travic

EBICS-Kompendium

Electronic Banking Internet Communication Standard



Dokumentversion: 4.2.3

Datum: 01.11.2013

Weitere Informationen: Michael Lembcke
michael.lembcke@ppi.de

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 im Markt etabliert und hat in der aktuellen Version 2.5 gute Chancen, der europäische Zahlungsverkehrsstandard im Firmenkundengeschäft und im Interbanken-Verkehr zu werden.

EBICS ist seit dem 1. Januar 2008 für die deutschen Banken verpflichtend und hat seit Anfang 2011 die vorherige FTAM-Variante komplett abgelöst. Auch in Frankreich ist die Migration des vorhandenen ETEBAC-Standards nach EBICS im November 2009 offiziell gestartet.

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, sowie die französischen Banken, vertreten durch das Comité Français d'Organisation et de Normalisation Bancaire (CFONB).

Ergänzend zu den Basisfunktionen, der „Internet-Kommunikation" im Firmenkundengeschäft im weitesten Sinne, liefert EBICS neue Features wie z. B. die verteilte Signatur oder die Authentifikationssignatur und ermöglicht auch den Einsatz von Zertifikaten. Gerade die Definitionen für den Aufbau einer PKI-Infrastruktur (Public Key Infrastructure) werden Schwerpunkte von Implementierungen auf Basis der aktuellen EBICS-Version 2.5 sein.

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 Informationstechnologie, Oktober 2013

Dokumentversion 4.2.3 vom 01.11.2013

Inhaltsverzeichnis

1 Einleitung 4

1.1 Anforderungen an EBICS 4

1.2 Aufbau der Spezifikation 6

2 Gesamtszenario EBICS 8

2.1 Zusammenspiel der Verfahren 8

2.2 Berücksichtigung der Produkte 9

2.3 Portale 9

2.4 Migration 9
2.4.1 Migrationsstatus in Frankreich 10

3 Kommunikation und Absicherung der Infrastruktur 11

3.1 HTTPS und TLS – Transport Layer Security 11

3.2 XML – Extensible Markup Language 11

3.3 Optimierung der Kommunikation 13

4 Datenmodell 14

5 Sicherheit 16

5.1 Infrastruktursicherheit 16

5.2 Signaturverfahren 17
5.2.1 Authentifikationssignatur X001 bzw. X002 17
5.2.2 Auftragssignaturen (EU) nach A004 bzw. A005/A006 18

5.3 Initialisierung 19
5.3.1 Zertifikate in Frankreich 19
5.3.1.1 Das Einreicherprofil T auf Basis von Zertifikaten 20
5.3.1.2 Autorisierungsprofil TS 20
5.3.1.3 INI-Brief als Fallback-Szenario 20
5.3.2 INI-Brief-Verfahren in Deutschland 21

5.4 Verschlüsselungsverfahren 21
5.4.1 TLS – Transport Layer Security 21
5.4.2 Verschlüsselung E001 und E002 22

6 Fachliche Funktionen von EBICS 23

6.1 Auftragsarten 23
6.1.1 Inlands- und Auslandszahlungsverkehr / Tagesauszüge 23
6.1.2 SEPA-Zahlungsverkehr 24
6.1.3 Standard Auftragsarten für Upload und Download FUL und FDL 25
6.1.4 Weitere Auftragsarten 26

6.2 Verteilte Elektronische Unterschrift (VEU) 26

6.3 Portalsysteme 28

6.4 Optionale Funktionen 29
6.4.1 Vorabprüfung 29
6.4.2 Teilnehmer-Daten 29

6.5 EBICS im Interbank-Betrieb 30

7 EBICS-Abläufe 31

8 Positionierung im internationalen Umfeld 33

8.1 FinTS 33

8.2 SWIFT 34

8.3 ETEBAC 35

8.4 Ausblick 35

9 Umsetzung 37

9.1 TRAVIC-Corporate 38

9.2 TRAVIC-Link 38

9.3 EBICS-Mobile 39

9.4 TRAVIC-Services-APIs für EBICS 40

9.5 TRAVIC-Web 40

9.6 TRAVIC-Port 40

Literaturverzeichnis 42

Abkürzungsverzeichnis 43

Abbildungsverzeichnis 45

1 Einleitung

1.1 Anforderungen an EBICS

Die grundsätzliche Zielsetzung bei der Schaffung des EBICS-Standards kann mit dem Motto „Evolution statt Revolution“ überschrieben werden.

Dieser Kernsatz galt für die inzwischen in Marktprodukten umgesetzte EBICS-Spezifikation 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 und Frankreich 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 sein.

Die Anforderungen an eine Erweiterung des BCS-Standards (Deutschland) und des ETEBAC-Standards (Frankreich), die im Folgenden nun durchgängig als EBICS bezeichnet werden, sind im Einzelnen:

Anforderung	Beschreibung
Internet	EBICS sollte konsequent auf Internet-Technologien aufsetzen. Dieser Aspekt – ursprünglich nur durch den Kommunikationsbereich getrieben – zieht sich nun konsequent durch die Spezifikation und betrifft außer Kommunikationsstandards wie HTTP und TLS auch Standards wie XML oder XML-Signaturen. Es sollten alle stabilen und geeigneten Internet-Standards verwendet werden.
Sicherheit	Internet lässt sich heute nur noch in einem Atemzug mit dem Thema Sicherheit nennen. Wenn schon der sichere Hafen der quasi geschlossenen Netze, die die bisherigen Standards benutzt haben, verlassen werden sollte, dann jedoch ohne Sicherheitseinbußen. Dies betrifft einige Bereiche der Umsetzung, nämlich (gedanklich mit berücksichtigte) Firewall-Strukturen genauso, wie den Bereich der Signatur und Verschlüsselung, aber auch die Tatsache, dass parallel zur Standardisierung auch ein Sicherheitskonzept erstellt und abgenommen wurde.

Anforderung	Beschreibung
Bandbreite	Einer der größten Vorteile sollte die Entkopplung des Kommunikationsprotokolls vom physischen Netz sein, 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 sollte idealerweise auf die Verarbeitung großer Datenmengen zugeschnitten sein und diese schnell, sicher und wirtschaftlich verarbeiten helfen. 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 sollten auch einige wenige neue Funktionen Einzug halten, im Wesentlichen die örtlich und zeitlich Verteilte Elektronische Unterschrift (VEU). Diese Funktion hatte sich inzwischen über die Marktprodukte bei den Kunden etabliert und sollte nun multibankfähig eingesetzt werden können.
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.
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 sollten aber auch konkrete Verpflichtungen eingegangen werden, 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.

