EBICS-Kompendium

Electronic Banking Internet Communication Standard

Dokumentversion:	9
Status:	Abgenommen
Datum:	05.04.2023

Versionsführung

Name	Datum	Dokument-version	Bemerkungen
Rolf Münster	01.03.2006	1	initiale Version
[…]			
Michael Lembcke	20.04.2020	7	Abschnitt 6.7: Beschreibung zu Echtzeitbenachrichtigungen ergänzt
			Abschnitt 6.8.4: Hinweis auf Delta-Dokument zur einschritten, nachrichtenbasierten Nutzung von EBICS 3.0 im RT1-Service ergänzt
			Abschnitt 9.5: Beschreibung zum TRAVIC-Push-Server ergänzt
Michael Lembcke	28.12.2021	8	Abschnitt 1: Einleitung um Österreich ergänzt
			Abschnitt 1.2: ■ Anlage 2 "Spezifikation Echtzeitbenachrichtigungen" ergänzt ■ Abbildungen aktualisiert
			Abschnitt 2.1: Krypto LifeCycle EBICS ergänzt
			Literaturverzeichnis: Dokumente und Versionen aktualisiert
Michael Lembcke	05.04.2023	9	Abschnitt 1 Version zu EBICS 3.0.2 aktualisiert
			Abschnitt 1.2: Abbildung 2 aktualisiert
			Abschnitt 1.3: R2P der EBA Clearing ergänzt
			Abschnitt 9.1: Abbildung 10 aktualisiert

Name	Datum	Dokument-version	Bemerkungen
			Abschnitt 9.3: R2P der EBA Clearing ergänzt
			Abschnitt 9.6: Bezeichnung aktualisiert
			Übergreifend: EBICS 3.0 ohne Unterversion
			Literaturverzeichnis: ■ Dokumente und Versionen aktualisiert ■ Krypto LifeCycle EBICS ergänzt

Inhaltsverzeichnis

Vorwort

Zur CeBIT-Messe 2006 ging der deutsche *Zentrale Kreditausschuss* (ZKA) – heute *Die Deutsche Kreditwirtschaft* (DK) – mit einer Erweiterung des DFÜ-Abkommens mit dem Namen EBICS (Electronic Banking Internet Communication Standard) an die breite Öffentlichkeit. Heute ist dieser Standard nicht nur im deutschen Markt etabliert, sondern auch in Frankreich, der Schweiz und in Österreich. Aber auch in viele andere Länder hat EBICS Einzug gehalten und gute Chancen, der europäische Zahlungsverkehrsstandard im Firmenkundengeschäft und im Interbankenverkehr zu werden.

EBICS ist seit dem 1. Januar 2008 für die deutschen Banken im Firmenkundengeschäft verpflichtend und hat seit Anfang 2011 die vorherige FTAM-Variante komplett abgelöst. In Frankreich ist die Migration von den ETEBAC-Standards auf EBICS abgeschlossen.

Am 17. Juni 2010 wurde die EBICS SCRL mit Sitz in Brüssel gegründet, eine Gesellschaft, deren Zweck das Halten der Namensrechte sowie die Weiterentwicklung des Standards ist. Mitglieder der EBICS SCRL sind die Spitzenverbände der deutschen Kreditwirtschaft, die im DK zusammengeschlossen sind, die französischen Banken, vertreten durch das Comité Français d'Organisation et de Normalisation Bancaire (CFONB), die Schweizer Banken und die Swiss Infrastructure and Exchange (SIX) sowie die Kreditinstitute in Österreich vertreten durch die PSA Payment Services Austria GmbH (PSA).

Die aktuelle EBICS-Spezifikation Version 3.0.2 ist ein Meilenstein in der Evolution des Standards. Mit dem gemeinsamen Business Transaction Format (BTF) ist eine Vereinheitlichung der unterschiedlichen nationalen EBICS-Formate umgesetzt. Auch andere, bisher nur national verfügbare Eigenschaften wie Zertifikate und verteilte elektronische Unterschriften stehen nun überall zur Verfügung. Die Version 3.0 ist seit dem 27. November 2018 offiziell verfügbar. Unabhängig von diesem Termin gelten in den EBICS-Ländern jedoch unterschiedliche Einführungszeitpunkte für die EBICS-Versionen und deren Geltungsbedingungen.

Ergänzend zu den Basisfunktionen, der „Internet-Kommunikation" im Firmenkundengeschäft im weitesten Sinne, liefert EBICS Features wie z. B. die verteilte Signatur oder die Authentifikationssignatur und ermöglicht den Einsatz von Zertifikaten. Zudem wird EBICS im Interbankenbereich erfolgreich eingesetzt. Aktuell wird EBICS sowohl an der Kundenschnittstelle als auch im Interbankenbereich auf die Unterstützung von Instant Payments vorbereitet.

Das vorliegende Kompendium soll dem Leser einen Einblick in die Funktionen von EBICS ermöglichen. Hierzu werden zunächst die Anforderungen vorgestellt, die bei der Entwicklung des Standards entscheidend waren, woraus sich die grundlegenden Eigenschaften von EBICS ergeben. Dem schließt sich eine strukturierte Beschreibung der Funktionen von EBICS an. Eine Positionierung gegenüber anderen Standards wie FinTS oder SWIFT rundet die Betrachtung ab. Den Abschluss bildet eine Darstellung der Umsetzung von EBICS am Beispiel der Produktfamilie TRAVIC.

Wenn Sie als Leser nach der Lektüre dieses Kompendiums eine klare Vorstellung haben, was der Übergang auf EBICS für Sie und Ihr Unternehmen bedeutet, ist der Zweck dieses Dokumentes erfüllt. Wir haben versucht, Ihnen die doch recht komplexen Zusammenhänge so anschaulich wie möglich darzulegen. In jedem Fall wünschen wir Ihnen viel Spaß beim Lesen.

PPI AG, April 2023

1 Einleitung

1.1 Anforderungen an EBICS

Die grundsätzliche Zielsetzung bei der Schaffung des EBICS-Standards 2006 kann mit dem Motto „Evolution statt Revolution“ überschrieben werden. Hinzu kommt mit Einführung der Version 3.0 das wichtige Thema der Harmonisierung, nachdem durch die Bildung der EBICS-Gesellschaft zusammen mit Frankreich und der Schweiz gewisse Dialekte entstanden waren.

Das Prinzip der Evolution galt für die inzwischen in Marktprodukten umgesetzte EBICS-Spezifikation [1] von Anfang an – denn bei all der innovativen Energie der Beteiligten musste vor allem ein unverzichtbares Gut erhalten werden: die Multibankfähigkeit. Dies lässt sich durch die beiden derzeitigen Einsatzszenarien in Deutschland, Frankreich und der Schweiz belegen. Kein Wunder also, dass die Spezifikation sich ganz konkret auf den Kommunikationsbereich, auf die kryptografischen Funktionalitäten für die Sicherheit und einige notwendige bzw. besonders attraktive neue Anwendungsfunktionen wie die Verteilte Elektronische Unterschrift (VEU) konzentriert. Es ist auch nicht weiter verwunderlich, dass EBICS in Deutschland von Beginn an unter dem rechtlichen Deckmantel des DFÜ-Abkommens behandelt wurde, wie beim Aufbau der Spezifikation noch klar zu erkennen sein wird. Der Verlust oder nur die Einschränkung der Multibankfähigkeit wäre mit einer Zersplitterung des Marktes gleichzusetzen gewesen, und das konnte nicht im Interesse der Beteiligten, insbesondere der Unternehmenskunden sein.

Die EBICS-3.0-Spezifikation [1] ist seit dem 27. November 2018 gültig und wurde zuletzt 2022 mit der Version 3.0.2 aktualisiert. Sie soll die bestehenden EBICS-Ausprägungen der Länder harmonisieren.

Die Eigenschaften des EBICS-Standards sind im Einzelnen:

Anforderung	Beschreibung
Internet	EBICS setzt konsequent auf Internet-Technologien. Dieser Aspekt – ursprünglich nur durch den Kommunikationsbereich getrieben – zieht sich durch die Spezifikation und betrifft außer Kommunikationsstandards wie HTTP und TLS auch Standards wie XML oder XML-Signaturen.

Anforderung	Beschreibung
Sicherheit	Internet lässt sich heute nur noch in einem Atemzug mit dem Thema Sicherheit nennen. Wenn schon der sichere Hafen der geschlossenen Netze, die die bisherigen Standards benutzt haben, verlassen werden sollte, dann jedoch ohne Sicherheitseinbußen. Dies betrifft einige Bereiche der Umsetzung, nämlich (gedanklich berücksichtigte) Firewall-Strukturen genauso, wie den Bereich der Signatur und Verschlüsselung, aber auch die Tatsache, dass parallel zur Standardisierung ein Sicherheitskonzept erstellt und abgenommen wurde.
Bandbreite	Einer der größten Vorteile ist die Entkopplung des Kommunikationsprotokolls vom physischen Netz, um die Vorteile von Flexibilität und vor allem von höheren Leitungsgeschwindigkeiten nutzen zu können.
Performance & Wirtschaftlichkeit	Auf den ersten Blick könnte man glauben, Aspekte wie Performance und Ressourcen hätten nichts mit einer fachlichen Spezifikation zu tun. Auf den zweiten Blick ist es aber entscheidend für die Umsetzung, wie ein Kommunikationsprotokoll aufgebaut ist, denn danach richten sich auch die Verarbeitungsprozesse. Das Protokoll wurde daher auf die Verarbeitung großer Datenmengen zugeschnitten und hilft, diese schnell, sicher und wirtschaftlich zu verarbeiten. Ein weiterer Punkt ergibt sich aus der Verwendung von Standards in ihrer originären Form. Dadurch lässt sich im Plattformbereich auf Marktprodukte bzw. Komponenten hoher Verbreitung (z. B. die ZIP-Komprimierung) zurückgreifen, was auch Garant für eine optimale und wirtschaftliche Verarbeitung ist.
Fachlichkeit	Mit EBICS hielten auch einige wenige neue Funktionen Einzug: im Wesentlichen die örtlich und zeitlich Verteilte Elektronische Unterschrift (VEU). Diese Funktion hat sich inzwischen über die Marktprodukte bei den deutschen Kunden etabliert und kann mit EBICS multibankfähig eingesetzt werden. Mit EBICS 3.0 wird diese Funktion als Electronic Digital Signature (EDS) auch für die anderen Länder verfügbar gemacht.

Anforderung	Beschreibung
Migration	Der Migrationsgedanke spielt für die weitere Verbreitung von EBICS eine große Rolle. In vielen europäischen Ländern gibt es nationale Ausprägungen und nahezu überall möchte man erstens einen Parallelbetrieb von alt und neu ermöglichen und zweitens möglichst wenig Aufwand auf der Kunden- und Institutsseite erzeugen. Durch die mit EBICS 3.0 angestrebte Harmonisierung erhält das Migrationsthema einen erweiterten Scope.
Verbindlichkeit	Als eine Aufgabe der Verbände bestand in Deutschland von Anfang an die Forderung, EBICS unter dem Dach der DK (und heute der EBICS-Gesellschaft) zu entwickeln. Darauf aufbauend wurden aber auch konkrete Verpflichtungen eingegangen, ab wann EBICS flächendeckend eingesetzt werden muss, aber auch, wann die alten Standards abgeschaltet werden können. Auch dies gilt für Deutschland und Frankreich in gleicher Weise.

1.2 Aufbau der Spezifikation

Den Abschluss dieser Einleitung bildet eine Übersicht über den Aufbau der Spezifikation und der dazu begleitenden weiteren Abkommens- und Spezifikationstexte. Seit dem 27.11.2018 gilt die EBICS-Spezifikation V3.0. Gleichzeitig ist auch die Vorgängerversion 2.5 gültig.

Da sich diese Versionen nicht nur inhaltlich, sondern auch im Aufbau unterscheiden, soll hier auf beide Varianten eingegangen werden.

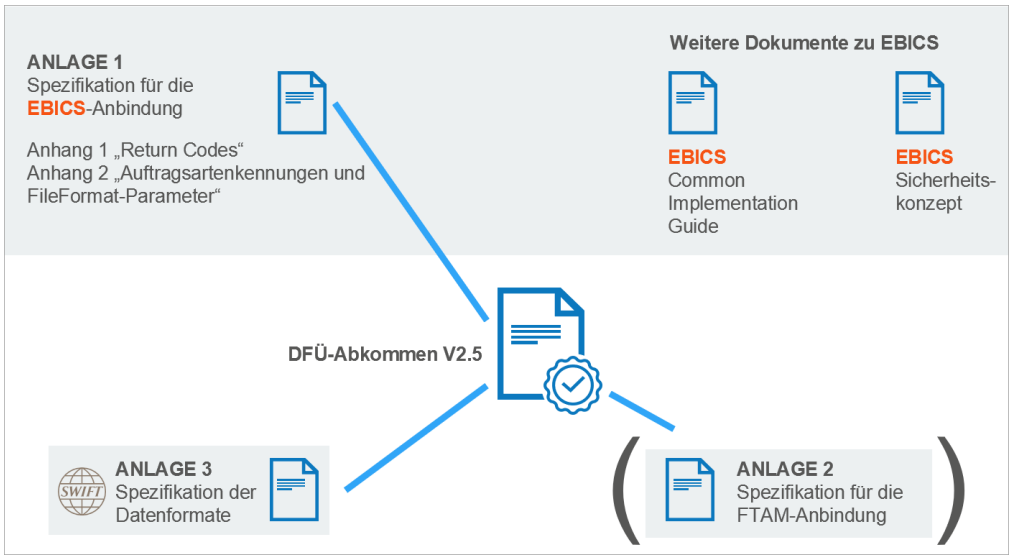


Abbildung 1: Aufbau der EBICS-Spezifikation V2.5 und Einbettung in das deutsche DFÜ-Abkommen

Die Anlage 1 „EBICS“ inkl. der beiden Anhänge wird federführend durch die EBICS-Gesellschaft gepflegt und ist unter ebics.org veröffentlicht. Als Konsequenz wird die Spezifikation [1] selbst im englischen Originaltext bearbeitet, und es finden nur Rückübersetzungen ins Deutsche und Französische statt. Diese Dokumente befinden sich unter ebics.de bzw. cfonb.org.

Zusätzlich zur Spezifikation in Anlage 1 ist zu EBICS noch ein Implementation Guide und in Deutschland [4] – auf Anfrage bei der DK – auch ein Sicherheitskonzept [5] erhältlich. Mit der Version 2.5 wurden die deutsche und die französische Fassung des Implementation Guide in einem gemeinsamen Dokument zusammengeführt. Für die Schweizer Kreditwirtschaft hat die SIX Payment Services in einem Implementation Guide die Nutzung von EBICS für die Schweiz definiert, zu finden unter six-group.com. Außerdem sind in einem weiteren Dokument Business Rules für den Einsatz von ISO20022-Payments in der Schweiz festgelegt. Damit wird den Forderungen nach leichter Implementierung und Migration sowie sicherem Betrieb Genüge getan.

Die Anlage 3 des DFÜ-Abkommens zur Spezifikation der Datenformate [3] wie SWIFT oder SEPA bleibt eine deutsche Standardisierung und ohne Belang für die internationalen EBICS-Aktivitäten.

