

EBICS-Kompendium

Electronic Banking Internet Communication Standard



Dokumentversion: 3

Datum: 17.06.2009

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

Vorwort

Pünktlich zur CeBIT 2006 ging der Zentrale Kreditausschuss (ZKA) mit einer Erweiterung des DFÜ-Abkommens mit dem Namen EBICS (Electronic Banking Internet Communication Standard) an die breite Öffentlichkeit. Heute, gut zwei Jahre später, ist dieser Standard im Markt etabliert und hat in der aktuellen Version 2.4 gute Chancen, der europäische Zahlungsverkehrsstandard im Firmenkundengeschäft zu werden.

Bei EBICS handelt es sich im Kern um eine Ergänzung der „Internet Communication“ im weitesten Sinne. EBICS ist seit dem 1. Januar 2008 für die Banken verpflichtend und soll bis 2010 die jetzige FTAM-Variante komplett ablösen.

EBICS erfordert auf Kunden- und Institutsseite keinen hohen Migrationsaufwände und Prozessanpassungen – alle etablierten Objekte wie Stammdaten, Schlüssel oder Auftragsarten können erhalten bleiben. Voraussetzung ist nur, dass auch die jetzige FTAM-Umgebung bereits A004 als Signaturverfahren unterstützt. Ist dies der Fall, ist der Übergang auf EBICS nicht mehr als ein Programm-Update und von bestehenden DFÜ-Kunden ohne große Umstellungsaufwände zu bewerkstelligen.

Zusätzlich liefert EBICS auch neue Funktionen wie z. B. die verteilte Signatur oder die Authentifikationssignatur, wodurch bereits heute in Marktprodukten vorhandene Features nun multibankfähig eingesetzt werden können.

Das vorliegende Kompodium soll dem Leser einen Einblick in die neuen Funktionen von EBICS ermöglichen. Hierzu wird zunächst durch einen historischen Abriss das Umfeld des Zahlungsverkehrs für Firmenkunden nach dem DFÜ-Abkommen dargestellt und die Notwendigkeit für die vorliegende Erweiterung erläutert. Dem schließt sich eine strukturierte Beschreibung der neuen Funktionen von EBICS an. Eine Positionierung gegenüber anderen Standards wie FinTS oder SWIFT rundet die Betrachtung von EBICS ab. Den Abschluss bildet eine Darstellung der Umsetzung von EBICS am Beispiel der Produktfamilie TRAVIC.

Wenn Sie als Leser nach der Lektüre dieses Kompodiums 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, September 2008

Inhaltsverzeichnis

1	Einleitung	4
1.1	Historie.....	4
1.1.1	Die Evolution des Standards	6
1.1.2	Der Ruf nach EBICS	7
1.2	Anforderungen an EBICS als Erweiterung des BCS-Standards	7
1.3	Aufbau der Spezifikation	10
2	Gesamtszenario BCS/EBICS.....	11
2.1	Zusammenspiel der Verfahren.....	11
2.2	Berücksichtigung der Produkte.....	12
2.3	Portale.....	12
2.4	Migration.....	12
3	Kommunikation und Absicherung der Infrastruktur	14
3.1	FTAM	14
3.2	Internet.....	15
3.2.1	HTTPS und TLS – Transport Layer Security.....	15
3.2.2	XML – Extensible Markup Language.....	15
3.2.3	Optimierung der Kommunikation	17
4	Datenmodell	18
5	Sicherheit	20
5.1	Infrastruktursicherheit.....	20
5.2	Signaturverfahren	21
5.2.1	Authentifikationssignatur X001 bzw. X002	21
5.2.2	Auftragssignaturen (EU) nach A004 bzw. A005/A006.....	22
5.3	(Teilnehmer-)Initialisierung	23
5.4	Verschlüsselungsverfahren	23
5.4.1	TLS – Transport Layer Security	24
5.4.2	Verschlüsselung E001 und E002	24
6	Fachliche Funktionen von EBICS	25

6.1	Auftragsarten	25
6.1.1	Inlands- und Auslandszahlungsverkehr / Tagesauszüge	25
6.1.2	SEPA-Zahlungsverkehr.....	26
6.1.3	Weitere Auftragsarten	27
6.2	Verteilte Elektronische Unterschrift (VEU)	28
6.3	Portalsysteme	29
6.4	Optionale Funktionen	30
6.4.1	Vorabprüfung	30
6.4.2	User-Daten.....	30
7	EBICS-Abläufe	32
8	Positionierung im internationalen Umfeld	34
8.1	FinTS.....	34
8.2	SWIFT	35
8.3	ETEBAC	36
8.4	Ausblick	36
9	Umsetzung	38
9.1	TRAVIC-Corporate.....	39
9.2	TRAVIC-Link	39
9.3	TRAVIC-Services-APIs für EBICS	40
9.4	TRAVIC-Web	41
9.5	TRAVIC-Port	41
	Literaturverzeichnis	42
	Abkürzungsverzeichnis	43
	Abbildungsverzeichnis	45

1 Einleitung

Der BCS-Standard (Banking Communication Standard) hat sich als Vorläufer von EBICS in den letzten 10 bis 15 Jahren zu dem akzeptierten Zahlungsverkehrsstandard der deutschen Kreditwirtschaft im Firmenkundengeschäft entwickelt. Getragen durch das DFÜ-Abkommen des Zentralen Kreditausschusses (ZKA) bietet jedes Institut entsprechende Schnittstellen an, über die Kunde-Bank- oder Bank-Bank-Kommunikation stattfinden kann.

Mit EBICS (Electronic Banking Internet Communication Standard) wurde das DFÜ-Abkommen in dem Bereich erweitert, der sich zunehmend als Schwachstelle herauskristallisiert hat: der Kommunikation selbst. FTAM mit ISDN als Trägerprotokoll konnte den Anforderungen moderner IT nicht mehr gerecht werden und wurde bei EBICS durch zeitgemäße Internet-Standards ersetzt. Neben diesem Hauptaspekt für die Schaffung der Erweiterung des Standards erfüllt EBICS jedoch noch viele weitere Anforderungen aus dem Bereich Electronic Banking und Internet-Kommunikation, wie in den folgenden Abschnitten dargestellt wird. Die in der Beschreibung enthaltenen Versionsbezeichnungen wie z. B. A005 / A006 für die Unterschriften beziehen sich durchgängig auf die EBICS-Version 2.4, die zum 1. September 2009 verpflichtend wird.