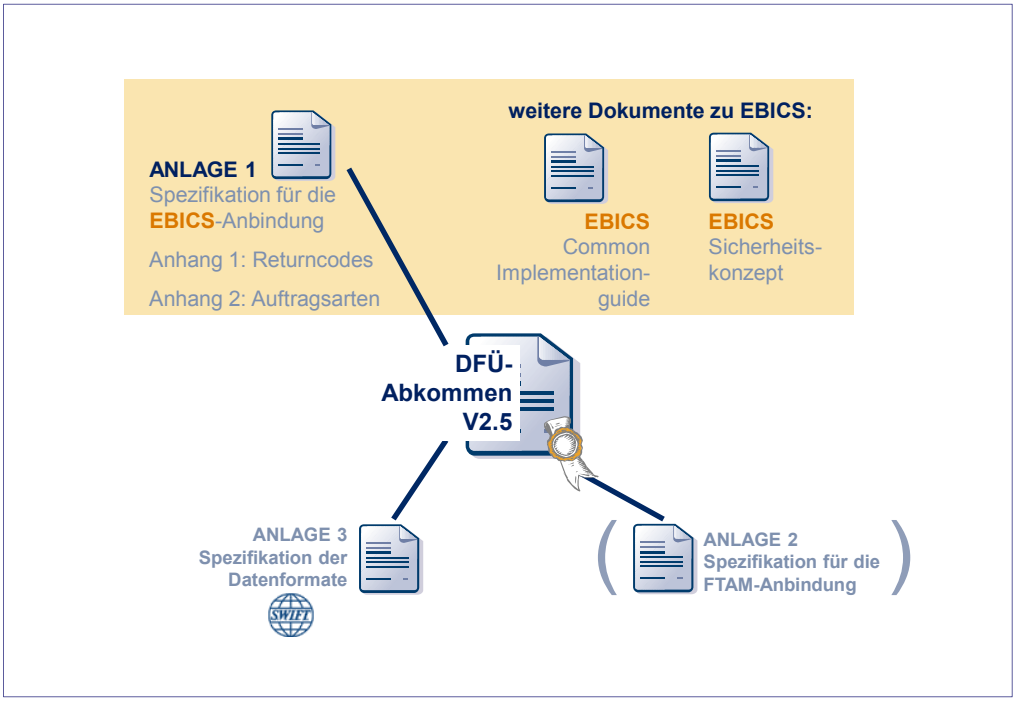

Abbildung 1: Aufbau der EBICS-Spezifikation und Einbettung in das deutsche DFÜ-Abkommen

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 selbst im englischen Originaltext bearbeitet und es finden nur Rückübersetzungen nach deutsch und französisch statt. Diese Dokumente befinden sich unter ebics.de bzw. cfonb.fr.

Zusätzlich zur Spezifikation in Anlage 1 ist zu EBICS noch ein Implementation Guide und in Deutschland – auf Anfrage bei der DK – auch ein Sicherheitskonzept erhältlich. Der Implementation Guide wurde mit der Version 2.5 aus den deutschen und französischen Fassungen zu einem gemeinsamen Dokument zusammengeführt. Damit wird den Forderungen nach leichter Implementierung/Migration und sicherem Betrieb Genüge getan.

Die Anlage 3 des DFÜ-Abkommens zur Spezifikation der Datenformate wie SWIFT oder SEPA bleibt eine deutsche Standardisierung und ohne Belang für die internationalen EBICS-Aktivitäten. Die derzeitige Bezeichnung V2.5 für die Anlage 3 korrespondiert nur zufällig mit der aktuellen EBICS-Version.

Die Anlage 2 zur Spezifikation des FTAM-Verfahrens ist inzwischen obsolet und nur noch der Vollständigkeit halber aufgeführt.

2 Gesamtszenario EBICS

In diesem Kapitel 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. Zum Zeitpunkt der Herausgabe dieses Kompendiums ist in Deutschland die Migration von FTAM auf EBICS bereits vollzogen. Trotzdem kann dieses Beispiel immer noch eindrucksvoll zeigen, wie von einem nationalen Standard auf EBICS migriert werden kann.

2.1 Zusammenspiel der Verfahren

Um von Altverfahren auf den EBICS-Standard zu migrieren, muss es grundsätzlich möglich sein, zumindest Altstandard (z. B. BCS-FTAM) und EBICS institutsseitig noch über einen längeren Zeitraum parallel zu betreiben. Eine mögliche Konfiguration zeigt die folgende Abbildung:

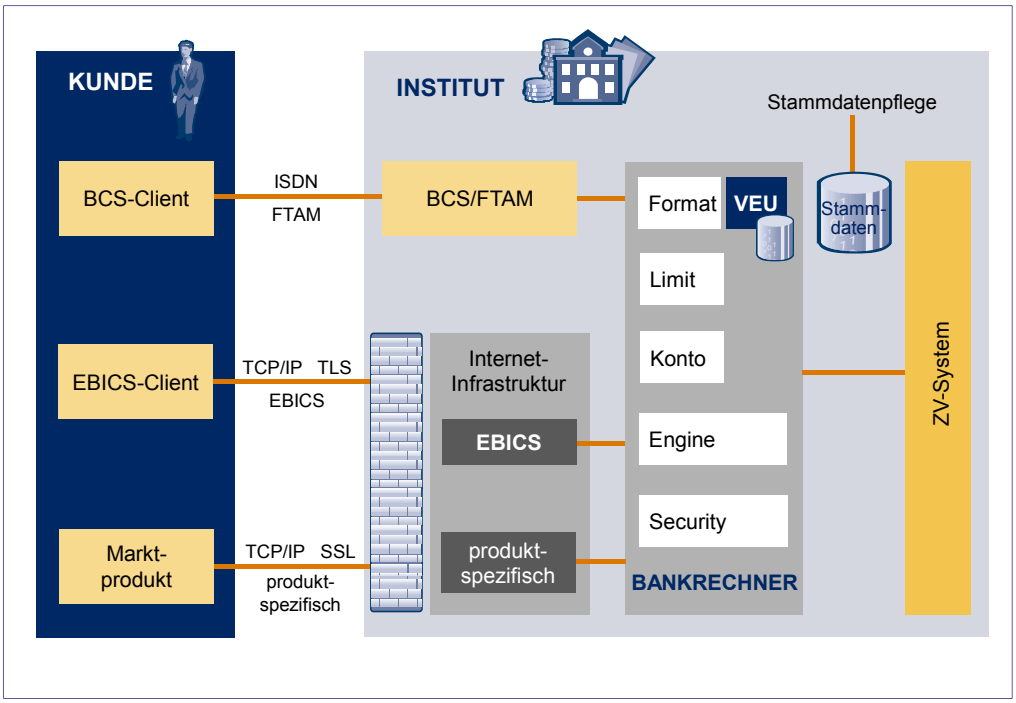

Abbildung 2: BCS/EBICS Gesamtszenario als Beispiel der Migration von einem nationalen Standard auf EBICS

In der gezeigten Konfiguration wird erkennbar, dass außer den Zugangskomponenten viele Bestandteile gemeinsam genutzt werden können. Da durch das identische A004-Sicherheitsverfahren und die gleichen Formate keine

Trennung der Systeme nötig ist, kann ein solches Gesamtszenario über einen längeren Zeitraum betrieben werden, wenn man von den erhöhten Betriebskosten bei den doppelten Komponenten absieht. Doch durch die im deutschen DFÜ-Abkommen festgelegte Roadmap wurde dieser Gesamtzeitraum ohnehin auf Ende 2010 begrenzt.