Die Anlage 2 zur Spezifikation des FTAM-Verfahrens [2] ist inzwischen obsolet und nur noch der Vollständigkeit halber aufgeführt. Ihren Platz hat ab 2019 die neue Anlage 2 der Spezifikation Echtzeitbenachrichtigungen [9] eingenommen.

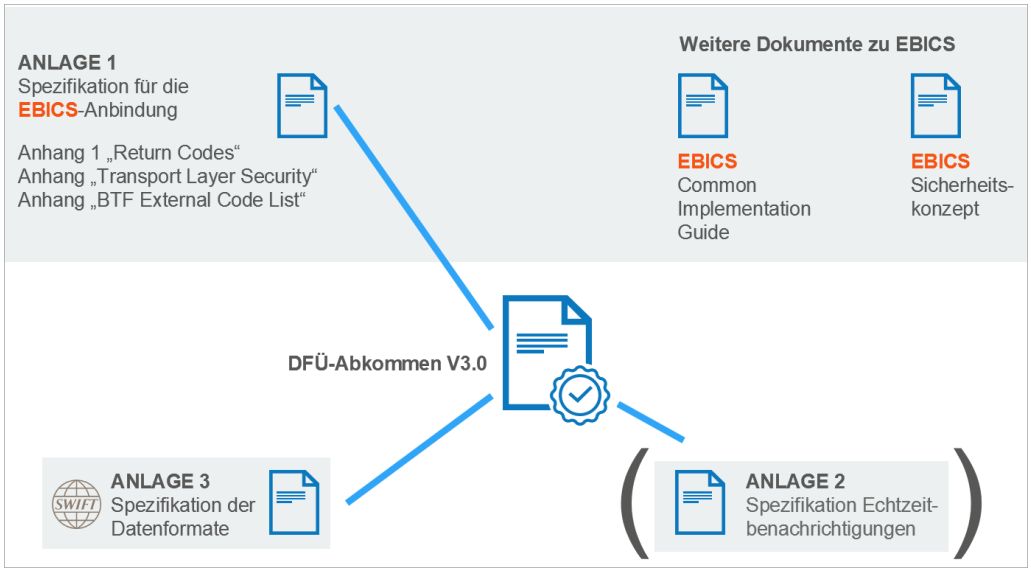


Abbildung 2: Aufbau der EBICS-Spezifikation V3.0 und Einbettung in das deutsche DFÜ-Abkommen

Der Aufbau der EBICS-Spezifikation Version 3.0 unterscheidet sich auf den ersten Blick nur unwesentlich von der Version 2.5. Die BTF-Code-Liste ersetzt erwartungsgemäß die ehemalige Liste der Auftragsarten, wobei unter *ebics.de* Referenzlisten für beide Richtungen verfügbar sind.

Ein wichtiger Schritt ist die Auslagerung der Transport Layer Security, woraus eine Konzentration der eigentlichen EBICS-Spezifikation auf die anwendungsspezifischen Protokollinhalte zu erkennen ist.

1.3 Zusatzdokumente

Zusätzlich zur offiziellen EBICS-Spezifikation sind noch spezifische Zusatzdokumente für die unterschiedlichen Einsatzszenarien von EBICS verfügbar.

Verfasser	Dokument
Deutsche Bundesbank	„ZV-Vereinbarung zur Kommunikation über EBICS mit Kreditinstitutionen/Zahlungsinstituten“ ■ Hashwert ■ Fingerprint ■ Implementation Guide im Internet frei verfügbar
EBA Clearing	EBA STEP2 EBICS Procedural Rules

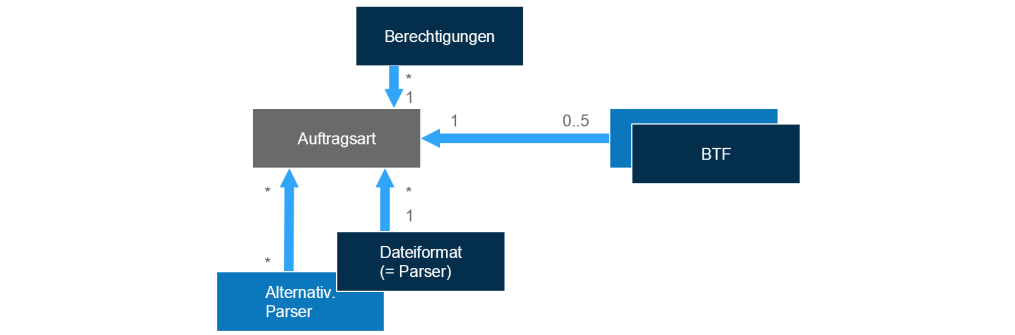
Verfasser	Dokument
EBA Clearing	RT1 System – SCT Inst Service Network Interfaces
EBA Clearing	R2P System – Pan-European Request to Pay (R2P) Service
Berlin Group	EBA Cards Clearing (ECC)
Die Deutsche Kreditwirtschaft	Datenaustausch unter Einbindung von Service-Rechenzentren (SRZ) www.die-dk.de
CFONB	EBICS Guide de mise en oeuvre en France (Implementation Guideline): Version 2.1.5 www.cfonb.org
SIX Group	Swiss Market Practice Guidelines EBICS 3.0 https://www.six-group.com/dam/download/banking-services/standardization/ebics/market-practice-guidelines-ebics3.0-de.pdf

2 Gesamtszenario EBICS

In diesem Abschnitt wird ein beispielhaftes Gesamtszenario entwickelt. Diese Betrachtung soll ein Verständnis dafür aufbauen, wie der Spagat geschafft werden kann bzw. konnte, eine stabile bestehende Infrastruktur genauso wie eine bereits etablierte Internet-Plattform auf Basis von Marktprodukten weich und unterbrechungsfrei auf ein EBICS-Zielsystem zu migrieren.

2.1 Zusammenspiel EBICS 3.0 und Vorgängerversionen

Die Einführung von EBICS 3.0 stellt Anforderungen an die Implementierungen, da für eine gewisse Übergangszeit parallel EBICS-2.5-Kunden unterstützt werden müssen. Ziel für die Umsetzung muss primär die volle Abdeckung der Anforderungen gemäß der EBICS-Spezifikation Version 3.0 sein, um Schritt für Schritt die gewünschte Harmonisierung erreichen zu können. Dabei sollen sich möglichst geringe Auswirkungen auf die Endkundenverträge ergeben, und der Umstellungsaufwand für Institute und Hersteller soll möglichst gering sein.



Service Name	Service Scope	Service Option	Service MsgName	Container-Typ	Auftragsart
SCC	DE	B2B	pain.008	XML	C2C

Abbildung 3: Zusammenspiel/Mapping zwischen BTF und Auftragsarten

Generell sind für das Zusammenspiel folgende Themen relevant:

- einheitlich im Zertifikatsformat
- Versionskompatibilität in einem Vertrag
- nationale BTF-Mappings
- Sonderfall VEU und Signatur-Flag
- Praxis-Anforderung: Beibehaltung der Schnittstellen
- Kryptografische Anforderungen

Einheitlich im Zertifikatsformat

Mit EBICS 3.0 ist X.509 das einzig zugelassene Zertifikatsformat. Dies bedeutet, dass zumindest die X.509-Syntax im Rahmen des H005-Schemas unterstützt werden muss. Aufgrund des Fehlens einer PKI-Infrastruktur werden für

eine Übergangszeit CA-basierte Zertifikate bei einem DK-Profil nicht gegen die ausgebende CA geprüft. Unabhängig davon wird jedoch lokal das Gültigkeitsdatum des Zertifikats gegen das aktuelle Datum geprüft.

Versionskompatibilität in einem Vertrag / BTF-Mappings

BTF wird zusätzlich zu den bekannten Auftragsarten und Datenformaten eingeführt. Damit ergibt sich für ein Institut die Situation, dass entsprechend den Kundeninstallationen Aufträge mit unterschiedlichen EBICS-Versionen 2.5 und 3.0 eingereicht werden können. Ein Mapping zwischen BTF und Auftragsart ermöglicht es, unter bestimmten Rahmenbedingungen auch für BTF-Aufträge auf der bestehenden, auf der Auftragsart basierenden Berechtigungsstruktur aufzusetzen und so eine Kompatibilität herzustellen.

Sonderfall VEU und Signatur-Flag

VEU-Steuerung

Kundenvertrag	Auftrag	VEU
erlaubt	erlaubt	ja
erlaubt	nicht erlaubt	nein
nicht erlaubt	erlaubt	nein
nicht erlaubt	nicht erlaubt	nein

Signatur-Flag

Auftragsartkonfiguration	Auftrag	Verarbeitung
O-Datei	Flag vorhanden	EU-Prüfung
O-Datei	Flag nicht vorhanden	ablehnen
nur D-Datei	Flag vorhanden	ablehnen
nur D-Datei	Flag nicht vorhanden	alternative Freigabe

Abbildung 4: VEU-Steuerung und Signatur-Flag

Wie in der Abbildung gezeigt, beeinflussen Kundenvertrag, Auftrag und Signatur-Flag, ob ein eingereichter Auftrag mit nicht ausreichender Autorisierung abgelehnt oder an die VEU-Verarbeitung weitergeleitet wird.

Praxisanforderung: Beibehaltung der Schnittstellen

Die Spezifikation von EBICS 3.0 öffnet die Tür zu einer weitgehenden Harmonisierung der europäischen EBICS-Landschaft und erhöht damit auch die Attraktivität für andere Länder, diesen Standard einzuführen.

Umgekehrt muss bei der Einführung von EBICS 3.0 in bestehende Implementierungen darauf geachtet werden, dass Schnittstellen zu Anwendungssystemen erhalten bleiben, um das Ziel einer ressourcenschonenden Migration erreichen zu können.

Berücksichtigung kryptografischer Anforderungen

Wie in den entsprechenden Folgeabschnitten noch beschrieben wird, werden mit EBICS 3.0 einige kryptografische Verfahren nicht mehr unterstützt. Betroffen davon sind die Authentifikationsverfahren X001, das Signaturverfahren A004 und das Verschlüsselungsverfahren E001.

Zudem sollen nur noch RSA-Schlüssel mit mindestens 2.048 Bit zum Einsatz kommen.

Die DK hat für Deutschland auf www.ebics.de eigens das Dokument „Krypto LifeCycle EBICS“ [6] veröffentlicht. Dieses Dokument macht Vorgaben für die im EBICS-Verfahren zur Anwendung kommenden kryptografischen Komponenten unter Berücksichtigung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das Dokument wird entkoppelt von der EBICS-Spezifikation gepflegt.

Nach dieser Beschreibung des Zusammenspiels der unterschiedlichen Versionen berücksichtigen die nächsten Abschnitte nur noch die aktuelle EBICS-Version 3.0.

2.2 Berücksichtigung der Produkte

Der EBICS-Spezifikation ist schon beim ersten Lesen anzumerken, dass sie nicht auf dem Reißbrett entstanden ist, sondern die in der Praxis vorkommenden Szenarien optimal abbildet. Dies liegt auch daran, dass im Vorfeld der Spezifikation bereits Produkte am Markt entstanden sind, die eine Art Proof of Concept darstellten. Allen Produkten war gemeinsam, dass sie Möglichkeiten aufzeigten, den Massenzahlungsverkehr für Firmenkunden auf Internet-Plattformen abzubilden. Ergänzend setzte jedes Produkt auch eigene Ideen für Anwendungserweiterungen um. So konnten aus diesem Portfolio die optimalen Lösungsansätze den Weg in den EBICS-Standard finden und dort typische Anfängerfehler vermeiden helfen. Auf diese Weise wird auch verständlich, dass bereits bei Einführung von EBICS Probleme wie die Segmentierung großer Nachrichten gelöst waren oder das Konzept für die Verteilte Elektronische Unterschrift bereits in ausgereifter und erprobter Form zur Verfügung stand und nicht erst mit dem ersten Praxiseinsatz ergänzt oder optimiert werden musste.

2.3 Portale

Bereits seit einigen Jahren gehören browserbasierte Firmenkundenportale zum Basisangebot eines jeden Instituts. Da EBICS ebenfalls auf Internet-Technologien aufsetzt, liegt der Schluss nahe, dass diese beiden Welten harmonisch zusammengeführt werden können. Dies ist auch in der Tat der Fall, solange es sich um ein institutseigenes Portal handelt.

3 Kommunikation und Absicherung der Infrastruktur

Dieser Abschnitt befasst sich mit dem Herzstück des EBICS-Standards, der Kommunikation über das Internet.

In der einführenden Literatur zum Internet als Kommunikationsverfahren wird immer versucht, das TCP/IP-Protokoll in den OSI-Stack zu zwängen, um eine historische Vergleichbarkeit herzustellen. Dies ist bis zu einem gewissen Grad auch möglich und nachvollziehbar, jedoch für eine Betrachtung des EBICS-Standards ohne Belang. Entscheidend ist vielmehr, dass mit diesem Schritt in Richtung Internet-Plattform sowohl auf Kunden- als auch auf Institutsseite vorhandene Infrastrukturen genutzt werden können und dass diese ein Vielfaches der Leistungsfähigkeit früherer Lösungen besitzen.

Die Verwendung der Internet-Technologie ermöglicht es auch, EBICS enger mit anderen Anwendungen zusammenrücken zu lassen. Da das Firmenkundengeschäft außer Massenzahlungsverkehr auch viele Anwendungsgebiete im transaktions- oder dialogorientierten Bereich hat, ist ein Zusammenspiel mit anderen Services, die z. B. auf dem zweiten signifikanten DK-Standard FinTS (Financial Transaction Services – in Deutschland [7]) aufsetzen, unerlässlich. Dies wird durch die Nutzung gemeinsamer Plattformen stark vereinfacht.

3.1 HTTPS und TLS – Transport Layer Security

Während das TCP/IP-Protokoll sich im Netz um Aufgaben wie z. B. das dynamische Routing bei Ausfall einer Teilstrecke kümmert, kontrolliert http die Session zwischen zwei Partnern. Bei EBICS kommt nur die gesicherte Variante HTTPS zum Einsatz, was z. B. im Browser durch ein Schloss in der unteren Ecke angezeigt wird. Verantwortlich für diese Absicherung ist TLS (Transport Layer Security), welches das bisherige SSL (Secure Socket Layer) ablöst.

Die Ablösung von SSL auf TLS weist auf ein grundsätzliches Problem der Verquickung von Internet-Technologien mit Anwendungsstandards hin: Inzwischen sind nämlich laut Aussage des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Versionen 1.0 und 1.1 des TLS-Protokolls ebenfalls als obsolet anzusehen und abzulösen. Bisher war man durch die Integration dieser Standards in die EBICS-Spezifikation sehr unflexibel. Mit Einführung von EBICS 3.0 wurden die Sicherheitsverfahren der Transportschicht in ein eigenes Dokument überführt, das nun unabhängig vom fachlichen Standard gepflegt werden kann.

TLS sorgt für eine sichere Übertragung zwischen dem Kundensystem und dem ersten http-Server oder besser Webserver im Institut. Aktuell wird mind. die Version 1.2 empfohlen. Diese Aufgabe erfüllt es auch hinreichend gut und sicher, was jedoch für die EBICS-Standardisierer nicht ausreichend war, wie im übernächsten Abschnitt erläutert wird.