1.1 Historie

Bevor der EBICS-Standard mit allen Funktionen beschrieben wird, werden noch mal ein paar Fakten zur Entwicklung des BCS-Standards genannt, der nach der Verpflichtung zur Unterstützung von EBICS als Protokollstandard seit Anfang dieses Jahres ab 2010 selbst nur noch Historie sein wird. Zu Beginn der 90er-Jahre wurde mehr und mehr der Ruf nach einer standardisierten Kommunikationsschnittstelle für Dateitransfer im Firmenkundengeschäft laut. Aufsetzend auf einem damals bereits verfügbaren Marktprodukt wurde im ZKA ein Standard definiert, der die Kommunikation, die Absicherung und die Inhalte des Datenaustauschs regelte. Entsprechend dieser Inhalte gliedert sich seit dieser ersten Version das dazu von den Verbänden geschlossene DFÜ-Abkommen:

- Anlage 1: Standards für die Kommunikation
- Anlage 2: Standards für die Sicherheit
- Anlage 3: Datenformate

Kommunikation

Als Kommunikationsverfahren wurde FTAM gewählt, das zu dieser Zeit als Filetransfer-Baustein des OSI-7-Schichtenmodells (OSI = Open Systems Interconnect) einen möglichst offenen und zukunftsweisenden Ansatz garantierte. Da die ersten drei Schichten dieses Stacks durch X.25 bzw. das deutsche Datex-P-Netz definiert wurden, kamen als Trägermedium hauptsächlich analoge Wählleitungen, teilweise auch festgeschaltete Verbindungen zum Einsatz.

Der Ruf nach mehr Datendurchsatz war Ende der 90er-Jahre die Geburtsstunde von ISDN als Übertragungsprotokoll. Meist erfüllte eine Vorschaltbox den Zweck, dieses schnellere und wirtschaftlichere Protokoll in die FTAM-Verarbeitung einzubinden.

Sicherheit

Der BCS-Standard bietet von jeher die Möglichkeit der Elektronischen Unterschrift (EU) von Dateien. Über ein RSA-Verfahren, das anfangs teilweise noch proprietär ausgeprägt war, konnten Unterschriftsdateien erzeugt werden, welche die Authentizität des Teilnehmers eines Kunden und die Integrität der Übermittlung sichern sowie die Aufträge gegenüber dem Institut für die Ausführung autorisieren.

Eine Signatur in Gegenrichtung ist im BCS-Standard nicht enthalten sondern erst jetzt im EBICS-Standard vorgesehen.

Aufgrund der relativ geringen Systemvoraussetzungen und bedingt dadurch, dass es keine unterschiedlichen Signaturverfahren gab, hatte sich die BCS-EU etabliert. Der überwiegende Teil der Kunden nutzte bis zum Übergang auf EBICS dieses Signaturverfahren. Daneben wurde noch der so genannte Datenträger-Begleitzettel angeboten, auf dem sich die Kerndaten eines Auftrags in gedruckter Form befanden und der – händisch unterschrieben – leicht z. B. per Fax an das entsprechende Institut übermittelt werden konnte. Die Freigabe eines Auftrags musste dann manuell durch einen Bankmitarbeiter erfolgen.

Erwähnt werden müssen im Sicherheitsbereich das so genannte DFÜ-Passwort, das als proprietäre Erweiterung im FTAM-Stack übermittelt wurde, sowie die Vorabprüfung des Kunden, des Teilnehmers und der Auftragsart gegen die Stammdaten des Instituts. Dadurch ließ sich ein potenzieller Angreifer bereits auf dem Kommunikationsstack ganz zu Beginn der Verarbeitung erkennen und abwehren.

Nachteil:

Die proprietäre FTAM-Erweiterung für die oben genannten Prüfungen verhinderte den Einsatz von Standardprodukten am Markt und limitierte diesen auf die Hersteller von Bankensoftware im engen Rahmen des BCS-Standards, was die Herstellerwahl stark einschränkte.

Eine Verschlüsselung der Übertragungsdaten war zu diesem frühen Zeitpunkt noch nicht vorgesehen, da von einem geschlossenen Netz, ja teilweise sogar von Festverbindungen ausgegangen werden konnte.

Dateninhalte

Bei den zu übertragenden Datenbeständen konzentrierte sich das DFÜ-Abkommen von Anfang an auf bestehende Standardformate wie z. B. DTA, DTAZV oder SWIFT. Diese wurden und werden durch so genannte Auftragsarten eindeutig referenziert. Einerseits existiert keine Nomenklatur zur Formulierung von Formaten für die Auftragsarten, wie dies bei anderen Standards

wie z. B. FinTS der Fall ist. Andererseits sah der BCS-Standard bewusst vor, dass ein Institut auf Basis von vorliegenden Formaten eigene Auftragsarten definieren und sie ihren Kunden anbieten konnte. Auf diese Tatsache ist wohl auch der hohe Grad an Multibankfähigkeit des Standards und die Akzeptanz – auch im internationalen Bereich – zurückzuführen.

Es gab ein paar Ausnahmen zu dieser Regel im administrativen Bereich. So existierten z. B. Auftragsarten zur Abholung eines Kundenprotokolls oder zum Austausch der kryptografischen Schlüssel im Rahmen der Teilnehmer-Initialisierung.

Ein wichtiger Aspekt war die Protokollfreiheit der Dateninhalte bei dieser Variante. Zu übertragen waren nur wenige Informationen wie z. B. die Auftragsart, Auftragsattribute und Auftragsparameter. Diese Informationen wurden bei BCS im Dateinamen kodiert. Dadurch erübrigte sich ein wie auch immer geariteter Protokollumschlag für derartige Steuerinformationen. Dieser Ansatz, der natürlich die Bewegungsfreiheit im Protokollbereich stark einschränkte, wird mit Internet-basierten weiteren Ausprägungen und natürlich auch mit EBICS über Bord geworfen – dort besteht die Möglichkeit, in größerem Umfang Protokollinformationen zwischen den Partnern auszutauschen, was aber auch den Overhead eines entsprechenden Protokollumschlags zur Folge hat.

1.1.1 Die Evolution des Standards

Aufbauend auf dieser Version 1.0 des DFÜ-Abkommens entstanden zahlreiche Ansätze für eine Weiterentwicklung des Standards. Einige wurden integraler Bestandteil, wie z. B. die Definition eines Verschlüsselungsverfahrens oder der Übergang auf internationale Standards im Signaturbereich, andere jedoch konnten keinen Konsens im ZKA finden.