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. Für die Integration rechtlich unabhängiger Dritter sind jedoch auch unter EBICS noch einige Probleme zu lösen, da eine eigene Rolle für einen Portalbetreiber momentan nicht vorgesehen ist.

2.4 Migration

In diesem Abschnitt werden die Aufgaben einer typischen BCS nach EBICS Migration auf Kundenseite näher beleuchtet. Die Institutsseite kann an dieser Stelle vernachlässigt werden, da zumindest für Deutschland bereits seit dem 1. Januar 2008 eine Verpflichtung zur Unterstützung von EBICS durch die Banken besteht.

Hinweis:

Bei den folgenden Migrationsüberlegungen wird davon ausgegangen, dass das verwendete BCS-Kundenprodukt sich auf dem aktuellen Release-Stand befindet.

So sollte die aktuelle Infrastruktur z. B. Signaturen nach A004 unterstützen, damit nicht zusätzlich zur Erneuerung/Ergänzung der Kommunikationsinfrastruktur noch ein neues Sicherheitsverfahren eingeführt werden muss. Somit wird auch davon ausgegangen, dass der Umstieg auf die neuen Sicherheitsverfahren A005 oder A006 gem. EBICS-Version 2.5 getrennt von der Migration erfolgt.

Weiterhin wird noch vorausgesetzt, dass bereits eine funktionierende Internet-Infrastruktur vorhanden ist, wie sie für andere Internet-Anwendungen obligatorisch ist.

Im Idealfall sollte sich die Migration auf Kundenseite auf ein Update des aktuellen Kundenprodukts beschränken, wenn die administrativen Voraussetzungen geschaffen sind. Obwohl die generellen Stammdaten wie Kunde oder Teilnehmer (vgl. Abschnitt über das Datenmodell) erhalten bleiben, ändern sich zumindest die Kommunikationsdaten. Die benötigten Parameter für die Anwahl sind in den BPD (Bankparameterdaten) zusammengefasst und werden vom Institut zur Verfügung gestellt.

Nach der Installation eines entsprechenden Updates und nachdem alle nötigen Einstellungen vorgenommen sind, sollte es nun möglich sein, Verbindung mit dem Institut über eine Internet-Verbindung aufzunehmen.

Nicht zu unterschätzen ist hierbei das Verständnis einiger neuer Prozesse wie z. B. der Vorabprüfung, soweit sich diese in den Einstellungen und Abläufen des Kundenproduktes niederschlägt. Auch die Verwendung durch EBICS neuer Funktionen wie der Verteilten Elektronischen Unterschrift erfordert ein tiefer gehendes Verständnis der Zusammenhänge. Die entsprechenden Kapitel dieses Kompendiums können hier sicherlich eine erste Hilfestellung geben.

Ein Problem, das es noch zu lösen gilt, ist die EBICS-Initialisierung eines bestehenden Teilnehmers, der zuvor bereits über FTAM initialisiert wurde. Dieser besitzt natürlich bereits einen privaten Schlüssel für die Unterzeichnung von Aufträgen, jedoch keine Schlüsselpaare für die Authentifikation und die Verschlüsselung. In EBICS existiert für diesen Fall die Auftragsart HSA, mit deren Hilfe ein Teilnehmer mit dem Status `Neu_FTAM` seine neuen – EBICS-spezifischen Schlüssel – unterschrieben mit seiner für FTAM freigeschalteten EU einreichen kann. Über dieses optionale Verfahren können Teilnehmer ohne eine Neu-Initialisierung mittels INI-Brief elegant in EBICS übernommen werden.

2.4.1 Migrationsstatus in Frankreich

In Frankreich steht die Abschaltung des X.25-Netzwerks kurz bevor. Damit kann der weit verbreitete ETEBAC 3 Standard nicht mehr eingesetzt werden und eine Migration auf EBICS muss bis dahin erfolgt sein.

Obwohl theoretisch auch ein Zwischenschritt über das TCP/IP basierte ETEBAC 5 möglich wäre, stellt dies für die EBICS-Einführung kein Problem dar. Der zertifikatsbasierte ETEBAC-5- Standard ist mit wenigen Tausend registrierten Kunden weitaus geringer verbreitet.

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 der heutigen Lösung besitzen. Beim alten BCS-Standard wurde z. B. ISDN als Übertragungsmedium benutzt, was aus heutiger Sicht beinahe undenkbar ist, wenn man an die Übertragung großer Zahlungsverkehrsdateien denkt.

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) aufsetzen, unerlässlich. Dies wird durch die Nutzung gemeinsamer Plattformen stark vereinfacht.

Letztlich führt die Verwendung dieser weit verbreiteten Technologie dazu, dass Komponenten und auch Produkte in breiterem Umfang zur Verfügung stehen, als das bei den Ursprungsstandards BCS oder ETEBAC jemals der Fall war.

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 besser bekannte SSL (Secure Socket Layer) ergänzt und mittelfristig ablöst.

TLS sorgt für eine sichere Übertragung zwischen dem Kundensystem und dem ersten HTTP- oder besser Webserver im Institut. 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 Kapitel besser verstehen zu können, wird an dieser Stelle der XML-Standard erläutert. Während die notwendigen Protokollaufgaben bei BCS 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 der definierten Auftragsarten und einem XML-Umschlag. Es handelt sich also um eine Art Hybridsystem, bei dem das Kernstück die bankfachlichen DTA-, 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 http://www.ebics.de abgelegt.