3.2 XML – Extensible Markup Language

Um die folgenden Abschnitte besser verstehen zu können, wird an dieser Stelle der XML-Standard erläutert. Während die notwendigen Protokollaufgaben bei

BCS noch im Dateinamen versteckt werden konnten, wird bei EBICS aufgrund der Fülle der Aufgaben ein separater Protokollumschlag benötigt. Im Rahmen der Internet-Technologie ist es sinnvoll, hierfür die Datenbeschreibungssprache XML – Extensible Markup Language – zu verwenden.

Bei EBICS besteht jeder Request bzw. Response aus einem Auftrag analog den definierten Auftragsarten bzw. einem BTF-Container und einem XML-Umschlag. Es handelt sich also um eine Art Hybridsystem, bei dem das Kernstück die bankfachlichen SEPA- oder SWIFT-Formate bleiben, die aber um XML-Strukturen ergänzt werden. Der Overhead, der durch diese Technik verursacht wird, ist minimal, wenn man bedenkt, dass es sich typischerweise um Massenzahlungsverkehr handelt, die Zahlungsverkehrsdatei also ein Vielfaches des XML-Umschlags darstellt.

Die folgende Abbildung zeigt alle in EBICS definierten XML-Schemata. Diese sind – entsprechend dem XML-Namespace-Konzept – unter den zugehörigen Adressen www.ebics.de abgelegt.

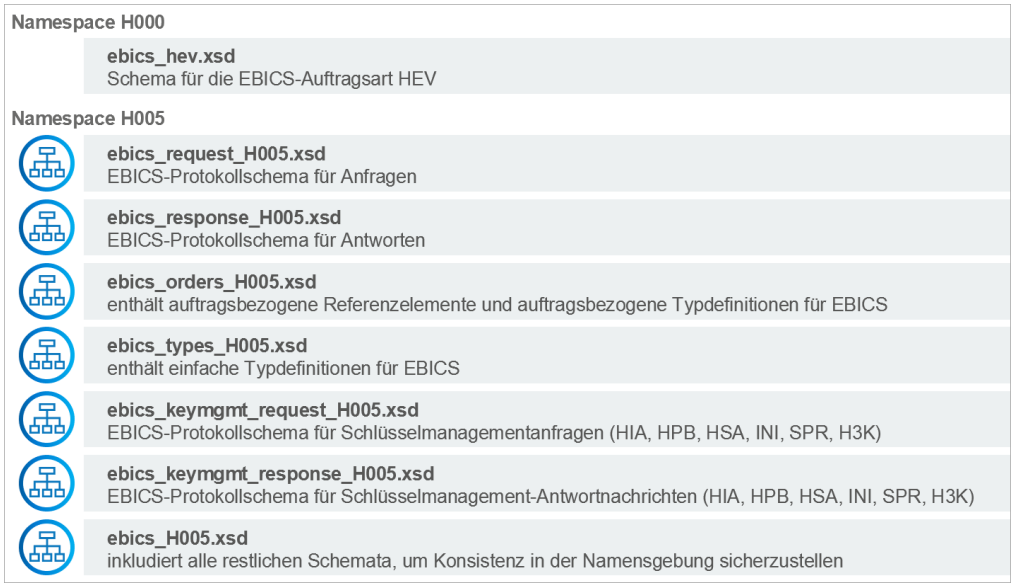


Abbildung 5: EBICS-XML-Schemata V3.0

Es wird erkennbar, dass die Schemata klar strukturiert sind und die Typ-Definitionen von den fachlichen Protokollschemata getrennt sind.

Eine Besonderheit stellt das erste Schema dar. H000 dient zur Versionsverwaltung und ermöglicht es dem Kundenprodukt abzufragen, welche Protokollversionen das Institut unterstützt.

Nicht dargestellt ist hier der Namespace S001, der das EBICS-Signaturschema enthält. Die aktuellen Versionen der EBICS-Schemata finden Sie auf den offiziellen Websites ebics.org bzw. ebics.de.

3.3 Optimierung der Kommunikation

Durch Optimierungen im Kommunikationsbereich wurde den speziellen Eigenschaften des Internets Rechnung getragen.

Bei EBICS besteht die Möglichkeit, die Übertragungsdaten zu komprimieren. Hierfür bedient sich EBICS des lizenzfreien und weit verbreiteten ZIP-Algorithmus.

Große Datenmengen können im EBICS-Protokoll segmentiert werden, um die Kapazitäten der Internet-Instanzen auf Institutsseite nicht zu blockieren.

Die optionale Recovery-Fähigkeit dieses Protokolls ermöglicht auch intelligentes Wiederaufsetzen der Transaktion, wenn eine Dateiübertragung abgebrochen ist. Bereits übertragene Segmente müssen also nicht doppelt über die Leitung geschickt werden.

EBICS stellt über `Nonce` und `Timestamp` auch ein Verfahren bereit, das es ermöglicht, Doppeleinreichungen (Replays) zu erkennen. Hierfür erzeugt ein Kundenprodukt einen zufälligen Wert „Nonce“ (zu übersetzen als „ad hoc-Wert“) und setzt diesen zusammen mit einem Zeitstempel in den EBICS-Umschlag. Institutsseitig wird eine Liste von bereits vom Teilnehmer verwendeten Werten für Nonce und Timestamp vorgehalten, wodurch die Eindeutigkeit eines Auftrags überprüft werden kann.

4 Datenmodell

Der vorliegende Abschnitt geht speziell auf das bei EBICS verwendete Datenmodell ein. Dieses findet sich in den Stammdatenverwaltungen der einzelnen Produkte wieder und unterscheidet sich, wie bereits bei den Migrationsaspekten erwähnt, kaum von dem ursprünglichen BCS-Modell.

Grob gesehen existieren im Datenmodell die folgenden Entitäten:

- Kunde
- Konto
- Teilnehmer
- Geschäftsvorfall

Den Einstieg bildet in der Nomenklatur ein `Kunde`. Dies ist der Oberbegriff z. B. für ein Unternehmen, das auf der einen Seite mehrere Konten bei einem Institut unterhält, andererseits mehreren Teilnehmern Zugriff auf diese Konten gewährt.

Ein `Teilnehmer` kann z. B. ein Mitarbeiter eines Unternehmens sein, der im Auftrag des Kunden agiert. Er bekommt eine Unterschriftsklasse zugeordnet, die festlegt, ob dieser Teilnehmer Aufträge autorisieren darf, allein oder zusammen mit anderen Teilnehmern.

Dabei werden folgende Unterschriftsklassen unterstützt:

- Unterschriftsklasse E Einzelunterschrift

  Es wird keine weitere Unterschrift mehr zur Autorisierung des Auftrags benötigt.

- Unterschriftsklasse A Erstunterschrift

  Es wird noch eine Unterschrift mindestens der Klasse B benötigt. Die Reihenfolge der Unterschriftsklassen ist dabei beliebig.

- Unterschriftsklasse B Zweitunterschrift

  Der Auftrag muss zusätzlich noch über eine Unterschrift mindestens der Klasse A verfügen. Die Reihenfolge der Unterschriftsklassen ist auch hier beliebig.

- Unterschriftsklasse T Transportunterschrift

  Kennzeichnung, dass es sich um eine Authentifikationssignatur, z. B. um einen technischen Teilnehmer handelt.

Einem Teilnehmer mit Unterschriftsklasse E, A oder B wird die Unterschriftsberechtigung für bestimmte Konten des Unternehmens gewährt und ihm werden speziell für ihn zugelassene Auftragsarten zugeordnet.

Auf diese Art lässt sich ein flexibles Kompetenzsystem aufbauen, das dann auf Kunden- und Institutsseite in den jeweiligen Produkten abgebildet wird.

Eine einfache Form des Datenmodells zeigt die folgende Abbildung:

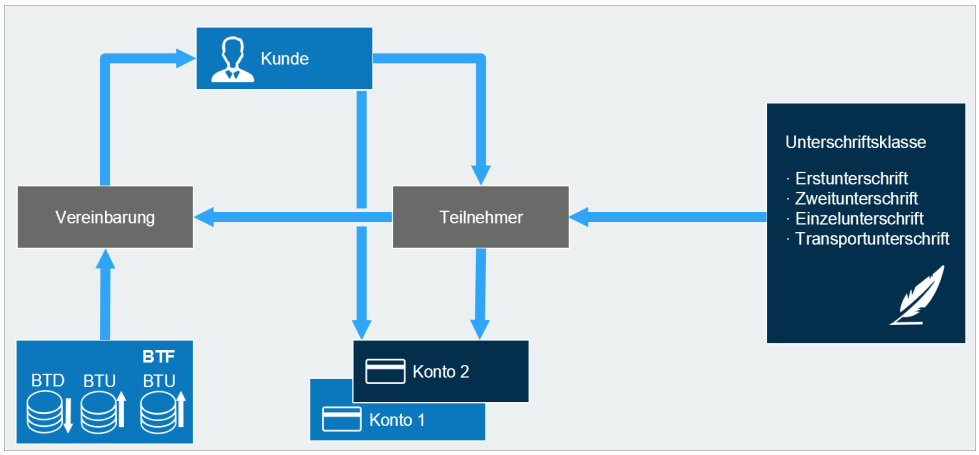


Abbildung 6: Datenmodell

Unter dem Stichwort Datenmodell sollen auch noch die Bankparameter- und User-Daten erwähnt werden. In den Bankparameterdaten, die vom EBICS-Server abrufbar sind, sind alle Informationen für den Zugang zum Institut sowie die vom Institut angebotenen optionalen Funktionen enthalten. Dazu gehört z. B. die Kommunikationsadresse (URL). Die optional vom Institut angebotenen User-Daten enthalten kunden- und teilnehmerspezifische Informationen wie z. B. zugelassene Konten oder Auftragsarten bzw. Message-Namen.

5 Sicherheit

Bereits mit der EBICS-Version 2.4 sind neue Sicherheitsverfahren A005 und A006 bzw. X002 und E002 eingeführt worden. Wichtiger sind jedoch die Festlegungen zur Verpflichtung, diese Verfahren auch einzusetzen – eine Neuerung mit Einführung des EBICS-Standards.

Nicht betrachtet werden die Sicherheitsmedien an sich, wie z. B. Chipkarte oder Diskette bzw. heute eher USB-Stick. Hier definiert auch EBICS keine Anforderungen, sondern überlässt die Auswahl dem Kunden bzw. den Herstellern der Kundenprodukte. Informell kann das Kundensystem jedoch mithilfe folgender Klassifizierung übermitteln, welche Art von Sicherheitsmedium der Kunde verwendet:

- keine Angabe
- Diskette
- Chipkarte
- sonstiges Sicherheitsmedium
- nicht wechselbares Sicherheitsmedium

Frankreich stellt besondere Anforderungen an das TS-Profil: Der Implementation Guide schreibt für das TS-Profil die Nutzung von besonderen HW-Token vor, die von einer Zertifizierungsstelle (CA) herausgegeben werden. Die Übermittlung erfolgt implizit über das X.509-Zertifikat (s. u.).

5.1 Infrastruktursicherheit

Ein wesentlicher Aspekt zur Erreichung eines hohen Niveaus an Infrastruktursicherheit ist das durchgängige Konzept für Signatur und Verschlüsselung in EBICS. Kundensignaturen sind bei EBICS Pflicht. Bankensignaturen sind vorgesehen und werden konkret definiert, wenn die rechtlichen Auswirkungen geregelt sind (Stichwort personenbezogene Bankensignatur vs. Firmenstempel). Hinzu kommt noch die zusätzliche Authentifikationssignatur X002.

Auch bei der Verschlüsselung macht EBICS keine halben Sachen: Außer der zwingenden Verschlüsselung mit TLS auf Transportebene ist ebenfalls das EBICS-eigene Verschlüsselungsverfahren E002 verpflichtend, um eine Ende-zu-Ende-Sicherheit zu gewährleisten.

In einem speziellen Initialisierungsschritt, in dem optional Vorabprüfungen durchgeführt werden können, wird unter anderem auch eine Transaktions-ID für die gesamte Transaktion vergeben. Dies ermöglicht die Bildung einer Transaktionsklammer und ist Voraussetzung für die Segmentierung bei der Übertragung großer Datenmengen.

Durch diese Festlegungen wird ein Maß an Sicherheit erreicht, welches einem Betrieb im Internet angemessen ist und dessen Stärke auch in einem entsprechenden Sicherheitskonzept untersucht und belegt wurde.

Mehr Details zu den Protokolleigenschaften selbst befinden sich im Abschnitt *EBICS-Abläufe* auf Seite 41.

5.2 Signaturverfahren

EBICS kennt zwei unterschiedliche Signaturen:

- Authentifikationssignaturen zur Identifizierung des Einreichers
- Auftragssignaturen, Elektronische Unterschrift (EU) zur bankfachlichen Autorisierung von Aufträgen

Die beiden Signaturarten unterscheiden sich grundsätzlich, wie die folgende Abbildung zeigt:

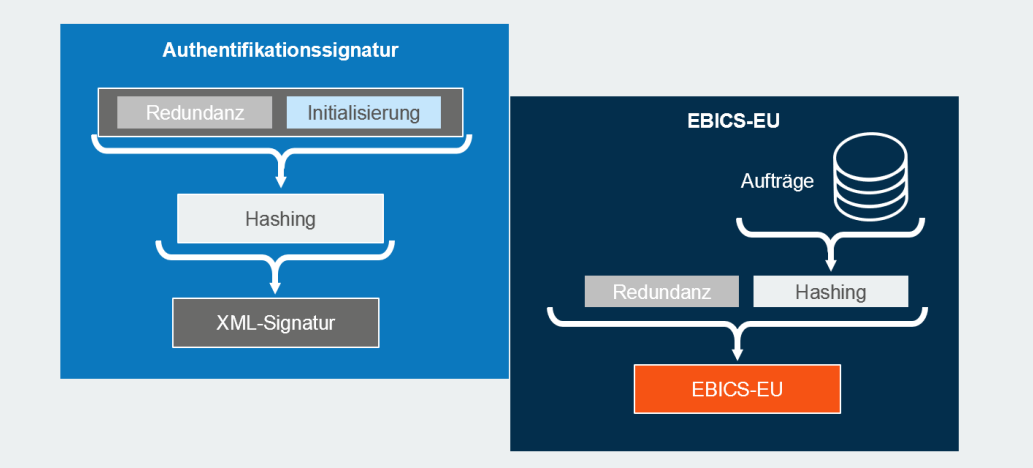


Abbildung 7: EBICS-Signaturverfahren

5.2.1 Authentifikationssignatur X001 bzw. X002

Die Authentifikationssignatur dient dazu, den Einreicher eindeutig zu identifizieren. Die Authentifikationssignatur wird im Rahmen des Initialisierungsschrittes sowie in jedem weiteren Transaktionsschritt geprüft, also noch bevor die eigentlichen Auftragsdaten übertragen werden (siehe Abschnitt *EBICS-Abläufe*, Seite 41).

Teilnehmer, die ausschließlich Aufträge einreichen, können die Unterschriftsklasse T besitzen, wodurch es auch möglich ist, reine „technische Teilnehmer“ einzurichten, die dann nur zur Einreichung von Aufträgen berechtigt sind.

