054.001.04
Auflösung Sammelbuchungen ESR Zahlungen zu Saldenreport camt.052 (FI sammelt)	ZE2	camt.054.001.04
Auflösung Sammelbuchungen SCOR Zahlungen zu Saldenreport camt.052 (FI sammelt)	ZR2	camt.054.001.04
Auflösung Sammelbuchungen CH-Lastschriften zu Saldenreport camt.052 (FI sammelt)	ZS6	camt.054.001.04
Auflösung Sammelbuchungen zu Saldenreport camt.052 (Kunde sammelt)	ZS7	camt.054.001.04

Tabelle 6: Codes für die Abholung von ISO-20022-Saldenreportmeldungen

Hinweis: Die Auslieferung der Meldungen erfolgt immer in einem ZIP-Container.

2.5.5 Codes für institutsspezifische Geschäftsarten von CH-Finanzinstituten

Die nachfolgende Tabelle gibt die in der Schweiz reservierten Codebereiche zur Kennzeichnung institutsspezifischer Auftragsarten für Abholung von / Upload zu den CH-Finanzinstituten an:

Geschäftsart	EBICS 2.5 Auftrags-arten-Code	Meldungstyp
Institutsspezifische Geschäftsfälle Upload	XZ*	*
Institutsspezifische Statusmeldungen Download	ZZ*	pain.002.*
Institutsspezifische Geschäftsfälle Download	ZY*	*

Tabelle 7: Codes für institutsspezifische Geschäftsarten

3 EBICS-Betrieb

3.1 Initialisierung mit Schlüsselpaaren

Die Initialisierung erfolgt in der Schweiz gemäss dem Standard (Ausprägung Deutschland), wobei der Ablauf wie folgt ist:

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 per Post mit seinen Hash-Werten an das Finanzinstitut.
5. Das Finanzinstitut vergleicht die Hash-Werte und führt eine Unterschriften-prüfung 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.

3.2 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:

1. Das Ereignis, das zur Sperrung führt, trifft ein (z.B. aufgrund Kundentelefonat).
2. Das Finanzinstitut sperrt den Vertrag manuell.
3. 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!

4 EBICS-Sicherheit

4.1 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.

4.2 Sicherheitsaspekte aus EU-Richtlinien und -Direktiven

Die EBA (European Banking Authority) hat am 19. Dezember 2014 Richtlinien für die sichere Abwicklung von Internet-Zahlungen erlassen: «Final Guidelines on the Security of Internet Payments» (siehe auch Referenz [6]).

Die EBA-Richtlinien gehen, u.a. wegen steigender Risiken auch im Bereich Corporate File Transfer, teilweise weiter, als im EBICS-Sicherheitskonzept formuliert. So sind bezüglich «starke Authentisierung» explizit folgende Anforderungen beschrieben (Referenz [6], im Abschnitt «Specific control and security measures for internet payments», ab Seite 18):

«The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure in line with the definition provided in these guidelines.»

«Strong customer authentication» ist dabei wie folgt definiert (Referenz [6], «Definitions», Seite 11):

«Strong customer authentication is, for the purpose of these guidelines, a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

i) something only the user knows, e.g. static password, code, personal identification number;

ii) something only the user possesses, e.g. token, smart card, mobile phone;

iii) something the user is, e.g. biometric characteristic, such as a fingerprint.

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet.

The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.»

Diese Anforderungen sind analog in die im Dezember 2015 publizierte «EU Payment Service Directive 2 (PSD2)» (siehe Art.97 und Art.98 in [7]) eingeflossen und gehen damit per 2018 in EU-weit verpflichtendes Recht für elektronisch-initiierte Zahlungen über. Das EBA Dokument wird in diesem Zusammenhang (gemäss Art.98) bis Mitte 2017 in einen ebenfalls EU-weit verpflichtenden «EBA regulatory technical standard (RTS) on authentication and communication» überführt.

Unabhängig vom genauen Zeitpunkt der verpflichtenden Umsetzung dieses RTS, sollten bereits heute, wo immer möglich, Verfahren zur starken Kunden-Authentisierung («*strong customer authentication*») sowie Verfahren zur sicheren Auftragsfreigabe (über einen «separaten EBICS oder non-EBICS Kanal») angewendet werden.

Der EBICS-Standard unterstützt sowohl die Nutzung von Hardware-Token-basierten Zertifikaten zwecks starker Authentifizierung als auch die verteilte elektronische Unterschrift über einen «separaten Kanal», so dass Finanzinstitute diese bereits heute anbieten können.

Anhang A: Tabellenverzeichnis