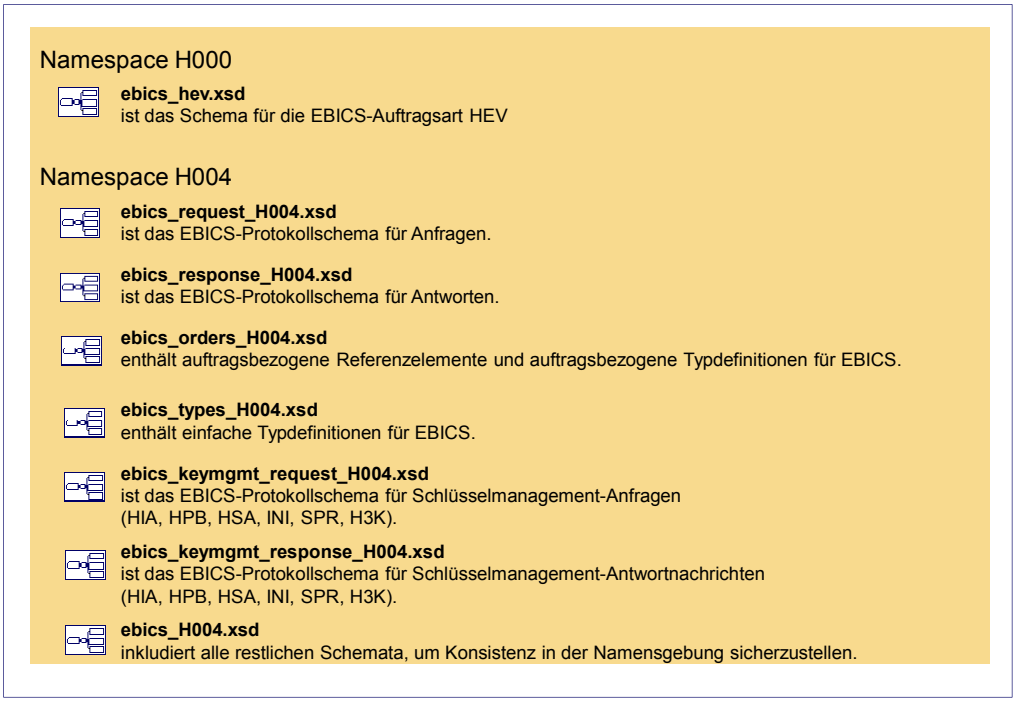

Abbildung 3: EBICS-XML-Schemata

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 Internet 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

Dieses Kapitel geht speziell auf das bei EBICS verwendete Datenmodell ein. Dieses findet sich in den Stammdatenverwaltungen der einzelnen Produkte wieder und ist, wie bereits bei den Migrationsaspekten erwähnt, bei beiden Standards nahezu identisch.

Grob gesehen existieren im Datenmodell die folgenden Entitäten:

- Kunde
- Konto
- Teilnehmer
- Auftragsart

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, alleine 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 mindestens eine Unterschrift der Klasse B benötigt.
Unterschriftsklasse B	Zweitunterschrift Der Auftrag muss bereits über eine Unterschrift der Klasse A verfügen.
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:

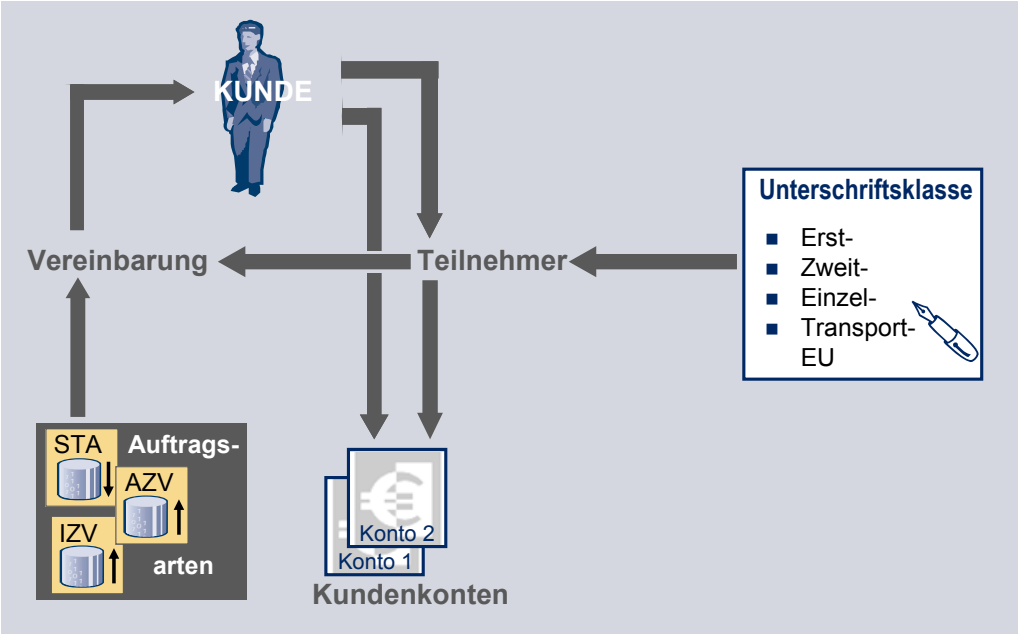

Abbildung 4: Datenmodell

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.

5 Sicherheit

Mit der EBICS Vorgängerversion V2.4, wurden neue Sicherheitsverfahren A005 und A006 bzw. X002 und E002 eingeführt. 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 mit Hilfe folgender Klassifizierung übermitteln, welche Art von Sicherheitsmedium der Kunde verwendet hat:

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

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 X001 bzw. X002.

Auch bei der Verschlüsselung macht EBICS keine halben Sachen: Außer der zwingenden Verschlüsselung mit TLS auf Transportebene ist auch das EBICS-eigene Verschlüsselungsverfahren E001 bzw. 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, das 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 Kapitel *EBICS-Abläufe* auf Seite 31.

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:

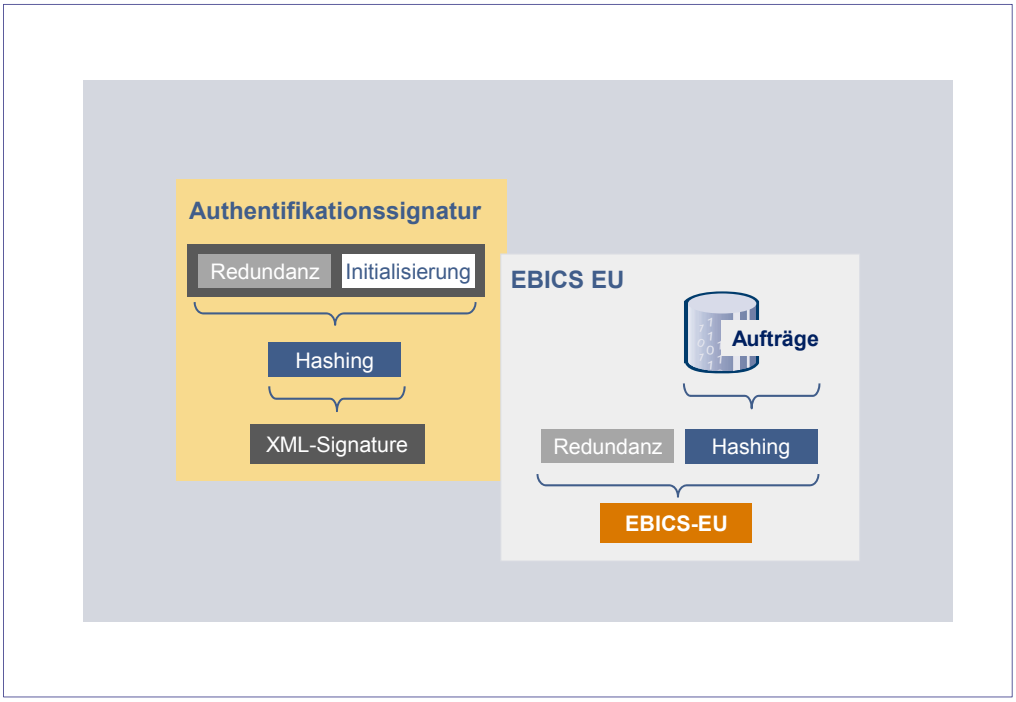

Abbildung 5: EBICS-Signaturverfahren

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 Kapitel *EBICS-Abläufe*, Seite 31).