Die Bildung der Authentifikationssignatur entspricht dem gängigen Vorgehen im Transaktionsbereich. Die Aufträge werden um dynamische Informationen wie Session-ID, Timestamp oder Ähnliches ergänzt, um bei gleichen Nutzdaten unterschiedliche und zur speziellen Situation gehörige Signaturen zu erhalten. Kryptologen verwenden hierfür den Begriff Redundanz. Über die gesamte Struktur wird eine kryptografische Prüfsumme, der Hashwert, gebildet. Die wichtigste Eigenschaft des Hashwerts ist es, mit konkret vorgegebenen Daten exakt einen Wert zu erzeugen, der über praktisch keine andere

Datenkombination erzeugt werden kann. Es besteht also eine 1:1-Beziehung zwischen Daten und Hashwert.

Über diesen Hashwert wird mithilfe eines Signaturschlüssels eine digitale Signatur gebildet. Um exakt zu sein, muss erwähnt werden, dass die Daten vor der Hashwertbildung nach einem vorgegebenen Algorithmus auf eine bestimmte Mindestlänge aufgefüllt werden (Padding), damit dieser Mechanismus auch bei kleinen Datenmengen funktioniert.

Da dieses Vorgehen im Transaktionsgeschäft gängig ist, wird es auch im W3C-Standard XML-Signature in dieser Weise unterstützt. Daher unterstützt EBICS die Authentifikationssignatur analog XML-Signature als Standard X002 und X001 (veraltet) und ab EBICS 3.0 nur noch X002.

5.2.2 Auftragssignaturen (EU) nach A004 bzw. A005/A006

Die Elektronische Unterschrift (EU) eines Auftrags auf Kundenseite (bzw. zukünftig auch auf Institutsseite) erfolgt seit EBICS 2.4 verpflichtend durch die neuen Verfahren A005 und A006. Im Gegensatz zur Signaturbildung bei der Authentifikationssignatur sind hier die Schritte Redundanzbildung und Hashwertbildung vertauscht. Aufgrund der Verwendung des Dateihashwerts als wichtige, direkte Repräsentanz der Originaldaten wird dieser ohne Redundanz direkt über die Auftragsdatei gebildet und ist somit an jeder Stelle direkt überprüfbar.

EBICS forderte aus Gründen der Migrationsfähigkeit die RSA-Signatur nach A004 als Einstieg – ältere Signaturvarianten des DFÜ-Abkommens wurden nicht mehr unterstützt. Bereits A004 war von den Verfahren her auf die aktuelle Signaturkarte der deutschen Kreditwirtschaft mit SECCOS als Betriebssystem zugeschnitten, unterstützte diese Verfahren aber wie gesagt auch über Disketten oder USB-Sticks.

Aus den von SECCOS unterstützten Verfahren wurde bei A004 ein Profil, bestehend aus folgenden Algorithmen unterstützt:

- RSA-Signatur mit Schlüssellängen von 1.024 Bit
- Padding nach ISO9796-2
- Hashwertverfahren RIPEMD160

Heute gängig und seit EBICS 2.4 auch als verpflichtend deklariert, unterstützen die robusteren EU-Verfahren A005 und A006 die folgenden Attribute:

	A005	A006
Schlüssellänge	(1.536)–4.096 Bit	(1.536)–4.096 Bit
Hashwertverfahren	SHA-256	SHA-256
Padding-Verfahren	PKCS#1	PSS

Die Darstellung zeigt, dass sich A005 und A006 lediglich im Padding-Verfahren unterscheiden.

Aus der Darstellung der Sicherheitsverfahren und dem Bezug zum SECCOS-Chipkartenbetriebssystem könnte man ableiten, dass es sich bei diesem Teil der EBICS-Spezifikation eher um eine deutsche Ausprägung handelt. Dies ist aber keineswegs der Fall. Gerade durch die DK-Kartenstrategie, die sich streng an dem jährlich erscheinenden BSI-Krypto-Katalog und damit an der nationalen Ausprägung der EU-Signaturrichtlinie orientiert, ist eine Verwendung internationaler Standards gewährleistet.

Mit EBICS 3.0 wird generell eine Schlüssellänge von mindestens 2048 Bit vorgegeben. Ebenso sollen noch vorhandene A004-Schlüssel umgestellt werden.

5.3 Initialisierung

Bevor ein Schlüsselpaar verwendet werden kann, muss erst über ein geeignetes Verfahren die Authentizität der Partner hergestellt werden. Hierfür werden entweder Zertifikate oder aber alternative Verfahren über separate Wege verwendet. Die Unterstützung von Zertifikaten nach X.509 ist in EBICS zwar vorgesehen, aktuell wird in Deutschland jedoch noch das Verfahren mittels Initialisierungsbrief verwendet. Frankreich verfügt zur Einführung des EBICS-Standards bereits über eine geregelte PKI-Infrastruktur. Daher können dort auch Zertifikate im Rahmen der Initialisierung verwendet werden, was durch den Standard seit EBICS 2.5 auch lückenlos unterstützt wird.

Beide Konzepte werden im Folgenden kurz dargestellt, wobei ersichtlich wird, dass die beiden Welten sich derzeit auch noch vermischen können, wie das Fallback-Szenario in Frankreich zeigt.

5.3.1 Zertifikate in Frankreich

Die Grundlage für ein zertifikatsbasiertes Verfahren stellt eine geeignete Security Policy dar. Dies bedeutet, es muss geregelt sein, welche Zertifikatsherausgeber bis zu welchem Grad als sicher angenommen werden können. In Frankreich gibt es hierfür klare und publizierte Definitionen für die Nutzung von Zertifikaten in EBICS. Die höchste Stufe stellen dabei die Herausgeber qualifizierter Zertifikate nach der europäischen Signaturrichtlinie dar. Für den reinen Austausch von Zahlungsverkehrsdateien sind in Frankreich aber auch geringere Sicherheitsniveaus ausreichend, wie die folgende Detaillierung zeigen soll.

In Frankreich werden die Unterschriftsklassen T und E eingesetzt. Derzeit wird keine verteilte EU unterstützt. Stattdessen existieren zwei Grundprofile für Einreichung (T) und Autorisierung (E).

Für die Einreichung von Zertifikaten kann ab Version 2.5 die neu geschaffene Auftragsart H3K verwendet werden. Die restlichen Prozesse zur Initialisierung eines Kunden bleiben aus EBICS-Sicht unverändert gültig.

- Einreicherprofil T auf Basis von Zertifikaten bereits ab EBICS 2.4

Die Initialisierung muss nicht zwingend über eine gelistete Zertifizierungsinstanz (CA) erfolgen. Auch selbstsignierte Zertifikate des Instituts mit INI-Brief sind möglich.

Falls das Zertifikat jedoch von einer CA ausgestellt ist, muss diese sich auf der Trusted List befinden.

- Autorisierungsprofil TS

  Hierbei werden die Elektronischen Unterschriften für Transport und Signatur verwendet. Das Verfahren entspricht grob dem ETEBAC-5-Standard. Das Zertifikat für den Signaturschlüssel muss in diesem Fall von einer CA herausgegeben und signiert sein und diese muss sich auch in der Trusted List befinden. Die Zertifikate für den Authentifikations- und Verschlüsselungsschlüssel können auch selbstsigniert sein.

  Die Zertifikatsprüfung ist für den Signaturschlüssel verpflichtend vorgeschrieben, für Zertifikate für den Authentifikations- und Verschlüsselungsschlüssel findet die Prüfung gegen die CA statt, wenn die Zertifikate von einer CA ausgestellt wurden.

- INI-Brief als Fallback-Szenario

  Auch bei der Verwendung von Zertifikaten sind INI-Briefe in Frankreich Bestandteil des Initialisierungsprozesses. Unabhängig von der Verwendung von Zertifikaten muss der Kunde zu Beginn in jedem Fall einen INI-Brief schicken.

  Nicht-CA-basierte Zertifikate werden ausschließlich über den INI-Brief freigeschaltet. CA-basierte Zertifikate müssen stets von der CA geprüft werden. Bei erfolgreicher Zertifikatsprüfung durch die CA müssen zusätzlich definierte Zertifikatsangaben mit übermittelten Angaben des Einreichers abgeglichen werden. Stimmen die Angaben nicht überein, kann immer noch – auf Basis der Angaben im INI-Brief – eine manuelle Freischaltung stattfinden.

Das Zertifikat des Kunden wird nach erfolgreicher Prüfung und Freischaltung im Anwendungssystem gespeichert. Auf dieser Basis werden die zukünftigen Sperrabfragen durchgeführt – der Kunde muss das Zertifikat also nur einmal einreichen.

Unabhängig von den in Frankreich üblichen Autorisierungs- und Einreichungsprofilen wird mit EBICS 3.0 generell das Zertifikatsformat für Schlüssel verwendet. Die Nutzung bleibt zunächst jedoch unterschiedlich, sodass der Effekt der Harmonisierung noch nicht sichtbar wird.

5.3.2 INI-Brief-Verfahren in Deutschland

Beim INI-Brief-Verfahren erzeugt ein Teilnehmer ein Schlüsselpaar und übermittelt seinen öffentlichen Schlüssel mit der Auftragsart INI (bzw. HIA, wenn es sich um einen öffentlichen Schlüssel für die Authentifikationssignatur oder für die Verschlüsselung handelt) an das Institut. Parallel hierzu wird ein Initialisierungsbrief ausgedruckt, der administrative Daten, den öffentlichen Schlüssel und den zugehörigen Hashwert enthält. Dieser Initialisierungsbrief wird vom

Teilnehmer manuell unterschrieben und per Briefpost oder Fax an das Institut geschickt und dort mit den elektronisch übermittelten Daten verglichen. Bei Gleichheit wird der Schlüssel freigeschaltet und kann nun vom Teilnehmer verwendet werden. Das gleiche Verfahren kann in umgekehrter Richtung verwendet werden, wenn zu einem späteren Zeitpunkt die Banksignatur eingeführt wird. Hier hat nun der Teilnehmer die Aufgabe, die elektronisch und postalisch übermittelten Schlüsseldaten zu vergleichen und deren Übereinstimmung zu bestätigen.

5.4 Verschlüsselungsverfahren

Bei EBICS wird eine doppelte Verschlüsselung nach TLS und dem eigenen EBICS-Verfahren aktuell E002 verwendet (E001 ist die veraltete Version), um sowohl die Standardverschlüsselung in HTTPS als auch eine Ende-zu-Ende-Verschlüsselung zu erhalten. Bei E002 wird das vom BSI seit 2009 empfohlene AES-Verfahren eingesetzt.

5.4.1 TLS – Transport Layer Security

TLS ist der Nachfolger des SSL. Beide Verschlüsselungsprotokolle besitzen die Eigenschaft, auf einer Transportstrecke sowohl Authentifizierung als auch Verschlüsselung zu gewährleisten. Entsprechende Implementierungen befinden sich kundenseitig z. B. im Internet-Browser und institutsseitig in gängigen Webservern.

Beim Aufbau einer TLS-Verbindung werden Zertifikate und unterstützte Verfahren zwischen den Partnern ausgetauscht und darauf basierend eine Session aufgebaut.

EBICS verwendet wie allgemein üblich nur die Server-Authentifizierung aus TLS und unterstützt derzeit keine TLS-Client-Zertifikate. Als Server-Zertifikate werden die allgemein von den Instituten verwendeten Internet-Zertifikate benutzt (die z. B. über VeriSign zertifiziert sind).

Verschlüsselt wird in beiden Richtungen. Als Verfahren werden nur die starken Verschlüsselungsverfahren bzw. Cipher Suites unterstützt. Gültige Cipher Suites sind auf der Website der Deutschen Bundesbank bzw. unter ebics.de abrufbar.

Hier nochmals der Hinweis, dass die Transport Layer Security mit EBICS 3.0 in ein eigenes Dokument ausgelagert wurde.

5.4.2 Verschlüsselung E001 bzw. E002

Bei E001/E002 handelt es sich um ein so genanntes Hybridverfahren, d. h., es besteht aus asymmetrischen und symmetrischen Algorithmen. Dabei wird grundsätzlich als Basis ein asymmetrischer RSA-Schlüssel als Verschlüsselungsschlüssel verwendet. Die Nachricht selbst wird aus Performance-Gründen symmetrisch verschlüsselt. Als Key wird ein dynamischer Schlüssel verwendet, der – mit dem Verschlüsselungsschlüssel gesichert – ausgetauscht wird.

E001 verwendete einen 1.024 Bit langen Verschlüsselungsschlüssel und den Padding-Algorithmus PKCS#1. Spätestens mit Einführung von EBICS 3.0 entfällt die Unterstützung von E001 in den Implementierungen. Mit Einführung von EBICS 3.0 und der Vorgängerversion 2.5 ist EBICS 2.4 obsolet und damit auch die Verfahren E001, X001 und A004.

Mit EBICS 2.4 wurde E002 als Weiterentwicklung eingesetzt. Hier erfolgt der Übergang von Triple-DES auf AES (BSI-Empfehlung ab 2009).

6 Fachliche Funktionen von EBICS

EBICS eröffnet neue Anwendungsfelder für den Kunden.

6.1 Auftragsarten

Im DFÜ-Abkommen für Deutschland, durch die Schweizer Implementation Guidelines sowie die Format-Standards des CFONB in Frankreich werden mit EBICS u. a. folgende Anwendungsgebiete durch operative Auftragsarten und FileFormat-Parameter – bzw. ab EBICS 3.0 einheitlich durch die betreffenden BTF-Vorgaben – unterstützt:

- SEPA-Zahlungsverkehr und sonstiger nationaler Zahlungsverkehr
- Auslandszahlungsverkehr
- Wertpapiergeschäft
- Akkreditivgeschäft
- Tageskontoauszugsinformationen sowie sonstige Informationen für gebuchte Umsätze und Kontoumsatz-Avise (u. a. in den Formaten MT940/MT942 oder camt-XML)

Zusätzlich werden mit EBICS 3.0 folgende neuartige Auftragsarten für BTF eingeführt:

- BTD: Administrative Auftragsart zum Abholen einer Datei, die durch eine BTF-Struktur näher gekennzeichnet ist
- BTU: Administrative Auftragsart zum Senden einer Datei, die durch eine BTF-Struktur näher gekennzeichnet ist

6.1.1 SEPA-Zahlungsverkehr

EBICS unterstützt Auftragsarten bzw. FileFormat-Parameter für den SEPA-Zahlungsverkehr Kunde-Bank und Bank-Bank (Bundesbank und Interbank STEP2). Unterstützt werden derzeit für die Kunde-Bank-Schnittstelle die SEPA-Nachrichten:

- SEPA Credit Transfer Initiation
- SEPA Direct Debit Initiation
- Rückgabe vor Settlement (Rejects)

Diese spiegeln sich in entsprechenden EBICS-Auftragsarten wider, wobei folgende Besonderheit zu berücksichtigen ist.