Hierzu gehörte z. B. der Versuch, FTAM durch FTP abzulösen („BCS/FTP“), was wieder durch ein entstandenes Marktprodukt initiiert wurde. Doch schlechte Erfahrungen mit der proprietären Erweiterung des FTAM-Verfahrens durch die Vorabprüfungen auf der FTAM-Ebene, welches 1:1 Einzug in die FTP-Spezifikation finden sollte, verhinderte einen Durchbruch auf breiter Basis.

Das gleiche Schicksal war auch einigen anderen Versuchen beschieden, den Standard in Richtung aktueller Internet-Standards zu bewegen, was unweigerlich dazu führen musste, dass der Markt begann, in diesem attraktiven Bereich eigene Produktlösungen zur Verfügung zu stellen. Beispiele hierfür waren WOP (WEB ONGUM Portal) des SIZ, MultiWEB der Firma CoCoNet oder MultiCash der Firma Omikron.

Allen Produkten war gemeinsam, dass sie die inzwischen bestehende Internet-Technologie als Basis für ihre Weiterentwicklung verwendeten und damit auch Verschlüsselung über SSL oder Datenbeschreibung über XML als standardisiertes Fundament zur Verfügung hatten. Damit konnte auch jedes dieser Produkte sich selbstbewusst als „Standard“ positionieren, obwohl natürlich die Multibankfähigkeit dabei auf der Strecke zu bleiben drohte.

1.1.2 Der Ruf nach EBICS

Durch diese Entwicklung am Markt wurde im ZKA mehr und mehr der Ruf nach einer Vereinheitlichung laut. Über ein Grobkonzept definierten die Verbände in Zusammenarbeit mit IT-Dienstleistern der Banken die Rahmenbedingungen für diese Erweiterung des BCS-Standards.

Welche Anforderungen sich an diesen neuen Kommunikationsstandard ergaben, ist Inhalt des nächsten Abschnitts.

1.2 Anforderungen an EBICS als Erweiterung des BCS-Standards

Die grundsätzliche Zielsetzung bei der Schaffung des neuen 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. 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 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, die im Folgenden nun durchgängig als EBICS 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-Signature. Es sollten alle stabilen und geeigneten Internet-Standards verwendet werden.

Anforderung	Beschreibung
Sicherheit	Internet lässt sich heute nur noch in einem Atemzug mit dem Thema Sicherheit nennen. Wenn schon der sichere Hafen der quasi geschlossenen Datex-P-/ISDN-Netze, die für die FTAM-Kommunikation benutzt werden, 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.
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.

Anforderung	Beschreibung
Migration	Direkt aus der Zielsetzung ergab sich die Anforderung, zu keinem Zeitpunkt die Multibankfähigkeit bzw. die Marktakzeptanz aus dem Auge zu verlieren. EBICS sollte auf Kunden- und Institutsseite parallel zu der bestehenden Infrastruktur betrieben werden können und auch leicht aus dieser überführt werden können. Dazu sollte es z. B. vom Standard aus nicht notwendig sein, mit der EBICS-Migration einen Schlüsselwechsel durchführen zu müssen. Im Idealfall sollte der Kunde im Rahmen eines Produkt-Updates überhaupt nicht merken, dass er nun den EBICS-Standard verwendet.
Verbindlichkeit	Als eine Aufgabe der ZKA-Verbände bestand von Anfang an die Forderung, EBICS unter dem Dach des DFÜ-Abkommens zu entwickeln. Darauf aufbauend sollten aber auch konkrete Verpflichtungen eingegangen werden, ab wann EBICS flächendeckend eingesetzt werden muss, aber auch, wann die alte FTAM-Plattform abgeschaltet werden kann.

1.3 Aufbau der Spezifikation

Den Abschluss dieser Einleitung bildet eine Übersicht über den Aufbau der Spezifikation unter der Berücksichtigung von EBICS.

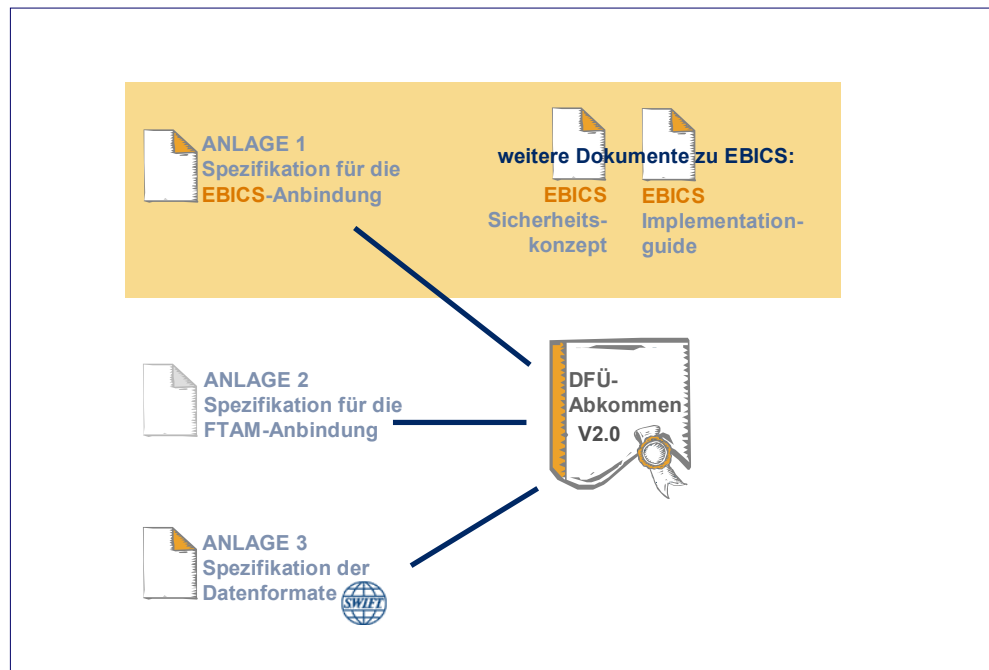


Abbildung 1: Aufbau der EBICS-Spezifikation

Auf dieser Übersicht ist sofort erkennbar, dass mit EBICS eine Verschiebung der generellen Struktur der im DFÜ-Abkommen referenzierten Dokumente stattgefunden hat. Die Spezifikation der Sicherheitsverfahren ist nämlich Bestandteil der Kommunikationsverfahren geworden und hat damit strukturell Platz geschaffen für ein zweites Kommunikationsverfahren „EBICS“ als Anlage 1. Damit bleibt die generelle Dokumentenstruktur im Abkommen (und das Abkommen selbst) weiterhin gültig.