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 Nutzda-

ten 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. Dessen wichtigste Eigenschaft 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 mit Hilfe eines Signaturschlüssels eine digitale Signatur gebildet. Um exakt zu sein, muss erwähnt werden, dass die Daten vor der Hashwert-Bildung 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 X001 bzw. 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 V2.4 durch die neuen Verfahren A005 und A006. Im Gegensatz zur Signaturbildung bei der Authentifikationssignatur sind hier die Schritte Redundanzbildung und Hashwert-Bildung vertauscht. Aufgrund der Verwendung des Datei-Hashwerts 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
- Hashwert-Verfahren RIPEMD160

Heute gängig und seit EBICS V2.4 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
Hashwert-Verfahren	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-Kryptokatalog und damit an der nationalen Ausprägung der EU-Signaturrichtlinie orientiert, ist eine Verwendung internationaler Standards gewährleistet.

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 V2.5 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 ist 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.

5.3.1.1 Das Einreicherprofil T auf Basis von Zertifikaten

Als Einstieg wird in Frankreich nur die Unterschriftsklasse T benötigt, d. h. der Auftrag wird über EBICS eingereicht und dann per Fax autorisiert. Dies entspricht dem Vorgehen beim älteren aber am meisten verbreiteten Standard ETEBAC 3.

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.

5.3.1.2 Autorisierungsprofil TS

Hierbei werden die Elektronischen Unterschriften für Transport und Signatur verwendet. Das Verfahren entspricht grob dem neueren 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.

5.3.1.3 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.

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 E001 bzw. E002 verwendet, um sowohl die Standardverschlüsselung in HTTPS als auch eine Ende-zu-Ende-Verschlüsselung zu erhalten. Bei E002 wird das vom BSI ab 2009 empfohlene AES-Verfahren eingesetzt.

5.4.1 TLS – Transport Layer Security

TLS löst als Standard das weit verbreitete SSL ab. 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. Cybersuites unterstützt. Im Standard sind vier Cybersuites benannt, die von jedem EBICS-Partner zu unterstützen sind.

5.4.2 Verschlüsselung E001 und E002

Bei E001 und 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 verwendet einen 1.024 Bit langen Verschlüsselungsschlüssel und den Padding-Algorithmus PKCS#1.

Mit EBICS V2.4 wurde E002 als Weiterentwicklung eingesetzt. Hier erfolgt der Übergang von Triple-DES auf AES (BSI-Empfehlung ab 2009).

6 Fachliche Funktionen von EBICS

Die Fachlichkeit von EBICS unterscheidet sich im Kern nicht von der des BCS-FTAM-Standards, d. h. die dort definierten Auftragsarten bleiben auch in EBICS erhalten, sofern sie sich nicht auf FTAM als Kommunikationsverfahren beziehen und damit obsolet sind.

Andererseits geht EBICS an vielen Stellen auch über BCS hinaus und öffnet neue Anwendungsfelder für den Kunden.

6.1 Auftragsarten

Im DFÜ-Abkommen werden folgende Anwendungsgebiete durch operative Auftragsarten unterstützt:

- Inlandszahlungsverkehr auf Basis verschiedener DTA-Formate
- SEPA-Zahlungsverkehr
- Deutscher Auslandszahlungsverkehr mit DTAZV
- Wertpapiergeschäft
- Akkreditivgeschäft
- Tageskontoauszugsinformationen mit MT940/MT942 für gebuchte Umsätze und Kontoumsatz-Avise

6.1.1 Inlands- und Auslandszahlungsverkehr / Tagesauszüge

Einige Beispiele in Deutschland genutzter Format gebundener standardisierter Auftragsarten zeigt die folgende Übersicht:

AZV	AZV-Auftrag im Diskettenformat senden
AZ2	AZV im Magnetbandformat senden (Satzlängenfeld 2 Byte)
AZ4	AZV im Magnetbandformat senden (Satzlängenfeld 4 Byte)
ESU	EU-Standardüberweisung senden (Zahlungsart 13)
DTE	Eilauftrag senden (IZV im DTAUS0-Format)
IZG	Inlandszahlungsverkehrsauftrag senden (nur Gutschriften)
IZL	Inlandszahlungsverkehrsauftrag senden (nur Lastschriften)
IZV	Inlandszahlungsverkehrsauftrag senden
MC2	IZV im Magnetbandformat senden (Satzlängenfeld 2 Byte)
MC4	IZV im Magnetbandformat senden (Satzlängenfeld 4 Byte)

STA	Abholen SWIFT-Tagesauszüge (SWIFT MT940)
VMK	Abholen kurzfristige Vormerkposten (SWIFT MT942)
VML	Abholen langfristige Vormerkposten (SWIFT MT942)

6.1.2 SEPA-Zahlungsverkehr

EBICS unterstützt Auftragsarten 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 aber noch folgende Besonderheit zu berücksichtigen ist.

Bei der Umsetzung der SEPA-Nachrichten für die deutsche Kreditwirtschaft wurde festgestellt, dass es sinnvoll ist, neben dem Standard-SEPA-Format noch 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	SEPA-Bezeichnung
SEPA-Daten-formate	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 zu Abwicklung des 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 942 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 Abhol-Auftragsarten 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.

6.1.3 Standard Auftragsarten für Upload und Download FUL und 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 V2.4 zur Verfügung. Die Auftragsart FUL (File Upload) wird für Einreichungen und die Auftragsart FDL (File Download) wird für Abholungen verwendet.

6.1.4 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. 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
- von EBICS nicht mehr unterstützte Auftragsarten

  z. B. PWA für Passwortänderung senden, da EBICS kein DFÜ-Passwort verwendet.

6.2 Verteilte Elektronische Unterschrift (VEU)

Die Verteilte Elektronische Unterschrift ist die wohl bedeutendste Anwendungsfunktion in EBICS. Getrieben von vorhandenen Marktprodukten fand diese Erweiterung Eingang in die DK-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 nun folgendermaßen ab:

1. Ein Teilnehmer reicht einen Auftrag, z. B. mit der Auftragsart IZV ein und fügt ggf. eine eigene bankfachliche EU mit der Unterschriftsklasse A hinzu.
2. Institutsseitig wird der Auftrag geprüft und festgestellt, ob noch weitere Signaturen erforderlich sind. In diesem Fall wird der Auftrag samt Hashwert im Institut zwischengespeichert.
3. 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.