Bei der Umsetzung der SEPA-Nachrichten für die DK wurde festgestellt, dass es sinnvoll ist, neben dem Standard-SEPA-Format erweiterte Formate einzuführen, die je nach Kreditinstitut bzw. Anwendungsfall Verwendung finden können. Im Speziellen handelt es sich hierbei um Sammelaufträge mit mehrfachen Gruppenbildungen wie z. B. Auftraggeberkonten oder Ausführungsdaten, die

auf unterschiedliche Art behandelt werden können (als Beispiel wird die Behandlung mehrerer Auftraggeberkonten herangezogen):

- SEPA-Standardformat

  Verwendung des SEPA-Standardformats, wobei als Einschränkung nur Aufträge für ein Auftraggeberkonto möglich sind. Für die Abwicklung von Aufträgen mehrerer Auftraggeberkonten müssen bei dieser Option mehrere Aufträge im SEPA-Standardformat eingereicht werden.

- SEPA-Container

  DK-spezifische Protokollerweiterung, um mehrere SEPA-Standardformate für mehrere Auftraggeberkonten im Rahmen einer Auftragsart einreichen zu können

- Erweiterte Grouping-Optionen

  SEPA-Standardformat, bei dem unter Ausnutzung der erweiterten Grouping-Optionen im SEPA-Format selbst die Möglichkeit besteht, Aufträge für mehrere Auftraggeberkonten einzureichen

Diese Aufteilung auf mehrere Ausprägungen ist durch die optimierte Verarbeitungsweise bei den unterschiedlichen IT-Dienstleistern begründet.

In der folgenden Tabelle sind einige der in Deutschland verwendeten SEPA-Auftragsarten nach den unterschiedlichen Ausprägungen aufgelistet:

Option	Auftragsart EBICS 2.x	SEPA-Bezeichnung
SEPA-Datenformate	CRZ	Payment Status Report for Credit Transfer
	CDZ	Payment Status Report for Direct Debit
Container	CCC	Credit Transfer Initiation
	CRC	Payment Status Report for Credit Transfer
	CDC	Direct Debit Initiation
	CBC	Payment Status Report for Direct Debit
Erweiterte Grouping-Option	CCT	Credit Transfer Initiation
	CDD	Direct Debit Initiation

Um den jeweiligen Geschäftsvorfällen der Deutschen Kreditwirtschaft gerecht zu werden, wurden zusätzlich zu den genannten SEPA-Auftragsarten weitere mit unterschiedlichen Formatausprägungen entwickelt. Dazu gehören vor allem die Auftragsarten zur Abwicklung des nationalen SRZ-Verfahrens.

Der Vollständigkeit halber sei noch erwähnt, dass zur Übermittlung der SEPA-relevanten Daten im Rahmen der SWIFT-Tagesauszüge mittels der Auftragsart STA die SWIFT-Formate MT940 und MT942 angepasst wurden.

Um den Zahlungsverkehr aus SEPA-Aufträgen verlustfrei abbilden zu können, wurden als Entsprechung zu den MT94x-Nachrichten (STA und VMK) sowie den DTAUS-Umsatzinformationen (DTI) neue Abholauftragsarten für die camt-Formate eingeführt (C52, C53 und C54).

Einzelheiten zu den SEPA-Datenformaten und deren Verwendung in Deutschland befinden sich in der Anlage 3 des DFÜ-Abkommens.

Je nach Land werden außerhalb von SEPA unterschiedliche nationale Zahlungsverkehrsformate mit eigens dafür definierten Auftragsarten und FileFormat-Parametern genutzt.

6.1.2 ISO 20022

Eine besondere Bedeutung im internationalen elektronischen Zahlungsverkehr spielt heutzutage der freie und offene Standard *ISO 20022: Financial Services – Universal financial industry message scheme*. Der Standard zielt auf die Vereinfachung und Vereinheitlichung der globalen Kommunikation innerhalb des Finanzsektors. Gegenstand der Standardisierung sind unter anderem Begriffe, Abläufe und Nachrichtenformate. Damit soll ein weltweiter Austausch von Finanzinformationen zwischen Systemen ermöglicht werden. Die Nachrichten werden zwischen Kunde und Bank bzw. Bank und Bank ausgetauscht und sind als XML-Dokumente (Extensible Markup Language) repräsentiert.[1] Dies ist ein Unterschied zu bisherigen Formaten, wie beim DTA-Format.

Hierfür wurde durch ISO 20022 eine große Menge an Nachrichtentypen standardisiert (zu finden unter https://www.iso20022.org/iso-20022-message-definitions). Für jeden Typ existiert eine formale Spezifikation der verfügbaren Elemente und Strukturen in Form von XML-Schema-Dateien. Zur eindeutigen Identifikation besitzt jeder Typ zudem einen Identifier bzw. Namen. Zudem sind die Nachrichtenbeschreibungen versioniert, sodass abweichende Versionen der zugrundeliegenden Nachrichtenbeschreibung unterschieden werden können. Jeder Nachrichtentyp ist geeignet, einen oder mehrere Geschäftsvorfälle (z. B. Einreichung einer SEPA-Überweisung) zu repräsentieren.

Nachfolgend sind einige relevante Nachrichten für die Kunde-Bank-Kommunikation aufgeführt:

Name	Nachricht
pain.001	Überweisungen
pain.002	Statusberichte
pain.008	Lastschriften
pain.007	Kundenrückgabe (customer to bank payment reversal)

[1] Siehe ISO 20022: https://www.iso20022.org/ als Startseite und für Überblicksinformationen z. B. https://www.iso20022.org/faq.page

Name	Nachricht
camt.052	Intraday Kontoumsätze
camt.053	Tagesauszüge
camt.054	Buchungsinformationen
camt.029	Information zum Rückruf/Rückgabe (Resolution of investigation)
camt.055	Kundenrückruf (customer payment cancellation request)

Für die Interbank-Kommunikation stehen ebenfalls entsprechende Nachrichten zur Verfügung (u. a. pacs-Nachrichten). Auch für Instant-Payments-Zahlungen werden ISO-20022-Nachrichten verwendet.

Durch ISO 20022 liegt somit eine einheitliche Beschreibungsform für den Nachrichtenaustausch im Finanzsektor vor. Auf dieser globalen Ebene wird zunächst pro Nachricht die insgesamt mögliche Menge an verfügbaren Elementen beschrieben.

Durch Einschränkungen der allgemeinen Vorgaben und durch zusätzliche Belegungsregeln (technisch und/oder fachlich) können Organisationen eigene Unterausprägungen von ISO-20022-Nachrichten für bestimmte Geltungsbereiche definieren.

Eine Organisation, die solche Konkretisierungen und zusätzlichen Regeln definiert hat, ist die CGI (Common Global Implementation) Group. Sie fokussiert sich auf den Nachrichtenaustausch im globalen und länderübergreifenden Zahlungsverkehr. Zugleich können vielfältige Zahlungsauftragsarten abgebildet werden. Es erfolgt dort keine Spezialisierung auf z. B. SEPA-Zahlungen.[2]

Eine weitere Organisation mit eigenen Festlegungen für ISO-20022-Nachrichten ist der European Payments Council (EPC).[3] So werden vom EPC spezifische Implementation Guidelines veröffentlicht, die die Anwendung für SEPA-Zahlungen mittels ISO 20022 erläutern, wie etwa Überweisungen (ISO-20022-Benennung pain.001).[4] Die Dokumente beschreiben eine Einschränkung der allgemeinen ISO-20022-Vorgaben, etwa welche Elemente zulässig sind und welche zusätzlichen zahlungsspezifischen Regeln zu beachten sind. So beinhaltet das EPC-Format nur solche Elemente, die für SEPA-Zahlungen

2 Siehe CGI Group / SWIFT: https://www.swift.com/standards/market-practice/common-global-implementation

3 Siehe European Payments Council (EPC): https://www.europeanpaymentscouncil.eu

4 Siehe European Payments Council (EPC): https://www.europeanpaymentscouncil.eu/document-library/implementation-guidelines/sepa-credit-transfer-inter-psp-implementation-guidelines

erforderlich sind. Die Formatbeschreibung zu u. a. den zulässigen Werten liegt für das EPC-Format nur allgemein in einer textuellen Beschreibung vor.

Auf Länderebene wurden teilweise eigene ISO-20022-Ausprägungen abgestimmt. So wurden etwa für Deutschland durch die DK spezifische Vorgaben festgelegt, wie XML-Nachrichten gemäß ISO 20022 aufgebaut sein müssen und welche Regeln für die transportierten Informationen zu beachten sind. Es werden die verschiedenen Datenformate und Abläufe detailliert beschrieben sowie entsprechende XML-Schema-Dateien veröffentlicht.[5] Ähnlich gilt dies für den Schweizer Finanzplatz. Die SIX (Swiss Infrastructure and Exchange) hat mit ihren Swiss Payment Standards entsprechende Festlegungen und Umsetzungsempfehlungen veröffentlicht, um die ISO-20022-Nachrichten zu realisieren. Darin enthalten sind konkrete Vorgaben, wie z. B. Überweisungsaufträge ausgetauscht werden können. Ebenso existieren Festlegungen für landeseigene Zahlungsaufträge, wie Schweizer Lastschriften.[6]

Sowohl die Vorgaben der DK als auch diejenigen der SIX übernehmen verschiedene Festlegungen der EPC-Vorgaben, gestalten jedoch landesspezifisch die ISO-20022-Vorgaben aus. Somit stellen die DK- und SIX-Vorgaben Konkretisierungen der EPC-Vorgaben dar. Insbesondere liegen die Formatbeschreibungen teilweise detaillierter als XML-Schema-Bestandteile vor, anders als beim EPC-Format. Es lassen sich dadurch viele Prüfungen direkt anhand des XML-Schemas durchführen (z. B. beim DK-Format). Allen gemein ist jedoch die ISO-20022-Basis in Form der universellen XML-Beschreibung.

Des Weiteren bieten etwa die SIX-Vorgaben den Finanzinstituten einen Rahmen für individuelle Ausgestaltungen, z. B. abhängig vom angebotenen Leistungsportfolio des Institutes.

Darüber hinaus existiert für Frankreich eine durch das CFONB herausgegebene Implementierungsbeschreibung für die dortige ISO-20022-Verwendung von unter anderem pain.001-Zahlungen[7] (SEPA, Nicht-SEPA usw.) oder pain.008-SEPA-Lastschriften[8]. In den Dokumenten werden die verschiedenen Ausprägungen unterschieden.

Ausgehend von der sehr allgemeinen Beschreibung des ISO-20022-Standards werden die verschiedenen Ausprägungsvarianten somit stets konkreter und spezifischer bzw. restriktiver.

Die ISO-20022-Nachrichten werden mittels EBICS als Upload- bzw. Download-Transaktionen kommuniziert (siehe Abschnitt *EBICS-Abläufe*, Seite 41). So wird etwa die pain.001-Nachricht (Überweisung) mittels EBICS vom Kundensystem an die Bank gesendet (siehe Abschnitt *SEPA-Zahlungsverkehr*,

5 Siehe DK, SIZ: https://www.ebics.de/de/datenformate

6 Siehe SIX: https://www.six-interbank-clearing.com/de/home/standardization/iso-payments/customer-bank/implementation-guidelines.html

7 Siehe CFONB: https://www.cfonb.org/index.php/instruments-de-paiement/virement

8 Siehe CFONB: https://www.cfonb.org/instruments-de-paiement/prelevement

Seite 28). Der Abholauftrag für den dazugehörigen pain.002-Statusbericht wird ebenfalls via EBICS erteilt (siehe Abschnitt *SEPA-Zahlungsverkehr*, Seite 28).

Die pain.002-Nachrichten können je nach Ausprägung des ISO-20022-Standards Positiv- und/oder Negativmeldungen zu Zahlungsaufträgen beinhalten. So ist es einer Bank mit einer pain.002-Nachricht möglich, maschinenlesbar für das verarbeitende Kundensystem auf Fehlergründe für zurückgewiesene Überweisungsaufträge hinzuweisen. Das Kundensystem kann diese Fehler geeignet berücksichtigen. Anhand verschiedener Statuscodes kann über den Status des Gesamtauftrags oder einzelner Teiltransaktionen informiert werden. Insbesondere kann ein Überweisungsauftrag, bestehend aus mehreren einzelnen fehlerhaften und fehlerfreien Transaktionen, partiell verarbeitet werden. Dabei würde die Verarbeitung nur die fehlerfreien Transaktionen berücksichtigen, wohingegen die fehlerhaften Transaktionen ausgesteuert würden und dem Kunden gemeldet werden. Fehlerinformationen und Reaktion sind damit sehr feingranular und maschinengestützt möglich.[9]

6.1.3 Auslandszahlungsverkehr und Umsatzinformationen

Einige Beispiele der in Deutschland und der Schweiz genutzten Formate von gebundenen standardisierten Auftragsarten zeigt die folgende Übersicht:

- AZV AZV-Auftrag im Diskettenformat senden (DTAZV in Deutschland)
- STA Abholen SWIFT-Tagesauszüge (SWIFT MT940)
- VMK Abholen kurzfristige Vormerkposten (SWIFT MT942)
- VML Abholen langfristige Vormerkposten (SWIFT MT942)
- C52 Abholen Bank-To-Customer Account Report
- C53 Abholen Bank-To-Customer Statement Report
- C54 Abholen Bank-To-Customer Debit Credit Notification
- ESR Abholung von ESR-Informationen (spezifisch in der Schweiz)

Darüber hinaus werden in Europa insbesondere zur Abwicklung von Auslandszahlungen unterschiedliche nationale Formate eingesetzt. Zunehmend gewinnen aber auch hier die ISO 20022 basierten Formate (z. B. ISO Global, CGI) an Bedeutung (siehe Abschnitt *ISO 20022*, Seite 30).

6.1.4 Standardauftragsarten für Upload (FUL) und Download (FDL)

Diese Auftragsarten kommen bisher vornehmlich in Frankreich zum Einsatz und dienen dem transparenten Dateitransfer beliebiger Formate. Dies bedingt, dass nicht, wie bisher in Deutschland üblich, am Namen der Auftragsart abzulesen ist, welches Format transportiert wird. Vielmehr wird der Auftragsart FUL bzw. FDL ein längerer Formatparameter mitgegeben, der dann eine weitere Steuerung erlaubt. Diese Auftragsarten stehen seit EBICS 2.4 zur Verfügung. Die Auftragsart FUL (File Upload) wird für Einreichungen und die Auftragsart FDL

[9] Zum Beispiel DK-Standard, siehe DK, SIZ: https://www.ebics.de/de/datenformate

(File Download) wird für Abholungen verwendet. Der Aufbau und die zu verwendenden Formatparameter sind zusammen mit den Auftragsarten als Anhang der EBICS-Spezifikation dokumentiert.

6.1.5 Weitere Auftragsarten

Zusätzlich zu den standardisierten Auftragsarten kann bezüglich der Verwendung in EBICS folgende Klassifizierung vorgenommen werden:

- systembedingte Auftragsarten – speziell für EBICS
  - z. B. Auftragsarten in Zusammenhang mit der VEU
- sonstige unterstützte systembedingte Auftragsarten
  - z. B. HAC, PTK für Abholen von Kundenprotokollen
- reservierte Auftragsarten für den zwischenbetrieblichen Dateiaustausch
  - z. B. FIN für EDIFACT-FINPAY senden
- sonstige in der Spezifikation reservierte Auftragsarten unter Verwendung nicht standardisierter Formate, z. B.:
  - FTB für Senden/Abholen beliebiger Dateien
  - FTD für Senden/Abholen freier Textdateien
- optionale EBICS-Auftragsarten
  - z. B. HVT für VEU-Transaktionsdetails abrufen

6.2 Business Transaction Format – BTF

BTF steht für Business Transaction Format. BTF vereinheitlicht mit Einführung von EBICS 3.0 die Beschreibung der zu transferierenden Formate in Deutschland, Frankreich und der Schweiz. Statt mit Auftragsarten bzw. Formatparametern wird in der Kommunikation mit dem Bankrechner mit BTF eine Struktur ausgetauscht, die einen Geschäftsvorfall identifiziert.