Zusätzlich zur Spezifikation in Anlage 1 ist zu EBICS noch ein Implementation Guide und – auf Anfrage im ZKA – auch ein Sicherheitskonzept erhältlich. Damit wird den Forderungen nach leichter Implementierung/Migration und sicherem Betrieb Genüge getan.

Die drei EBICS-Dokumente sind auch in englischen Übersetzungen verfügbar, was die Marktdurchdringung – auch im europäischen Ausland – beschleunigen soll.

2 Gesamtszenario BCS/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 FTAM-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 Kompodiums ist der erste Schritt der verpflichtenden Einführung von EBICS auf Institutsseite bereits vollzogen, jedoch verwendet noch eine hohe Anzahl von Kunden ihr bestehendes FTAM-Kundenprodukt, da dieser Standard ja noch bis 30.10.2010 verpflichtend von den Banken unterstützt wird.

2.1 Zusammenspiel der Verfahren

Um ein solches Szenario aufzubauen, muss es grundsätzlich möglich sein, zumindest FTAM und EBICS institutsseitig noch über einen längeren Zeitraum, also mindestens bis 30.10.2010 parallel zu betreiben. Eine mögliche Konfiguration zeigt die folgende Abbildung:

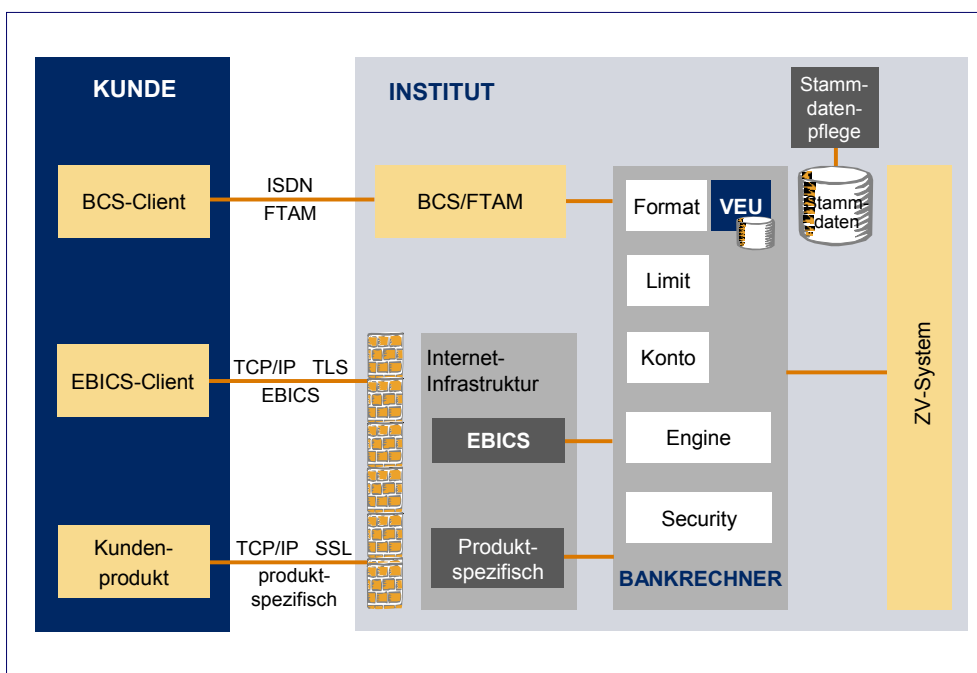


Abbildung 2: BCS/EBICS Gesamtszenario

In der gezeigten Konfiguration wird erkennbar, dass außer den Zugangskomponenten viele Bestandteile gemeinsam genutzt werden können, solange man vom jetzigen Funktionsumfang des BCS-Standards ausgeht. Da durch das identische A004-Sicherheitsverfahren und die gleichen Formate keine Trennung der Systeme nötig ist, kann ein solches Gesamtszenario über einen län-

geren Zeitraum betrieben werden, wenn man von den erhöhten Betriebskosten bei den doppelten Komponenten absieht. Doch durch die im DFÜ-Abkommen festgelegte Roadmap wird dieser Gesamtzeitraum ohnehin auf ein zumutbares Maß 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 im Gegensatz zu BCS auf Internet-Technologien aufsetzt, liegt der Schluss nahe, dass nun eine bessere Integration als bisher möglich sein sollte. 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 EBICS-Migration auf Kundenseite näher beleuchtet. Die Institutsseite kann an dieser Stelle vernachlässigt werden, da bereits seit 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 aus der EBICS-Version 2.4 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 neuer Funktionen wie der Verteilten Elektronischen Unterschrift erfordert ein tiefer gehendes Verständnis der Zusammenhänge. Die entsprechenden Kapitel dieses Kompodiums 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.

3 Kommunikation und Absicherung der Infrastruktur

Dieser Abschnitt befasst sich mit dem Herzstück des EBICS-Standards, der Kommunikation über das Internet. Aus Gründen der Vergleichbarkeit und Vollständigkeit wurde jedoch das FTAM-Verfahren in die Darstellung mit aufgenommen.

3.1 FTAM

FTAM (File Transfer Access and Management) ist der Anwendungsstack für Dateiübertragung nach dem OSI-Schichtenmodell der ISO. Dieses in den 80er-Jahren entwickelte Architekturmodell gliedert die Vorgänge einer Kommunikation zwischen zwei Partnern in sieben Schichten mit unterschiedlichen Aufgaben. Die unteren drei Schichten des OSI-Modells werden durch die physischen Netzwerkverbindungen, einem Leitungsprotokoll sowie durch das X.25-Protokoll repräsentiert. Der Paketvermittlungsdienst X.25 wird in Deutschland z. B. unter dem Produktnamen Datex-P angeboten. Die darüber liegenden Schichten wickeln das eigentliche Anwendungsprotokoll für die Dateiübertragung ab.

Da X.25-Netze ursprünglich nur Leitungsgeschwindigkeiten von 2.400 bit/s bis typischerweise 64 kbit/s unterstützten und X.25 aufgrund der paketweisen Übertragung generell wenig performant arbeitet, nahm ISDN ziemlich schnell diesen Platz ein und stellt heutzutage den Grenzwert von 128 kbit/s bei Bündelung zweier Kanäle zur Verfügung.