4. Nach Analyse der vorliegenden Aufträge hat der Teilnehmer nun eine der folgenden Möglichkeiten
   - mit Auftragsart HVE zu signieren
   - mittels HVS zu stornieren

Die folgende Abbildung, die der Darstellung in der *Spezifikation für die EBICS-Anbindung* [1] auf Seite 142 nachempfunden ist, gibt einen verständlichen Überblick über die doch etwas komplexen Zusammenhänge:

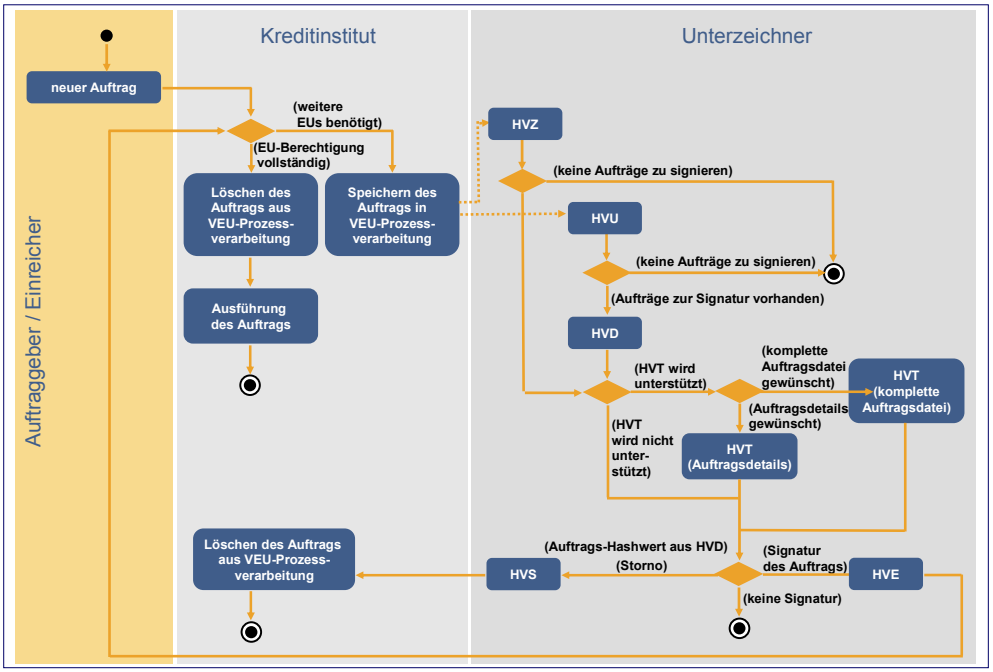

Abbildung 6: Abläufe beim VEU-Verfahren

Während die VEU in Deutschland gut verbreitet genutzt wird, ist sie in Frankreich bisher nicht üblich.

In Frankreich ist es üblich, die Signaturen mit dem Auftrag vervollständigt 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 eine der beiden Signaturen 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.

6.3 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.

6.4 Optionale Funktionen

Bereits in den vorangegangenen Kapiteln war öfter 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.

6.4.1 Vorabprüfung

Wie im Kapitel *EBICS-Abläufe* auf Seite 31 näher beschrieben, läuft eine EBICS-Transaktion in zwei Schritten ab. Im ersten Schritt wird mit Hilfe 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.

6.4.2 Teilnehmer-Daten

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.

6.5 EBICS im Interbank-Betrieb

Eine weitere Form des EBICS-Einsatzes ist die Verwendung im Interbank-Betrieb und STEP2.

In Deutschland werden im bilateralen Clearing die herstellerbasierten Lösungen (z. B. rvs und Connect:Direct) zunehmend durch EBICS als offenen Standard abgelöst.

Ein Szenario im Interbanken-Verkehr 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.

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

Für den direkten bilateralen Austausch zwischen Banken gibt es noch keine Vorgaben.

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:

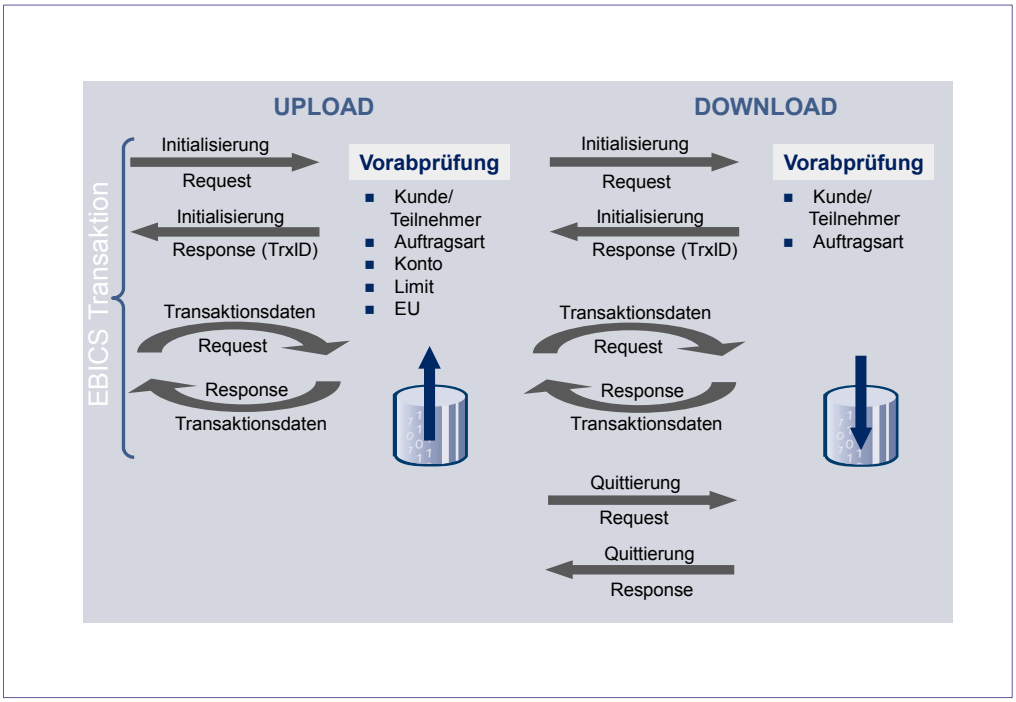

Abbildung 7: Ablauf einer EBICS-Transaktion

Nach dieser abschließenden und zugegebenermaßen etwas trockenen Materie der EBICS-Transaktionsabläufe widmet sich der nächste Abschnitt der Positionierung von EBICS im nationalen und internationalen Umfeld.

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 wie im internationalen Umfeld Standards, die ergänzend und überlappend mit EBICS zu sehen sind. Einige davon werden im Folgenden kurz dargestellt und zu EBICS in Bezug gesetzt.

Den Abschluss dieses Kapitels bildet ein Ausblick auf die zu erwartende Bedeutung und weitere Entwicklung des Standards.