Um die Kompatibilität zu älteren EBICS-Versionen zu gewährleisten, sind Anpassungen von Formatparametern und Auftragsarten an BTF-Standards durch Zuordnungsübersichten (Mappings) erleichtert. Auf nationaler Ebene sind Zuordnungsübersichten für Auftragsarten und Formatparameter definiert. Die EBICS-Clients müssen diese Zuordnungen berücksichtigen. In der Übergangszeit kann es zu Mischformen von unterstützten EBICS-Versionen kommen:

- clientseitig

  Bank A unterstützt z. B. bereits BTF, während Bank B nur EBICS 2.x anbietet. Die Bankzugänge in einem EBICS-Client sollten auf die jeweilige Version des Bankrechners ausgerichtet sein.

- serverseitig

  Die Mitarbeiter eines Kunden nutzen EBICS-Clients mit unterschiedlichen Versionen. Während der Einreicher mit einer älteren Version per

Auftragsart einen Auftrag einreicht, unterschreibt ein weiterer Mitarbeiter mit einem EBICS-3.0-Client den Auftrag in der VEU per BTF.

6.3 Verteilte Elektronische Unterschrift (VEU)

Die Verteilte Elektronische Unterschrift (VEU) ist die wohl bedeutendste Anwendungsfunktion in EBICS. Getrieben von vorhandenen Marktprodukten fand diese Erweiterung Eingang in die EBICS-Spezifikation.

Durch die Verteilte Elektronische Unterschrift wird es möglich, dass die Einreichung eines Auftrags – der ggf. bereits mit einer ersten Unterschrift versehen ist – von der eigentlichen Freigabe getrennt werden kann. Eine Signaturdatei kann zeitlich und örtlich getrennt vom Auftrag eingereicht werden. Die Verbindung zwischen beiden Dateien wird über eine Auftragsnummer bzw. Auftrags-ID hergestellt.

Das Verfahren läuft folgendermaßen ab:

- Ein Teilnehmer reicht einen Auftrag z. B. mit der Auftragsart CCT ein und fügt ggf. eine eigene bankfachliche EU mit der Unterschriftsklasse A hinzu.
- Institutsseitig wird der Auftrag geprüft und festgestellt, ob noch weitere Signaturen erforderlich sind. In diesem Fall wird der Auftrag samt Hashwert im Institut zwischengespeichert.
- Ein zweiter Teilnehmer möchte nun den Auftrag freigeben und hat auf alternativem Weg die benötigten Daten wie Auftragsnummer und Hashwert erhalten (Die Bereitstellung der Auftragsnummer und des Hashwerts liegt außerhalb EBICS und ist nicht Bestandteil der institutsseitigen Server-Komponenten).

  Er hat nun folgende Möglichkeiten:

  - Er fragt mit Auftragsart HVU oder HVZ die für ihn zur Unterschrift vorliegenden Aufträge ab und erhält eine Übersicht geliefert, die unter anderem die Auftragsart, geleistete und fehlende Signaturen und die Länge des unkomprimierten Auftrags enthält.
  - Über die Auftragsart HVD kann er sich zu den Aufträgen einzeln noch weitere Details wie Begleitzettelinformationen und den Hashwert über die Aufträge übertragen lassen.

    Dieser Schritt entfällt, wenn die Übersicht mit der Auftragsart HVZ abgeholt wurde, da HVZ bereits alle erforderlichen Detailinformationen liefert.
  - Mit der optionalen Auftragsart HVT liefert das Institut auf Anfragen des Teilnehmers Informationen wie z. B. Einzeltransaktionen des Auftrags, Verwendungszwecke bis hin zum gesamten Auftrag.
- Nach Analyse der vorliegenden Aufträge hat der Teilnehmer nun eine der folgenden Möglichkeiten:
  - Signatur mit Auftragsart HVE

- Stornierung mittels HVS

Die folgende Abbildung, die der Darstellung in der *Spezifikation für die EBICS-Anbindung* [1] nachempfunden ist, gibt einen verständlichen Überblick über die doch etwas komplexen Zusammenhänge:

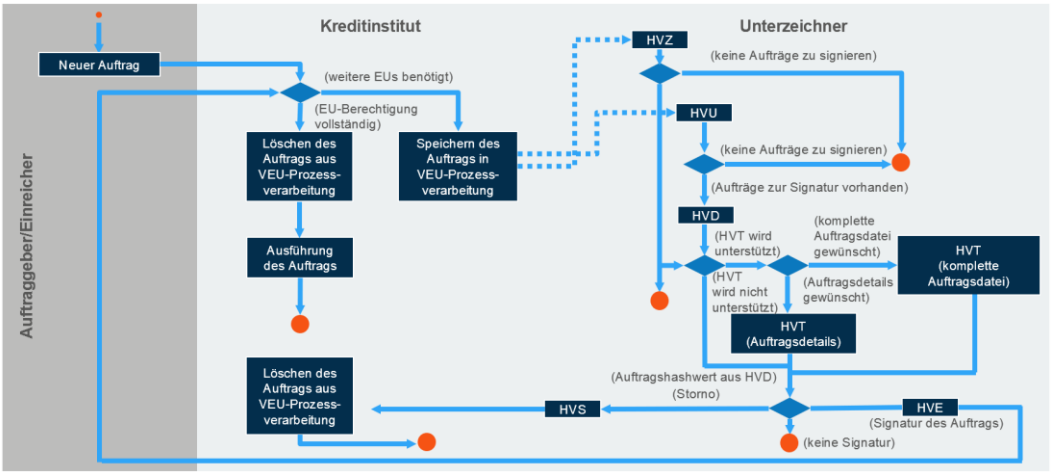


Abbildung 8: Abläufe beim VEU-Verfahren

Während die VEU in Deutschland gut verbreitet genutzt wird, ist sie in Frankreich und der Schweiz bisher nicht üblich, soll mit EBICS 3.0 aber ebenfalls eingeführt werden.

In Frankreich ist es üblich, die Signaturen mit dem Auftrag zu schicken. Bei EBICS-Profil TS wird bei einem Auftrag abhängig von der Anzahl der Signaturen folgendermaßen reagiert:

- Eine Signatur am Auftrag: Der Auftrag ist mit einer Signatur vollständig autorisiert und wird ausgeführt.
- Zwei Signaturen am Auftrag: Im Anwendungssystem wird entschieden, ob die zweite Signatur benötigt wird und ob der Auftrag ausreichend autorisiert ist. Dort wird auch entschieden, ob der Auftrag z. B. auch ausgeführt wird, falls einer der beiden Unterzeichner keine Berechtigung besitzt.
- Eine Signatur am Auftrag, zweite Signatur abhängig vom Limit: Im Anwendungssystem wird entschieden, ob der Auftrag ausreichend autorisiert ist oder ob abhängig vom Limit eine zweite Signatur notwendig ist.

Mit Einführung von EBICS 3.0 kann es während der Migrationsphase zu Mischverträgen aus Auftragsarten und BTF kommen. Um auf bestehenden Berechtigungsmodellen aufsetzen zu können, müssen bestimmte Rahmenbedingungen für BTF-Aufträge (hier BTU für die Einreichung) eingehalten werden wie z. B.:

- BTU muss nicht mit dem des Auftrags übereinstimmen, aber an derselben Auftragsart konfiguriert sein.
- BTU wird für die Abfrage der Unterschriftenmappe verwendet.
- Leere Felder im BTF-Filter sind laut Spezifikation Wildcards:

Es werden alle passenden Aufträge aus der Unterschriftenmappe geliefert (Es ist nicht möglich, mit einem leeren Feld ein bestimmtes BTU zu adressieren).

- BTU aus dem HVx wird in Exits nicht zusätzlich zum Auftrags-BTU gemeldet.

6.4 Portalsysteme

Obwohl in der EBICS-Spezifikation nirgends der Begriff Portal explizit auftaucht, ergibt sich durch die Verwendung der Authentifikationssignatur die Möglichkeit der Einbindung von Dritten bei der Einreichung von Aufträgen. Dabei geht EBICS nicht so weit wie FinTS, wo Portalbetreiber oder Intermediäre mit einer eigenen Rolle versehen sind – die Trennung von Einreicher (Technischer Teilnehmer) und Auftraggeber(n) lässt jedoch die Abbildung einfacher Portalszenarien zu. Durch die Verwendung der Unterschriftsklasse T wird diese Transportinstanz auch mit dazu passenden Regeln versehen.

6.5 Optionale Funktionen

Bereits in den vorangegangenen Abschnitten war die Rede davon, dass bestimmte Funktionen wie z. B. Recovery oder die Detailabfrage bei VEU optionalen Charakter haben. Einige spezielle Funktionen aus diesem Portfolio sollen jetzt kurz vorgestellt werden.

6.5.1 Vorabprüfung

Wie im Abschnitt *EBICS-Abläufe* auf Seite 41 detaillierter beschrieben, läuft eine EBICS-Transaktion in zwei Schritten ab. Im ersten Schritt wird mithilfe einer kurzen Nachricht, der Initialisierung, die Vorbereitung für einen – unter Umständen recht umfangreichen – Filetransfer getroffen.

In diesem Schritt ist es nun optional möglich, bei Upload-Transaktionen in bestimmtem Umfang Vorabprüfungen durchzuführen und einen unberechtigten Transfer gar nicht erst zuzulassen. Folgende Details können im Rahmen der Vorabprüfung verifiziert werden:

- Kontoberechtigungsprüfung
- Limitprüfung
- EU-Verifikation auf Basis des mitgelieferten Hashwerts der Datei

Der mögliche Umfang der Vorabprüfung hängt davon ab, welche dieser Prüfungen konkret vom Institut unterstützt werden und welche Informationen das Kundenprodukt liefert bzw. liefern kann. Es handelt sich hierbei also nicht um die Abwehr von Angriffen, sondern um eine Funktionalität zur Erhöhung der Betriebssicherheit und der Optimierung von Ressourcenbedarf, da nicht korrekte Datei-Uploads überhaupt nicht erst gestartet werden.

6.6 Teilnehmerdaten

Das folgende Set von Auftragsarten ermöglicht es dem Kundenprodukt, Informationen über die getroffenen Vereinbarungen vom Institut abzuholen:

- HAA abrufbare Auftragsarten abholen
- HPD Bankparameter abholen
- HKD Kunden- und Teilnehmerdaten des Kunden abholen
- HTD Kunden- und Teilnehmerdaten des Teilnehmers abholen

Über diese optionalen Auftragsarten kann ein Teilnehmer sein Kundenprodukt korrekt für den Zugang vorbereiten bzw. kann das Kundenprodukt lokal eine zum Teilnehmer passende Umgebung einrichten, indem es z. B. nur die unterstützten Auftragsarten anzeigt.

Bei der Übermittlung wird außer den eigentlichen Zugangsparametern wie URL und Institutsname auch übertragen, welche optionalen Funktionen wie z. B. Vorabprüfung oder Recovery vom Institut unterstützt werden.

Die Kunden- und Teilnehmerdaten informieren über folgende Details der Geschäftsvereinbarungen:

- Kundeninformationen, z. B. Adressdaten
- Kontoinformationen, z. B. Kontonummern und Währungen
- zugelassene Auftragsarten
- Teilnehmerattribute, z. B. Teilnehmer-ID und Unterschriftsklasse

Mit diesen sehr detaillierten Informationen kann ein Kundenprodukt eine vollautomatische Konfiguration der lokalen Umgebung durchführen. Durch ebenfalls enthaltene Statusinformationen ist auch im Fehlerfall eine gezielte Analyse möglich.

6.7 Echtzeitbenachrichtigungen

Es zeigt sich, dass auch Firmenkunden für ihre Geschäftsmodelle immer häufiger zeitnahe Benachrichtigungen über Zahlungseingänge in Echtzeit benötigen. Dieser Trend ist nicht zuletzt auch den Instant-Payments-Prozessen zu verdanken. Bei der EBICS-Kommunikation geht die Initiative stets vom Firmenkunden (EBICS-Client) aus. Der EBICS-Server einer Bank reagiert nur auf eingehende Anfragen (Inbound), initiiert jedoch selbst keinen Austausch. Wie soll jedoch eine Information zeitnah von der Bank an den Kunden übermittelt werden? Dazu hat sich die DK auf die Umsetzung einer Schnittstelle für Echtzeitbenachrichtigungen verständigt, über die unter Beibehaltung des EBICS-Rollenmodells ein Abholprozess des Kundensystems bankseitig angestoßen werden kann (siehe Anlage 2 *Anlage 2: Spezifikation „Echtzeitbenachrichtigungen“* [9]). Für die ausgehende Kommunikation (Outbound) von der Bank zum Firmenkunden wird dazu ein Pushdienst auf Basis von WebSocket genutzt, der als zentrale Komponente für das aktive Senden von Benachrichtigungen an EBICS-Kunden und –Teilnehmer fungiert.

6.8 EBICS im Interbank-Betrieb

Eine weitere Form des EBICS-Einsatzes ist die Verwendung im Interbank-Betrieb zum Austausch des Massenzahlungsverkehrs (SEPA-Zahlungen) sowie für Instant-Payments-Zahlungen.

6.8.1 Anbindung an den SEPA-Clearer der Deutschen Bundesbank

In Deutschland werden im bilateralen Clearing die früher oft herstellerbasierten Lösungen zunehmend durch den offenen Standard EBICS abgelöst.

Ein Szenario im Interbankenverkehr ist die Anbindung der Institute an die Bundesbank. Die Bundesbank bietet hierzu mit SEPA nur noch zwei Schnittstellen an:

- EBICS mit SEPA pacs messages
- SWIFT FileAct

Die Bundesbank hat eigene Auftragsarten in EBICS eingebracht und Formatfestlegungen (z. B. für PTKs) getroffen.

6.8.2 Anbindung an die STEP2-Plattform der EBA Clearing

Ein weiteres Szenario im Interbankenverkehr für SEPA-Zahlungen ist die Anbindung von Banken an STEP2 der EBA Clearing. Diesen Zugang bietet die EBA Clearing den angeschlossenen Banken seit Ende 2013 alternativ zum SWIFT-Zugang auch über EBICS (ab EBICS 2.5) an. Auch die EBA Clearing hat für den Datenaustausch per EBICS eigene Auftragsarten in EBICS eingebracht und Formate spezifiziert.

6.8.3 Bilateraler Interbankenaustausch („Garagen-Clearing“)

Für den direkten bilateralen Austausch zwischen Banken gibt es keine Vorgaben in der EBICS-Spezifikation. Grundsätzlich treffen die Partner ihre Vereinbarungen bilateral. Diese Vereinbarungen betreffen neben dem Umgang mit Rückläufern (R-Transaktionen) auch geschäftspolitische Fragen wie den Haftungsübergang oder spezifische SLAs (z. B. maximale Dateigrößen).