Dies ist in einer Welt von DSL und Satellitentechnik als Relikt aus der Vergangenheit anzusehen. Die Forderung höherer Geschwindigkeiten begründet aber nicht alleine die Notwendigkeit von schnelleren Durchlaufzeiten. In vielen Firmen wird diese teure ISDN-Infrastruktur nur noch exklusiv für BCS am Leben gehalten – alle anderen Datendienste bedienen sich schneller Glasfasertechnik. Zudem stellen ISDN-Anschlüsse an einem PC-Arbeitsplatz in einem Firmennetzwerk ein Sicherheitsrisiko dar, da hierüber an der firmenspezifischen Firewall vorbei ein Internet-Zugriff möglich ist. So liegt es auf der Hand, dass der Wunsch nach Abschaltung dieser in die Jahre gekommenen Technik besteht.

Andererseits stellt dieses etablierte Verfahren eine große Herausforderung an EBICS dar. Denn bei aller Beschränkung im Geschwindigkeitsbereich kann die FTAM-Infrastruktur doch als hinreichend sicher bezeichnet werden. Durch die proprietäre Erweiterung um die Vorabprüfungen auf der FTAM-Ebene besteht sogar die Möglichkeit, bereits im Transportprotokoll unberechtigte User abzuweisen, wenn auch aller Wahrscheinlichkeit mit teuren Mitteln realisiert.

Die folgenden Kapitel werden jedoch zeigen, dass die Vorteile der FTAM-Infrastruktur sehr wohl betrachtet wurden und EBICS diesen Herausforderungen durchaus gewachsen ist.

3.2 Internet

In der einführenden Literatur zum Internet als Kommunikationsverfahren wird immer versucht, das TCP/IP-Protokoll in den OSI-Stack zu zwingen, 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.

Dadurch werden – bildlich gesprochen – Schleusentore geöffnet, denn die Leistungsfähigkeit der Rechner, auf denen die fachliche Verarbeitung durchgeführt wird, wurde durch die bisherige ISDN-Leitungsgeschwindigkeit buchstäblich ausgebremst. Da es sich im Firmenkundengeschäft oft um große DTA-Dateien mit Tausenden von Einzelsätzen handelt, ist dieser Effekt höchst willkommen.

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 ZKA-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 BCS jemals der Fall war.

3.2.1 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-Standardisierung nicht ausreichend war, wie im übernächsten Abschnitt erläutert wird.

3.2.2 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.

Im Unterschied zu BCS besteht bei EBICS 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- 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 DTA-Datei also ein Vielfaches des XML-Umschlags darstellt. Eine Ausnahme bilden die Nachrichten, die im Rahmen der so genannten Initialisierung, der Verteilten Elektronischen Unterschrift und der Vorabprüfungen ausgetauscht werden. Da es sich hierbei um reine EBICS-Protokollstrukturen ohne Auftragsarten handelt, bestehen diese nur aus XML-Daten.

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/H003> und S001 abgelegt.

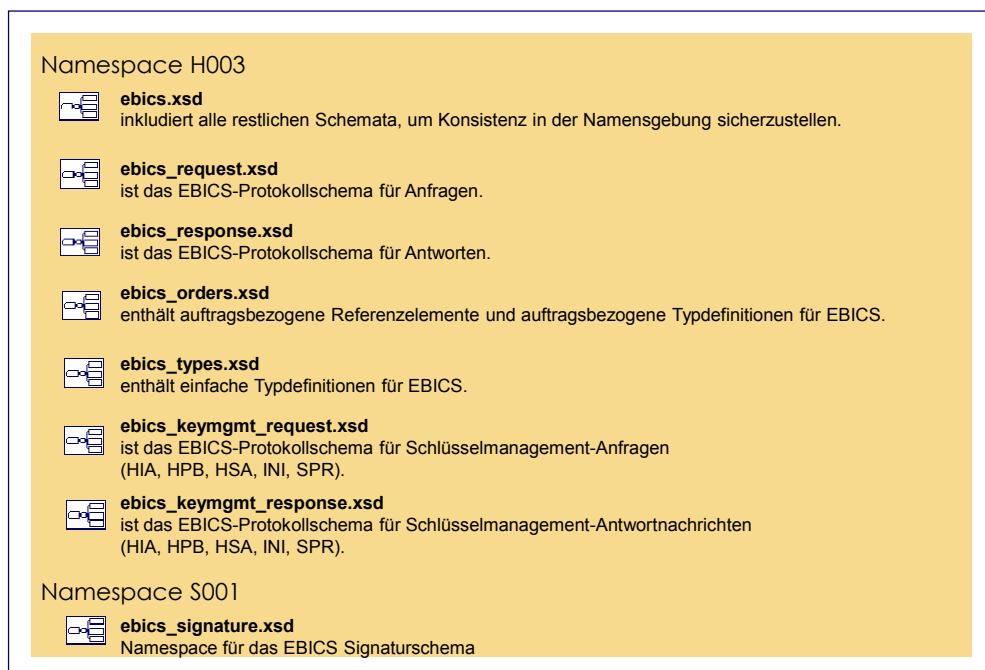


Abbildung 3: EBICS-XML-Schemata (Quelle: www.ebics.de)

Es wird erkennbar, dass die Schemata klar strukturiert sind und die Typ-Definitionen von den fachlichen Protokollschemas getrennt sind. Eine Besonderheit stellt das letzte Schema dar. Hierbei handelt es sich um das EBICS Signaturschema.

3.2.3 Optimierung der Kommunikation

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

Wie bereits bei BCS existiert auch bei EBICS die Möglichkeit, die Übertragungsdaten zu komprimieren. Entgegen der Lösung über FLAM bedient sich EBICS hingegen 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 BCS und 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 BCS-Datenmodell die folgenden Entitäten:

- Kunde
- Konto
- Teilnehmer
- Auftragsart

Den Einstieg bildet in der BCS-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 Authentifikations-signatur, 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 BCS-Datenmodells zeigt die folgende Abbildung:

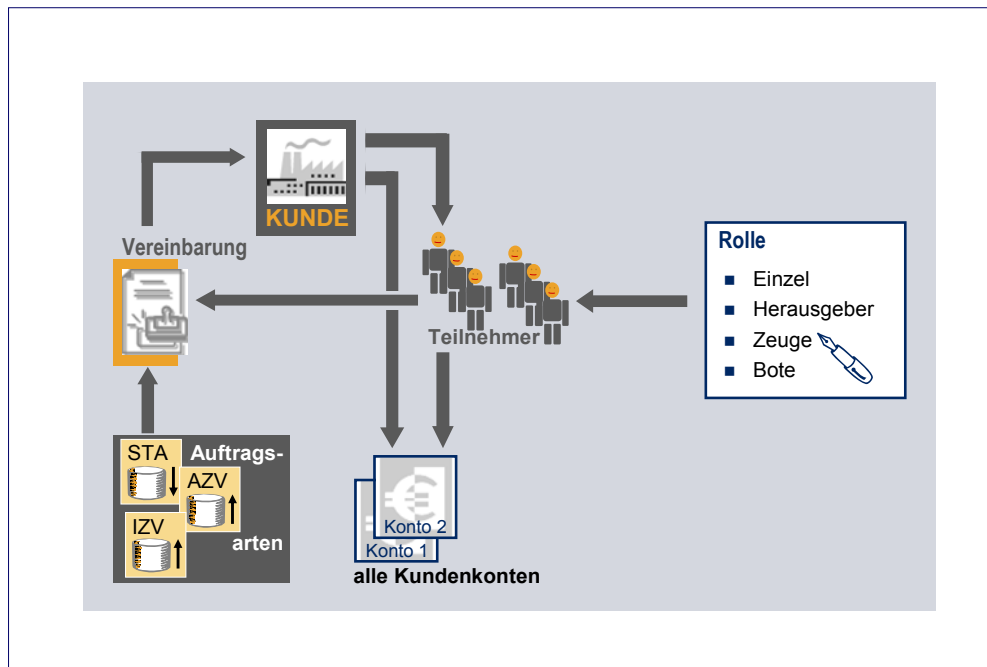


Abbildung 4: BCS-Datenmodell

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

5 Sicherheit

Es wurde bereits mehrfach erwähnt, dass EBICS einige Vorkehrungen zur Erhöhung der Sicherheit treffen musste, um dem offenen Charakter des Internets Rechnung zu tragen.

Dies betraf anfangs weniger die Sicherheitsverfahren direkt – diese waren aus Migrationsgründen identisch mit denen von BCS. Jetzt, mit der aktuellen Version 2.4, werden die neuen Sicherheitsverfahren A005 und A006 bzw. X002 und E002 eingeführt. Wichtiger sind jedoch die Festlegungen zur Verpflichtung, diese Verfahren auch einzusetzen, die EBICS von BCS abheben.

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. Im Gegensatz zu BCS, wo die Signatur nur auf Kundenseite unterstützt war, sind Kundensignaturen 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, die den eher schwachen Schutz durch das DFÜ-Passwort in FTAM mehr als ersetzt.

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 32.

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:

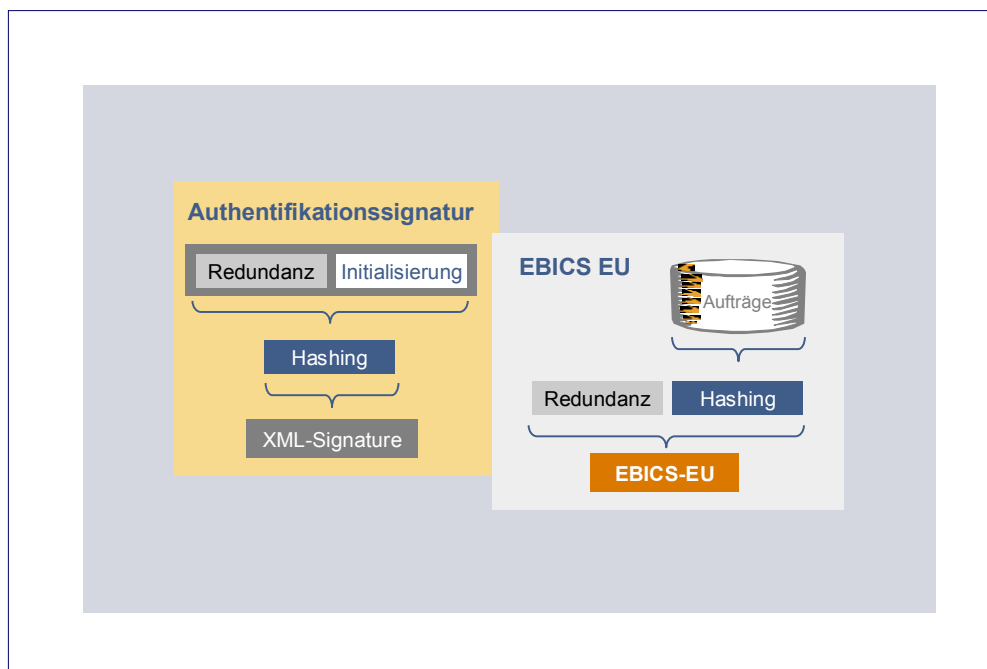


Abbildung 5: EBICS-Signaturverfahren

5.2.1 Authentifikationssignatur X001 bzw. X002

Die Authentifikationssignatur löst das schwache Authentifikationsverfahren über das DFÜ-Passwort in FTAM ab, jedoch mit dem gleichen Ziel, 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 32).

Teilnehmer, die ausschließlich Aufträge einreichen, können die Unterschrifts-klasse 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. 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) erfolgte anfangs wie auch in BCS mit dem Signaturverfahren A004. Mit EBICS V2.4 wurden die neuen Verfahren A005 und A006 spezifiziert. 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. Diese Vorgehensweise von BCS wurde in EBICS übernommen. Dabei wurde bewusst in Kauf genommen, dass diese Art der Signaturbildung über XML-Signatur schlecht abbildbar ist und daher die eigenen BCS-Regeln übernommen werden mussten.

EBICS fordert die RSA-Signatur nach A004 als Einstieg – ältere Signaturvarianten des DFÜ-Abkommens werden nicht unterstützt. A004 ist von den Verfahren her auf die aktuelle Signaturkarte der deutschen Kreditwirtschaft mit SECCOS als Betriebssystem zugeschnitten, unterstützt diese Verfahren aber wie gesagt auch über Disketten oder USB-Sticks.

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

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

Seit EBICS V2.4 werden mit den EU-Verfahren A005 und A006 folgende Attribute unterstützt:

	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.

5.3 (Teilnehmer-)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 jedoch das Verfahren mittels Initialisierungsbrief ähnlich dem in BCS verwendet.

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 Standardver-

schlüsselung 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

Bereits im BCS-Standard wurde ein Verschlüsselungsverfahren V001 eingeführt. Es handelt sich hierbei um ein so genanntes Hybridverfahren, d. h. aus asymmetrischen und symmetrischen Algorithmen bestehend. 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.