8.1 FinTS

FinTS (Financial Transaction Services) ist ebenfalls ein DK-Standard, der jedoch seinen Schwerpunkt auf Online Banking mit Privat- und Gewerbekunden setzt. Die Wurzeln von FinTS reichen noch bis zum klassischen Bildschirmtextsystem zurück, wurden aber bereits mit HBCI (Homebanking Computer Interface) komplett von diesem Kommunikationsstandard entkoppelt. Daher bildet FinTS 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 4.0 setzt auch FinTS konsequent auf Internet-Standards wie HTTP oder XML. Auch die Kommunikationsverfahren wurden um dialogfreie, so genannte Datagramme und die Kommunikation Bank → Kunde 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 DTA, DTAZV, SEPA und SWIFT unterstützt – sie werden dort als Geschäftsvorfälle bezeichnet. 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 Ziel-

gruppe 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:

www.fints.org

8.2 SWIFT

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

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

Zu den klassischen FIN-Formaten, wie z. B. MT904, 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, welche 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.

Mit dieser internationalen Bedeutung ist SWIFT nun mit anderen internationalen Standards wie TWIST, IFX oder auch SEPA eng verknüpft und trägt auch Mitverantwortung für die Weiterentwicklung dieses so genannten Payment-Kernels als generalisiertes Zahlungsverkehrsmodell unter dem Dach der OAGi.

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 bleibt die These bestehen, dass es sich bei SWIFT und EBICS um ein harmonisches Nebeneinander handelt.

www.swift.com

8.3 ETEBAC

Der französische Standard ETEBAC (Echange Télématique Banque-Clients) kann als Komplementärstandard zu EBICS betrachtet werden. Auch hier ist das Durchführen von Massenzahlungen und das Abholen von Umsatzdaten möglich. Bei Firmenkunden, die in Frankreich angesiedelt sind, werden oft Produkte eingesetzt, die auch ein ETEBAC-Modul besitzen.

Frankreich hat sich in Hinblick auf die Abschaltung des X.25-Netzes Anfang 2012 entschieden, EBICS als Nachfolger des ETEBAC-Standards einzusetzen. Die meisten französischen Kreditinstitute sind mittlerweile auf EBICS umgeschwenkt. EBICS V2.5 enthält alle Erweiterungen, die für eine Migration von ETEBAC auf EBICS benötigt werden.

Es wird mit Spannung erwartet, wie sich andere EU-Länder nach diesem ersten Schritt in Richtung Internationalität in nächster Zeit zu EBICS positionieren werden.

www.etebac.org

8.4 Ausblick

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

Daraus wird erkennbar, dass EBICS auch in Zukunft der bestimmende Standard im Massenzahlungsverkehr sein wird.

Umso wichtiger ist daher die Tatsache, dass durch EBICS nun eine Standarderweiterung zur Verfügung steht, die alle Schwächen alter Kommunikationsstandards grundlegend beseitigt. Dies ist auch dadurch erkennbar, dass die

Einführung von EBICS sehr rasch und flächendeckend von statten ging, gerade auch weil ein weiches Migrationskonzept berücksichtigt ist.

Weitaus interessanter ist aber die Frage, wie sich der Standard nun auf weitere europäische Länder bzw. einzelne Banken innerhalb der Europäischen Union verbreiten wird. Einige Initiativen sind aktuell bekannt, jedoch lassen sich noch keine konkreten Informationen hierzu nennen.

Das abschließende Kapitel 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 Kapitel 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 Kernfunktionalitäten auf Institutsseite zur Abbildung von BCS-FTAM und EBICS bzw. auch EBICS Interbank.
TRAVIC-Link	stellt ein übergreifendes Filetransfer-Portfolio zur Verfügung, mit dem z. B. Aufträge über EBICS oder andere Filetransferverfahren, versehen mit bankfachlichen Elektronischen Unterschriften, an ein Institut weitergeleitet werden können.
EBICS-Mobile	gibt Benutzern die Möglichkeit, Auftragsdateien des nationalen und internationalen Zahlungsverkehrs, die im Kreditinstitut vorliegen, von unterwegs freizugeben – d. h. zu signieren.
TRAVIC-Services	API, welche alle EBICS-Funktionen auf Kundenseite – zur Unterstützung von Kundenprodukten beinhaltet.
TRAVIC-Web	bietet einen kompletten EBICS-Client auf Java-Basis im Zusammenspiel mit den TRAVIC-Corporate-Komponenten.
TRAVIC Port	Implementierung eines EBICS-Portals zur Abwicklung von Zahlungsverkehrsdienstleistungen über eine Portlet-Infrastruktur
TRAVIC-Retail	rundet den Baukasten ab und stellt alle Kernfunktionalitäten für ein institutsseitiges FinTS-System zur Verfügung.

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

9.1 TRAVIC-Corporate

Die Funktionalitäten von TRAVIC-Corporate decken sowohl BCS-FTAM als auch EBICS ab. Dabei wird soweit irgend möglich auf Wiederverwendbarkeit geachtet, sodass sowohl eine weiche Migration als auch eine gemeinsame Administration möglich ist, wie die folgende Abbildung zeigt:

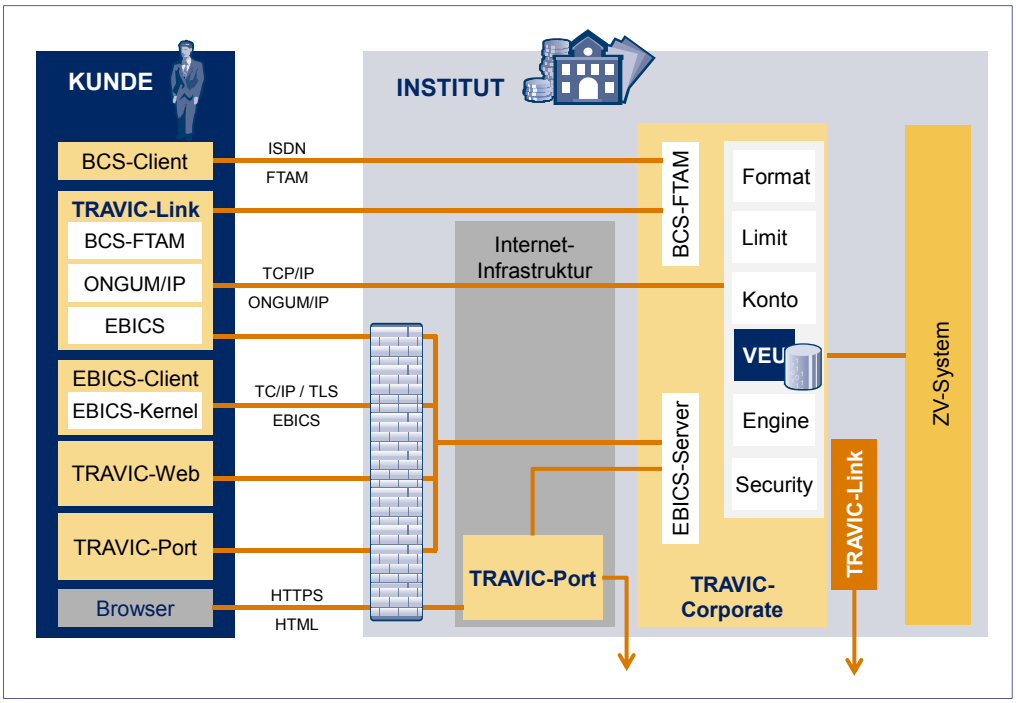

Abbildung 8: Komponenten der TRAVIC-Produktfamilie

TRAVIC-Corporate stellt alle in EBICS beschriebenen Funktionen zur Verfügung, also auch die optionalen Bestandteile wie z. B. die Schlüsselübernahme aus dem BCS-Umfeld. Zusätzlich erhältliche Tools ermöglichen auch die Übernahme von Stammdaten und kryptografischen Schlüsseln der BCS-Implementierungen anderer Hersteller im Rahmen einer Migration.