Für Auftragsarten und technische Regelungen werden üblicherweise die Regelungen der EBA Clearing für die STEP2-Anbindung übernommen.

6.8.4 Instant Payments

Instant Payments, auch als ‘immediate’ oder ‘real-time’ Payments bezeichnet, stellen den nächsten Schritt bei der Harmonisierung von Zahlungen innerhalb des SEPA-Raums dar, mit dem Ziel, Europas Wettbewerbsfähigkeit und Wirtschaftswachstum zu unterstützen. Nachdem die Umstellung auf SEPA-Überweisungen und –Lastschriften nahezu vollzogen ist und die Digitalisierung der gesamten Wirtschaft zu neuen Erwartungen bei Kunden und Händlern führt,

werden Instant Payments den Schwerpunkt des European Payment Council (EPC) für die nächsten Jahre darstellen.

Herzstück ist ein neues SEPA Instant Credit Transfer (SCT Inst) Schema. Dieses bietet durch spezielle Belegung des Standard-SEPA-Überweisungsschemas eine starke Verbindung zum bestehenden SEPA-Zahlungsverkehr und den bereits etablierten Prozessen und Implementierungen. Obwohl das Schema selbst nur Euro unterstützt, können Belastungs- und Zielkonten natürlich auch in anderen Währungen geführt sein.

Die EBA Clearing bietet auf Basis der SCT Inst einen Instant-Payments-Service (RT1) seit November 2017 auf europäischer Ebene an. Die EZB plant ab Herbst 2018 den Target Instant Payments Service (TIPS). Daneben sind noch lokale Verfahren in einzelnen Ländern produktiv.

Eine Haupteigenschaft von Instant Payments ist die Zeitdauer zwischen dem Übertragen eines validierten SCT Inst Auftrags von der Bank des Auftraggebers bis zur Rückmeldung der Bank des Begünstigten. Diese Zeitdauer darf im Normalfall 10 Sekunden nicht überschreiten. Tritt in einem Ausnahmefall ein Timeout auf, so sind im Rulebook Regelungen für Statusabfragen getroffen. In jedem Fall wird bis zu einer negativen Rückmeldung durch die Bank des Begünstigten davon ausgegangen, dass die Zahlung erfolgreich durchgeführt werden wird. Dabei wird vorausgesetzt, dass alle beteiligten Systeme eine 24/7/365-Verfügbarkeit besitzen.

Eine einzelne Instant-Payments-Zahlung ist aus Sicherheitsgründen auf 15.000 Euro limitiert, es können bilateral höhere Beträge vereinbart werden. SEPA Instant Payments ist innerhalb der 34 Länder des SEPA-Raums gegeben. Die Unterstützung von SCT Inst ist derzeit für Banken nicht verpflichtend. Für das Zustandekommen einer Instant-Payments-Zahlung ist die Unterstützung dieser Funktion bei der Bank des Begünstigten Voraussetzung.

Als Zugangskanal zum RT1-Service bietet die EBA Clearing sowohl das SiaNet als auch EBICS (ab EBICS 2.5) an. Analog zur Step2-Anbindung stellt die EBA Clearing einen Implementation Guide für die Anbindung über EBICS zur Verfügung. Die Instant-Payments-Messages werden hierbei einschrittig via EBICS, die dateibasierten Reports analog dem STEP2 via EBICS übertragen. Für die einschrittige, nachrichtenbasierte Nutzung von EBICS 3.0 im RT1-Service wurde eigens eine Spezifikation in Form eines Deltadokumentes erstellt (siehe *Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)* [8]) und auf der EBICS-Webseite (www.ebics.de bzw. www.ebics.org) veröffentlicht.

7 EBICS-Abläufe

Nach dieser Beschreibung der Funktionalitäten, die in EBICS enthalten sind, folgt nun im letzten fachlichen Absatz die Darstellung der eigentlichen Protokollabläufe.

Eine abgeschlossene Verarbeitungseinheit wird hierbei als Transaktion bezeichnet. EBICS unterscheidet grundlegend zwischen Upload- und Download-Transaktionen. Upload-Transaktionen dienen beispielsweise zur Einreichung von Aufträgen, Download-Transaktionen z. B. zum Abholen von Kontoumsätzen.

Transaktionen sind unterteilt in Transaktionsphasen und -schritte. Folgende Transaktionsphasen sind möglich:

Upload-Transaktion	Download-Transaktion
Initialisierung	Initialisierung
Datentransfer	Datentransfer
–	Quittierung

In den Transaktionsphasen können wiederum mehrere Schritte enthalten sein, die jeweils aus einem EBICS-Request und zugehörigem –Response bestehen. Während die Initialisierungsphase aus nur einem Schritt besteht, kann die Datentransferphase aufgrund von Segmentierung mehrere Schritte enthalten.

Eine Transaktion wird grundsätzlich vom Kundenprodukt initiiert. Das System auf Institutsseite kann nur initiierend eingreifen, indem es z. B. dem Kundensystem nach einem Abbruch einen Wiederaufsetzpunkt (Recovery) mitteilt.

Die Verbindung der einzelnen Transaktionsphasen untereinander geschieht über eine Transaktions-ID, die vom Banksystem generiert und im Initialisierungs-Response mitgeteilt wird.

Jeder EBICS-Request und jede EBICS-Response enthält die Authentifikationsunterschrift des Kunden/Teilnehmers bzw. des Instituts.

Die folgende Abbildung zeigt den Ablauf einer EBICS-Transaktion:

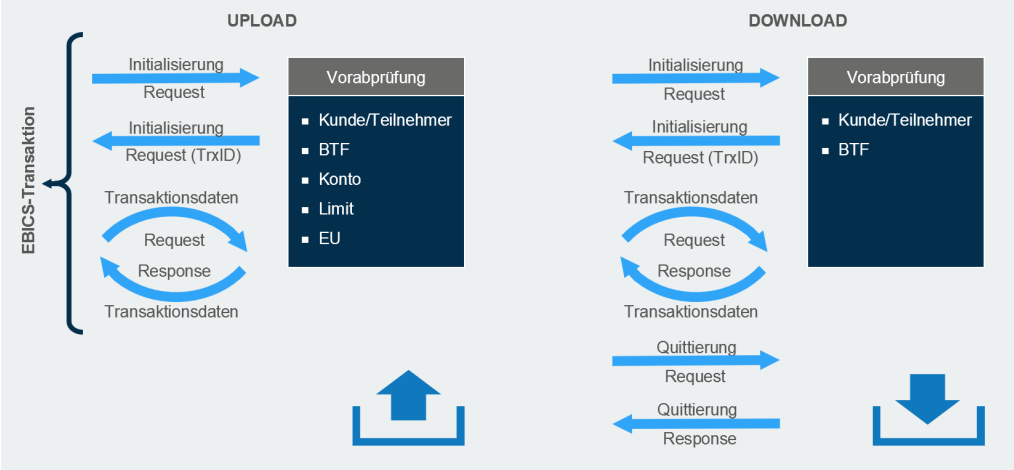


Abbildung 9: Ablauf einer EBICS-Transaktion

8 Positionierung im internationalen Umfeld

EBICS als Erweiterung des deutschen DFÜ-Abkommens schreibt die Kommunikations- und Sicherheitsdefinitionen für Massenzahlungsverkehr im Firmenkundengeschäft fest. Es gibt sowohl im nationalen als auch im internationalen Umfeld Standards vor, die ergänzend und überlappend mit EBICS zu sehen sind. Einige davon werden im Folgenden kurz dargestellt und zu EBICS in Bezug gesetzt.

8.1 FinTS

FinTS (Financial Transaction Services, vormals HBCI – Homebanking Computer Interface) ist ebenfalls ein DK-Standard, der jedoch seinen Schwerpunkt auf Online-Banking mit Privat- und Gewerbekunden setzt. FinTS bildet in seiner klassischen Form Dialoge zwischen Kunde und Institut ab und verarbeitet nachrichtenorientierte Einzeltransaktionen. Funktionalitäten wie Bank- oder User-Parameterdaten sind in FinTS vergleichbar zu EBICS enthalten.

In seiner neuesten Version 4.1 setzt auch FinTS konsequent auf Internet-Standards wie http oder XML. Auch die Kommunikationsverfahren wurden um dialogfreie, so genannte Datagramme und die Bank-Kunde-Kommunikation erweitert.

FinTS unterstützt im Sicherheitsbereich ebenfalls elektronische Signaturen, alternativ aber auch das PIN/TAN-Verfahren in unterschiedlichen Ausprägungen.

Wie in EBICS werden auch von FinTS die gängigen Finanzdatenformate wie SEPA, camt, DTAZV und SWIFT unterstützt – sie werden dort als Geschäftsvorfälle bezeichnet. Auch Instant Payments ist in FinTS enthalten. Die DK sorgt mittlerweile auch dafür, dass Versionen und Inhalte dieser Formate von beiden Standards in gleicher Weise genutzt werden. Zusätzlich verfügt FinTS aber über die Möglichkeit, zahlreiche eigene Geschäftsvorfälle zu definieren, die von Daueraufträgen über Termingeld bis zu freien Mitteilungen an das Institut reichen. Diese Geschäftsvorfälle schaffen (wenigstens) einen nationalen Standard überall dort, wo eine internationale Definition fehlt.

Im Bereich der gewerblichen Kunden steht dem Kunden in FinTS, außer den zu EBICS identischen Geschäftsvorfällen z. B. für Sammler oder Kontoumsätze, eine eigene Implementierung der Verteilten Elektronischen Unterschrift (VEU) zur Verfügung. Was dem Standard momentan fehlt, sind all die Möglichkeiten des Massenzahlungsverkehrs wie Segmentierung oder Recovery.

Zusammenfassend muss man FinTS als Ergänzung zu EBICS positionieren. Dies gilt überall dort, wo Gewerbe- oder Firmenkunden als gemeinsame Zielgruppe betrachtet werden müssen, da sie in beiden Welten ihre Finanzgeschäfte tätigen. So wird ein Unternehmen sowohl Massenzahlungen durchführen als auch im Anlagen- oder Wertpapiergeschäft tätig sein. Bei einigen Geschäftsarten wird es sogar ausschlaggebend sein, wo ein Geschäft getätigt wird, in der Buchhaltungsabteilung oder von einem Geschäftsführer unterwegs.

Moderne Kundenprodukte haben sich bereits auf diese Situation eingestellt und bieten mit EBICS und FinTS bereits zwei Kommunikationsverfahren an.

Zur tieferen Betrachtung von FinTS empfiehlt sich die Lektüre des FinTS-Kompendiums, das unter *fints.org* zum Download bereitsteht:

8.2 SWIFT

Im Zusammenspiel von EBICS und SWIFT sind folgende Strukturen zu nennen:

- klassische FIN-Formate im internationalen Zahlungsverkehr
- XML- und ISO-Aktivitäten von SWIFT
- SWIFTNet als eigener Kommunikationsstandard
- SWIFT FileAct als eigener Filetransfer-Standard

Zu den klassischen FIN-Formaten, wie z. B. MT940, lässt sich nicht viel bemerken. Sie sind stabil, nur noch gesetzlichen Änderungen unterworfen und werden in den beiden relevanten deutschen Standards EBICS und FinTS in gleicher Weise in das jeweilige Protokoll eingepackt. Dadurch ergibt sich auch eine gewisse Unabhängigkeit von SWIFT, da nur mit Referenzierungen gearbeitet wird.

Die Tatsache, dass mit SWIFT XML auch eine XML-basierte Version der Formate zur Verfügung steht, ändert nichts an der klaren Aufgabentrennung zwischen den Standards. Bedeutender ist hierbei, dass SWIFT bei der Erzeugung der XML-Formate sehr abstrakt vorgegangen ist und quasi ein Reverse Engineering der bestehenden Welt durchgeführt hat. Es wurden nämlich in jahrelanger Kleinarbeit mittels UML Prozessmodelle für den internationalen Zahlungsverkehr angefertigt, die heute nur als Ableitungen die FIN- und XML-Formate erzeugen. Durch diesen methodischen Ansatz hat sich SWIFT auch in der Konkurrenz internationaler Zahlungsverkehrsstandards nach vorne geschoben und hat es geschafft, die Kernkomponenten dieser Modelle als ISO-Standard 20022 zu positionieren.

Während die ISO-Bestrebungen von SWIFT die weitere Entwicklung der Zahlungsverkehrsformate sehr stark beeinflussen dürften, ist das zugehörige Transportprotokoll, das die Grundlage für SWIFTNet bietet, eher von untergeordneter Bedeutung und als proprietäre Entwicklung zu sehen. Sicherlich hat SWIFTNet einen stabilen Verbreitungsgrad im Interbankengeschäft – in der Kunde-Bank-Beziehung spielt es jedoch so gut wie keine Rolle.

Dadurch lässt sich der SWIFT-Standard in seiner bedeutenden Rolle als Instanz zur Herausgabe und Pflege von Zahlungsverkehrsformaten einordnen. Seine Positionierung zu EBICS ist damit auch eindeutig beschrieben und dürfte für die nächsten Jahre auch stabil bleiben.

Mit dem Einbeziehen Frankreichs in die SEPA-Gesellschaft hat sich auch der Einfluss von SWIFT verstärkt, da dieser Standard in Frankreich eine große Rolle spielt. Auch SWIFT FileAct ist als Filetransferprotokoll vermehrt anzutreffen. Trotzdem gilt, dass es sich bei SWIFT (siehe *swift.com*) und EBICS um ein harmonisches Nebeneinander handelt.

8.3 PeSIT-IP

Der französische Herstellerstandard PeSIT kann als Komplementärstandard zu EBICS insbesondere im Interbankenverkehr, z. T. aber auch für große Unternehmen betrachtet werden. Auch mit PeSIT können Massenzahlungen eingereicht und Umsatzdaten ausgeliefert werden. Firmenkunden in Frankreich setzen oft Produkte ein, die neben EBICS auch ein PeSIT-IP-Modul besitzen.

8.4 SFTP und FTP(S)

Die auf FTP basierenden Filetransfer-Verfahren werden in Europa auch im Zahlungsverkehr vereinzelt eingesetzt. Anders als die bisher diskutierten Verfahren, regeln sie allerdings nur den Transport, nicht jedoch irgendeine Art von fachlicher Verarbeitung. Auch die Sicherheit der Verfahren hält heutigen Anforderungen an den Zahlungsverkehr nicht Stand. Durch die breite Verfügbarkeit als Systemsoftware kommt SFTP oder FTPS oft beim allgemeinen Filetransfer zum Einsatz.

8.5 Ausblick

Dieser Beschreibung von Standards lässt sich entnehmen, dass es – auch im internationalen Bereich – derzeit keine vergleichbaren Industriestandards gibt.

Daraus wird erkennbar, dass EBICS in Zukunft der bestimmende Standard im Massenzahlungsverkehr in Europa und darüber hinaus sein wird. Dies wird dadurch erhärtet, dass außer den bisherigen Partnern der EBICS-Gesellschaft (Deutschland, Frankreich und Schweiz) auch in anderen Ländern wie Österreich, Spanien, Italien, Portugal und Irland zunehmend EBICS seitens der Banken unterstützt wird. Diese Entwicklung wird durch Einführung von EBICS 3.0 und der damit verbundenen Harmonisierung noch erleichtert.