Auf dieser Basis setzt auch das mit EBICS eingeführte Verfahren E001 auf. Es unterscheidet sich zu V001 lediglich an einigen Stellen, wie z. B. der Länge des Verschlüsselungsschlüssels (768 Bit → 1.024 Bit) und dem Padding-Algorithmus (0-Padding → 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-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 Auftragsarten unterstützt:

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

6.1.1 Inlands- und Auslandszahlungsverkehr / Tagesauszüge

Einige Beispiele 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

Seit Version 2.3 unterstützt EBICS auch neue Auftragsarten für den SEPA-Zahlungsverkehr. 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

ZKA-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 die verwendeten SEPA-Auftragsarten nach den unterschiedlichen Ausprägungen aufgelistet:

Option	Auftragsart	SEPA-Bezeichnung
SEPA-Datenformate	CCM	Credit Transfer Initiation
	CRJ	Payment Status Report for Credit Transfer
	CDM	Direct Debit Initiation
	CDR	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

Der Vollständigkeit halber sei noch erwähnt, dass zur Übermittlung der SEPA-relevanten Daten im Rahmen der SWIFT-Tagesauszüge, die SWIFT-Formate MT940 und 942 angepasst wurden, diese aber unverändert über die Auftragsart STA abgewickelt werden.

6.1.3 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 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 neue Anwendungsfunktion in EBICS. Getrieben von vorhandenen Marktprodukten fand diese Erweiterung Eingang in die ZKA-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 getriggert durch Anfragen des Teilnehmers Informationen wie z. B. Einzeltransaktio-

nen 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:

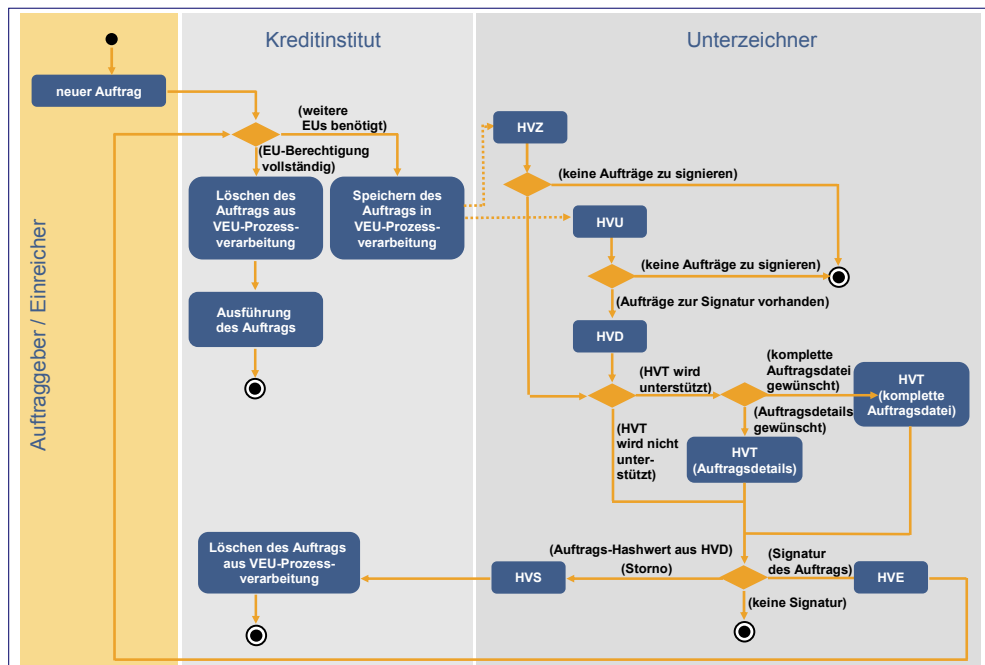


Abbildung 6: Abläufe beim VEU-Verfahren

6.3 Portalsysteme

Obwohl in der EBICS-Spezifikation nirgends der Begriff Portal explizit auftaucht, ergibt sich durch die Verwendung der Authentifikations-signatur 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 32 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 User-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.

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 initierend 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:

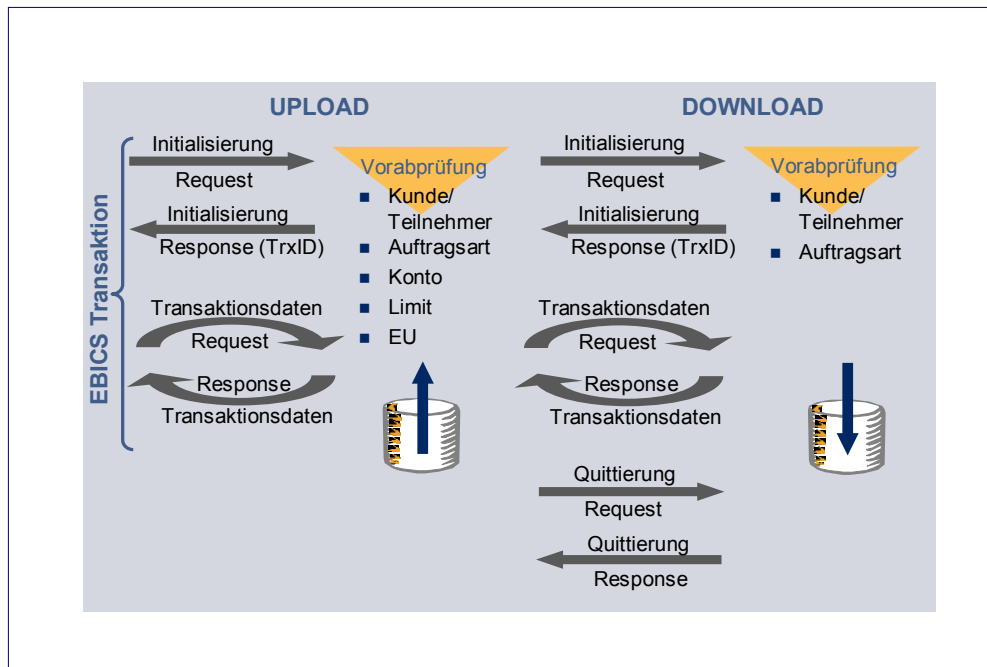


Abbildung 7: Ablauf einer EBICS-Transaktion

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 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 ZKA-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. Der ZKA 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 Finanzge-

schäfte 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 BCS-FTAM und FinTS zwei Kommunikationsverfahren an. Diese beiden Welten rücken mit der Einführung von EBICS auf Basis der gemeinsamen Internet-Technologien noch näher zusammen.