TRAVIC-Corporate steht auf mehreren UNIX-Plattformen und für IBM z/OS zur Verfügung, um für jeden Einsatzzweck die optimale Umgebung auswählen zu können.

9.2 TRAVIC-Link

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

Im Umfeld des elektronischen Zahlungsverkehrs für das Firmenkundengeschäft nimmt TRAVIC-Link die Rolle der so genannten Kundensysteme gemäß dem DFÜ-Abkommen mit Kunden ein. In diesen Szenarien unterstützt TRAVIC-Link die Standards BCS und EBICS. Hier ergänzt TRAVIC-Link Fi-

nanzbuchhaltungssysteme 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 Standard-Software. Hierzu bietet TRAVIC-Link entsprechende Schnittstellen an.

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

- Electronic Banking im Firmenkundenumfeld
  - EBICS
  - BCS-FTAM
  - SWIFT FileAct
  - SWIFT FIN
- integrierte Filetransfer-Verfahren
  - ONGUM-IP
  - Secure-FTP
  - FTPS
  - (Native) FTAM
- über Schnittstellen integrierbare Standard-Software
  - rvs (gedas Deutschland GmbH)
  - CONNECT:Direct (Sterling Commerce)
  - UDM (Stonebranch)
  - CFT (Axway)

9.3 EBICS-Mobile

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

Weiterhin können Kontoinformationen (Salden um 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.

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
- push-fähig durch Banken, die TRAVIC-Corporate betreiben

9.4 TRAVIC-Services-APIs für EBICS

Während die etablierten Hersteller von Bankrechner-Implementierungen 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 TRAVIC-Services-API für EBICS, die eine komplette und leicht verständliche EBICS-Suite für die Kundenseite zur Einbindung bereitstellt.

9.5 TRAVIC-Web

Für Kunden, die ein Kundenprodukt mit Cash-Management-Funktionen wünschen, steht mit TRAVIC-Web eine entsprechende Implementierung zur Verfügung. Die Java-Applikation dient zum Erfassen und Verwalten von Kunden, Teilnehmern, Instituten und Aufträgen, um diese dann per EBICS an das Institut zu senden. Dies beinhaltet auch den Support von Sicherheitsmedien wie Chipkarten oder Disketten.

9.6 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 EBICS-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. TRAVIC-Port verfügt auch über eine eigene portletbasierte Benutzeroberfläche.

Mit diesen Mitteln ist es mit wenig Implementierungsaufwand möglich, den transaktionsabhängigen Teil eines Firmenkundenportals aufzubauen und durch weitere fachliche Funktionen anzureichern. Die Verwendung der Portlet-Technologie sorgt zudem für eine attraktive und flexible Darstellung für den Kunden.

Literaturverzeichnis

[1] DFÜ-Abkommen
Anlage 1: Spezifikation für die EBICS-Anbindung
Version 2.5 vom 16. Mai 2011
Zentraler Kreditausschuss

[2] DFÜ-Abkommen
Anlage 2: Spezifikation für die FTAM-Anbindung
Version 2.0 vom 3. November 2005 (obsolet seit 1. Januar 2011)
Zentraler Kreditausschuss

[3] DFÜ-Abkommen
Anlage 3: Spezifikation der Datenformate
Version 2.7 vom 25. März 2013
Zentraler Kreditausschuss

[4] EBICS-Implementationguide
basierend auf EBICS-Version 2.5 vom 16. Mai 2011
Zentraler Kreditausschuss

[5] EBICS-Sicherheitskonzept
Version 1.4
Zentraler Kreditausschuss

[6] FinTS V4.0
Version 4.0 vom 22.06.2004
Zentraler Kreditausschuss

Abkürzungsverzeichnis

BCS	Banking Communication Standard
BPD	Bankparameterdaten
CFONB	Comité Français d'Organisation et de Normalisation Bancaire
DFÜ	Datenfernübertragung
DK	Die Deutsche Kreditwirtschaft (vormals ZKA)
DTA	Datenträgeraustausch
EBICS	Electronic Banking Internet Communication Standard
ETEBAC	Echange TElematique BAnque-Clients
EU	Elektronische Unterschrift
FIX	Financial Information Exchange
FTP	Filetransfer Protocol
HTTP	Hypertext Transport Protocol
FinTS	Financial Transaction Services
FTAM	Filetransfer Access and Management
HBCI	HomeBanking Computer Interface
IFX	Interactive Financial Exchange
IT	Informationstechnologie
ISO	International Standards Organisation
OAGi	Open Application Group
OFX	Open Financial Exchange
OSI	Open Systems Interconnect
SEPA	Single European Payment Area
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
W3C	WWW-Konsortium, Internet Standardisierungsgremium
XML	Extensible Markup Language
ZKA	Zentraler Kreditausschuss (heute DK)

Abbildungsverzeichnis

Abbildung 1: Aufbau der EBICS-Spezifikation und Einbettung in das deutsche DFÜ-Abkommen 6
Abbildung 2: BCS/EBICS Gesamtszenario als Beispiel der Migration von einem nationalen Standard auf EBICS 8
Abbildung 3: EBICS-XML-Schemata 12
Abbildung 4: Datenmodell 15
Abbildung 5: EBICS-Signaturverfahren 17
Abbildung 6: Abläufe beim VEU-Verfahren 28
Abbildung 7: Ablauf einer EBICS-Transaktion 32
Abbildung 8: Komponenten der TRAVIC-Produktfamilie 38

PPI AG

Moorfuhrtweg 13
22301 Hamburg
Tel.: +49 40 227433-0
Fax: +49 40 227433-333

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

Dokumentversion 4.2.3 vom 01.11.2013

Copyright

Dieses Dokument wurde von der PPI AG Informationstechnologie erstellt und ist gegenüber Dritten urheberrechtlich geschützt. Alle Rechte, auch die der Übersetzung, des Nachdrucks oder der Vervielfältigung des gesamten Dokumentes oder Teilen daraus, bedürfen der Zustimmung der PPI AG Informationstechnologie.

Die in diesem Dokument erwähnten Software- und Hardware-Bezeichnungen sind in den meisten Fällen auch eingetragene Warenzeichen und unterliegen als solche den gesetzlichen Bestimmungen.