Als weiterer Motivator für die Einführung von EBICS in weiteren EU-Staaten kann Instant Payments dienen, da hier eine europaweit einheitliche Verarbeitung für alle Beteiligten Vorteile bringen wird.

Der abschließende Abschnitt zeigt nun, wie eine beispielhafte EBICS-Implementierung und Migration auf Basis einer konkreten Produktfamilie aussehen kann.

9 Umsetzung

Nach dem Überblick über die Funktionalität von EBICS und der Darstellung des Gesamtszenarios soll im letzten Abschnitt eine Umsetzung im Mittelpunkt stehen, die zeigt, dass und wie das Zusammenspiel von alt und neu funktionieren kann.

Dazu wird im Folgenden die Produktfamilie TRAVIC (Transaction Services) vorgestellt, deren einzelne Bausteine zum Aufbau eines solchen Gesamtszenarios dienen können.

TRAVIC besteht aus folgenden Bestandteilen, die je nach Bedarf kombiniert werden können:

Komponente	Beschreibung
TRAVIC-Corporate	umfasst vollständig die Funktionalitäten auf Institutsseite zur Abbildung von EBICS und EBICS Interbank und darüber hinaus die Kanäle PeSIT und SFTP/FTP(S)
TRAVIC-Port	Implementierung eines EBICS-Portals zur Abwicklung von Zahlungsverkehrsdienstleistungen
TRAVIC-Interbank	bietet die Möglichkeit, Zahlungen per EBICS bei den europäischen Clearinghäusern oder bei Instant Payments über EBA Clearing einzureichen
TRAVIC-Link	stellt ein übergreifendes Filetransfer-Portfolio zur Verfügung, mit dem z. B. Aufträge über EBICS oder andere Filetransferverfahren, versehen mit bankfachlichen Elektronischen Unterschriften, vollautomatisch an ein Institut weitergeleitet werden können
TRAVIC-EBICS-Mobile	gibt Benutzern die Möglichkeit, Auftragsdateien des nationalen und internationalen Zahlungsverkehrs, die im Kreditinstitut vorliegen, von unterwegs freizugeben, d. h. zu signieren
TRAVIC-Push-Server	aktive Information des Kunden zu EBICS-Aufträgen an seine App, E-Mail, WebSocket oder über andere Wege
TRAVIC-Retail	rundet den Baukasten ab und stellt alle Kernfunktionalitäten für ein institutsseitiges FinTS-System zur Verfügung
TRAVIC-Services-APIs für EBICS	hilft bei der Umsetzung von EBICS in Kundenprodukten durch eine TRAVIC-Services-API für EBICS und die TRAVIC-EBICS-API, die eine komplette und leicht verständliche EBICS-Suite für die Kundenseite zur Einbindung bereitstellt

Komponente	Beschreibung
Target Instant Payment Settlement (TIPS)	beinhaltet Clearing- und Settlementfunktionen für Instant Payments

Bis auf TRAVIC-Retail, das in diesem Zusammenhang nicht betrachtet wird, werden die einzelnen Bausteine im Folgenden detaillierter vorgestellt.

9.1 TRAVIC-Corporate

TRAVIC-Corporate stellt alle in EBICS beschriebenen Funktionen zur Verfügung, also auch die optionalen Funktionen. Zusätzlich erhältliche Tools ermöglichen auch die Übernahme von Stammdaten und kryptografischen Schlüsseln aus Produkten anderer Hersteller im Rahmen einer Migration:

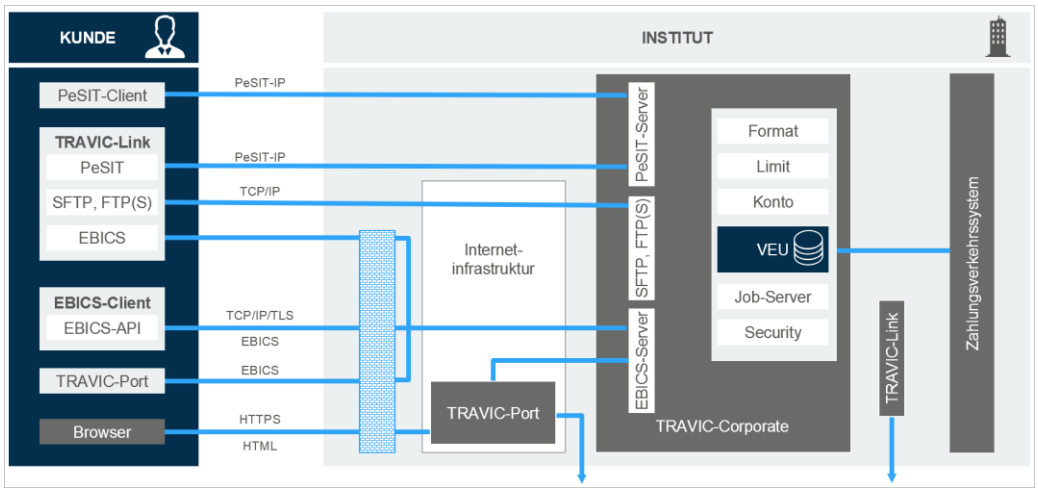


Abbildung 10: Komponenten der TRAVIC-Produktfamilie

TRAVIC-Corporate steht auf mehreren Unix-Plattformen und Linux zur Verfügung, um für jeden Einsatzzweck die optimale Umgebung auswählen zu können.

9.2 TRAVIC-Port

Im Bereich der verteilten Signatur sowie bei geringer Anzahl von zu erfassenden und einzureichenden Aufträgen ist eine Portaleinbindung mit EBICS eine ideale Ergänzung des Leistungsangebotes einer Bank. Daher ist es kein Wunder, dass immer mehr Institute Firmenkundenportale in ihr Internet-Banking-Portfolio aufnehmen.

TRAVIC-Port verwendet einen EBICS-Protokollbaustein, den so genannten E-BICS-Kernel, als Herzstück für die multibankfähige Kommunikation. Diese Kernfunktionen werden angereichert durch Webservices für den fachlichen

Aufbau von Zahlungsverkehrsgeschäftsvorfällen und eine Benutzerprofilverwaltung, mit deren Hilfe Kunden administrative Aufgaben erledigen können.

Um die Integration in vorhandene Internet-Banking-Lösungen zu erleichtern, erfolgt die Visualisierung der Portalfunktionen über Webservice-Schnittstellen, d. h., die Präsentation kann durch das Institut bzw. dessen IT-Dienstleister selbst vorgenommen werden. Auch verfügt TRAVIC-Port über Single Sign-on-Funktionalität, welche die Integration von Portalen in TRAVIC-Port ermöglicht und umgekehrt.

Mit diesen Mitteln ist es mit wenig Implementierungsaufwand möglich, den transaktionsabhängigen Teil eines Firmenkundenportals aufzubauen und durch weitere fachliche Funktionen anzureichern.

9.3 TRAVIC-Interbank

EBICS im Interbankenverkehr zeichnet sich insbesondere durch gleichartige Rollen beider Kommunikationspartner aus. Jeder Partner verfügt über einen EBICS-Server und einen EBICS-Client. TRAVIC-Interbank verfügt über die Komponenten für beide Rollen. Autorisierungen des Datenaustausches erfolgen direkt mit dem Datentransfer. TRAVIC-Interbank unterstützt die folgenden Einsatzszenarien:

- Interbank-, Bundesbankverfahren, den Austausch des Elektronischen Massenzahlungsverkehrs SEPA-Clearer der Deutschen Bundesbank oder STEP2 der EBA-Clearing per EBICS
- TRAVIC-Interbank für Instant Payments RT1 der EBA Clearing
- TRAVIC-Interbank für Request to Pay R2P der EBA Clearing

9.4 TRAVIC-Link

TRAVIC-Link ist ein universelles Filetransfer-Produkt, das in unterschiedlichen Szenarien eingesetzt werden kann.

Im Umfeld des elektronischen Zahlungsverkehrs für das Firmenkundengeschäft übernimmt TRAVIC-Link die Rolle der so genannten Kundensysteme gemäß dem DFÜ-Abkommen mit Kunden. In diesen Szenarien unterstützt TRAVIC-Link die Standards BCS und EBICS. Hier ergänzt TRAVIC-Link Finanzbuchhaltungssysteme um die automatische Übertragung von Aufträgen und um die automatische Abholung und Weiterleitung von Kontoumsatzdateien. An ein Institut zu übertragende Auftragsdateien können im Vorfeld der Übertragung mit Elektronischen Unterschriften versehen werden.

Das in TRAVIC-Link integrierte Kommunikationsprotokoll ONGUM-IP ermöglicht Übertragungen von Dateien beliebigen Inhalts zwischen mehreren TRAVIC-Link-Systemen.

Eine weitere Funktionalität von TRAVIC-Link ist die Kommunikation über so genannte Standardsoftware. Hierzu bietet TRAVIC-Link entsprechende Schnittstellen an.

Die folgenden Kommunikationsverfahren bzw. Kommunikationsmodule werden derzeit von TRAVIC-Link unterstützt.

Electronic Banking im Firmenkundenumfeld

- EBICS
- PeSIT-IP

Integrierte Filetransfer-Verfahren

- ONGUM-IP
- Secure-FTP
- HTTP
- JMS
- FTP(S)

Über Schnittstellen integrierbare Standardsoftware

- Connect:Direct (Sterling Commerce)
- UDM (Stonebranch)

9.5 TRAVIC-EBICS-Mobile, TRAVIC-Push-Server

TRAVIC-EBICS-Mobile ist eine mobile Anwendung zum Signieren von Zahlungsaufträgen, die bei Kreditinstituten über das EBICS-Verfahren eingereicht wurden.

Weiterhin können Kontoinformationen (Salden und Umsätze) angezeigt werden.

Die Anwendung richtet sich an Banken und große Unternehmen, die ihren Kunden bzw. Mitarbeitern die Möglichkeit bieten wollen, mobil, also außerhalb des jeweiligen Unternehmensstandorts, Zahlungsaufträge freizugeben.

TRAVIC-EBICS-Mobile ist:

- multibankfähig aufgrund standardisierter Schnittstellen und konsequenter Nutzung des EBICS-Standards im Gateway-Server
- individuell konfigurierbar
- sicher im Betrieb durch Elektronische Unterschriften und verschlüsselten Nachrichtentransfer
- pushfähig durch Banken, die TRAVIC-Corporate mit dem TRAVIC-Push-Server betreiben

TRAVIC-Push-Server dient der ausgehenden Kommunikation (Outbound) von der Bank zum Firmenkunden. Er fungiert als die zentrale Komponente für das aktive Senden von Benachrichtigungen über die präferierten Kommunika-

tionskanäle der EBICS-Kunden und –Teilnehmer. Neben den Push-Kanälen Mobile und E-Mail bietet der TRAVIC-Push-Server gemäß der neuen *Anlage 2: Spezifikation „Echtzeitbenachrichtigungen“* [9] die Signalisierung der Informationen in Echtzeit über eine WebSocket-Schnittstelle an.

9.6 TRAVIC-EBICS-API

Während die etablierten Hersteller von Bankrechnern emsig dabei sind, ihre Produkte EBICS-fähig zu machen, stehen die Kundenprodukt-Hersteller vor einem Problem.

Hunderte Seiten an Dokumentation sind umzusetzen und zu integrieren, nur um z. B. ein Zahlungsverkehrsprodukt um einen neuen Transportweg zu ergänzen. Dabei ist es aus heutiger Sicht nicht klar, in welchem Umfang die optionalen EBICS-Features zukünftig genutzt werden, also ob sie von Anfang an zu berücksichtigen sind.

Hierbei hilft eine Services-API für EBICS, die TRAVIC-EBICS-API, die eine komplette und leicht verständliche EBICS-Suite für die Kundenseite zur Einbindung bereitstellt.

Literaturverzeichnis

[1] DFÜ-Abkommen
Anlage 1: Spezifikation für die EBICS-Anbindung
Version 3.0.2 vom 27. Juni 2022
Die Deutsche Kreditwirtschaft

[2] DFÜ-Abkommen
Anlage 2: FTAM-Anbindung
- obsolet -
Die Deutsche Kreditwirtschaft

[3] DFÜ-Abkommen
Anlage 3: Spezifikation der Datenformate
Version 3.6 vom 06.04.2022
Die Deutsche Kreditwirtschaft

[4] EBICS-Implementation Guide (engl.)
basierend auf EBICS-Version 3.0 vom 27. Juni 2022
EBICS Working Group

[5] EBICS-Sicherheitskonzept (nur auf Anfrage)
Version 1.6 vom 3. Februar 2021
Die Deutsche Kreditwirtschaft

[6] Krypto LifeCycle EBICS
Version 1.2 vom 29.04.2022

[7] FinTS V4.1
Version 4.1 vom 12.09.2019
Die Deutsche Kreditwirtschaft

[8] Use of EBICS for the Clearing & Settlement of Instant Payment Transactions (Delta - Concept)
vom 30.10.2019
EBICS Working Group

[9] DFÜ-Abkommen
Anlage 2: Spezifikation „Echtzeitbenachrichtigungen“
Die Deutsche Kreditwirtschaft (DK)
Version 1.0 vom 17.07.2019

Abkürzungsverzeichnis

BCS	Banking Communication Standard
BPD	Bankparameterdaten
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTD	Administrative Auftragsart zum Abholen einer Datei, die durch eine BTF-Struktur näher gekennzeichnet ist
BTF	Business Transaction Formats
BTU	Administrative Auftragsart zum Senden einer Datei, die durch eine BTF-Struktur näher gekennzeichnet ist
CFONB	Comité Français d'Organisation et de Normalisation Bancaire
DFÜ	Datenfernübertragung
DK	Die Deutsche Kreditwirtschaft (vormals →ZKA)
EBICS	Electronic Banking Internet Communication Standard
EDS	Electronic Distributed Signature (siehe auch →VEU)
ETEBAC	Echange TElematique BAnque-Clients
EU	Elektronische Unterschrift
FTP	Filetransfer Protocol
HTTP	Hypertext Transport Protocol
FinTS	Financial Transaction Services
FTAM	Filetransfer Access and Management
HBCI	HomeBanking Computer Interface
IP	Instant Payments
IT	Informationstechnologie
ISO	International Standards Organisation
OAGi	Open Application Group
OSI	Open Systems Interconnect

PSA	Payment Services Austria GmbH
RT1	Instant Payments Service der EBA Clearing
SEPA	Single European Payment Area
SIX	Swiss Infrastructure and Exchange
SRZ	Service-Rechenzentrum
SSL	Secure Socket Layer
TCP/IP	Transport Communication Protocol/Internet Protocol
TLS	Transport Layer Security
UML	Unified Modelling Language
TWIST	Transaction Workflow Innovation Standards Team
VEU	Verteilte Elektronische Unterschrift (siehe auch →EDS)
W3C	World Wide Web Consortium, Gremium zur Standardisierung der Techniken im Internet
XML	Extensible Markup Language
ZKA	Zentraler Kreditausschuss (heute →DK)

Abbildungsverzeichnis

Moorfuhrtweg 13
22301 Hamburg
Tel.: +49 40 227433-0
Fax: +49 40 227433-1333

E-Mail: info@ppi.de
Internet: www.ppi.de