Zur tieferen Betrachtung von FinTS empfiehlt sich die Lektüre des FinTS-Kompodiums, 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

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.

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. Als Standards werden EDIFACT-Formate unterstützt. Bei Firmen, die auch in Frankreich angesiedelt sind, werden oft Produkte eingesetzt, die auch ein ETEBAC-Modul besitzen.

Bei Erscheinen dieses Kompodiums ist bereits absehbar, dass Frankreich in absehbarer Zeit ebenfalls EBICS als Nachfolger des ETEBAC-Standards einsetzen wird. Die fachliche Abstimmung ist bereits abgeschlossen und die organisatorischen Rahmenbedingungen befinden sich auf der Zielgeraden. EBICS V2.4 enthält bereits drei Erweiterungen, die als französische Anforderungen in den Standard eingeflossen sind.

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 im Umfeld des DFÜ-Abkommens lässt sich entnehmen, dass es – auch im internationalen Bereich – derzeit keine vergleichbaren Industriestandards gibt, wenn man von anderen nationalen Initiativen wie ETEBAC einmal absieht.

Daraus wird erkennbar, dass das DFÜ-Abkommen zumindest in Deutschland auch in Zukunft der bestimmende Standard im Massenzahlungsverkehr bleiben wird. Umso wichtiger ist daher die Tatsache, dass durch EBICS nun eine Standarderweiterung zur Verfügung steht, die alle Schwächen des bisherigen BCS-Standards grundlegend beseitigt. Daher ist zu erwarten, dass die Einführung von EBICS sehr rasch und flächendeckend von statten gehen dürfte, gerade auch weil ein weiches Migrationskonzept besteht.

In zukünftigen Versionen könnte es ggf. noch eine weitere Annäherung mit FinTS geben, wenn daraus Mehrwerte für beide Kundengruppen entstehen.

Weitaus interessanter ist aber die Frage, wie sich eine absehbare Übernahme des Standards durch Frankreich auf die weitere Verbreitung innerhalb der Europäischen Union auswirkt.

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
TRAVIC-Link	stellt ein übergreifendes Filetransfer-Portfolio zur Verfügung, mit dem z. B. Aufträge über BCS-FTAM oder EBICS, versehen mit bankfachlichen Elektronischen Unterschriften, an ein Institut weitergeleitet werden können
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:

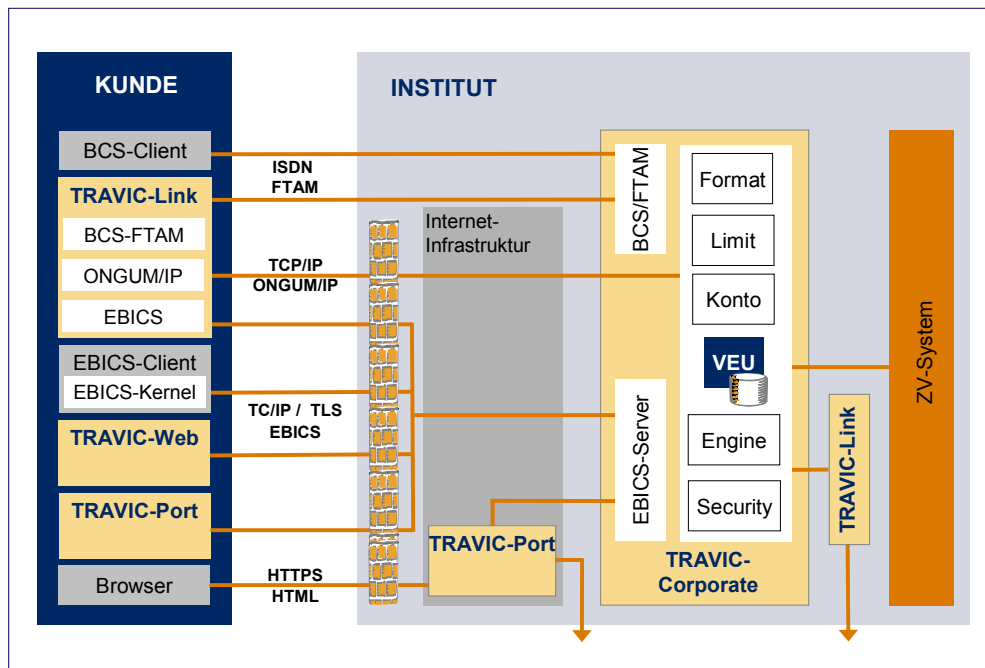


Abbildung 8: Komponenten der TRAVIC-Produktfamilie

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 ZKA-Abkommen für die DFÜ mit Kunden ein. In diesen Szenarien unterstützt TRAVIC-Link die Standards BCS und EBICS. Hier ergänzt TRA-

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

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

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

9.3 TRAVIC-Services-APIs für EBICS

Während die etablierten Hersteller von Bankrechner-Implementierungen ernstig 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.

9.4 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.

9.5 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 2.3 vom 4. Oktober 2007
Zentraler Kreditausschuss
- [2] DFÜ-Abkommen
Anlage 2: Spezifikation für die FTAM-Anbindung
Version 2.0 vom 3. November 2005
Zentraler Kreditausschuss
- [3] DFÜ-Abkommen
Anlage 3: Spezifikation der Datenformate
Version 2.2 vom 29. Oktober 2007
Zentraler Kreditausschuss
- [4] EBICS-Implementationsguide
Version 1.6 vom 4. Oktober 2007
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
DFÜ	Datenfernübertragung
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
FLAM	Frankenstein-Limes-Access-Method
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
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
WOP	WEB ONGUM Portal
XML	Extensible Markup Language
ZKA	Zentraler Kreditausschuss

Abbildungsverzeichnis

Abbildung 1:	Aufbau der EBICS-Spezifikation	10
Abbildung 2:	BCS/EBICS Gesamtszenario	11
Abbildung 3:	EBICS-XML-Schemata (Quelle: www.ebics.de).....	16
Abbildung 4:	BCS-Datenmodell.....	19
Abbildung 5:	EBICS-Signaturverfahren.....	21
Abbildung 6:	Abläufe beim VEU-Verfahren	29
Abbildung 7:	Ablauf einer EBICS-Transaktion	33
Abbildung 8:	Komponenten der TRAVIC-Produktfamilie.....	39



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

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

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.

