Hinweise zum Einsatz von Electronic-Banking-Systemen

Verfasser: Herbert **Gruschka**

Inhaltsübersicht Seite

1 Einführung

Bei unseren überörtlichen Kassen- und Rechnungsprüfungen stellen wir immer wieder fest, dass beim Einsatz von **Electronic-Banking-Systemen**[1] grundlegende haushaltsrechtliche Anforderungen oder Empfehlungen der Kreditwirtschaft und des Bundesamtes für Sicherheit in der Informationstechnik (BSI[2]), die der Sicherheit dieser Rechnersysteme dienen, nicht beachtet werden. Hierdurch wird die äußere und innere Kassensicherheit unnötig gefährdet, zumal die grundlegenden organisatorischen und technischen Schutzmaßnahmen meistens ohne größeren Aufwand realisierbar sind. Zum Teil entstehen die Risiken aber auch aus Unkenntnis der von der Kreditwirtschaft angebotenen Konfigurations- und Sicherungsmöglichkeiten und der Gefahrenpotenziale, die von immer raffinierteren und leistungsfähigeren Schadprogrammen ausgehen.

Wir wollen mit diesem Beitrag unsere bisherigen Erkenntnisse[3] auf diesem Gebiet zusammenfassen und Hinweise/Empfehlungen zum sicheren und effizienten Einsatz der Electronic-Banking-Systeme geben. Zugleich wollen wir die Vor- und Nachteile der Electronic-Banking-Varianten und der zur Verfügung stehenden Sicherungs- und Übertragungsverfahren darstellen. Aus aktuellem Anlass werden wir zum Schluss auf die Unterschiede zwischen den elektronischen Umsatz- bzw. Buchungsinformationen und dem als Nachweis für die ordnungsgemäße Buchführung dienenden Kontoauszug eingehen und hierbei insbesondere die vom Bayerischen Landesamt für Steuern nunmehr seit Mitte letzten Jahres vertretene Rechtsauffassung berücksichtigen.

Der Leitgedanke sollte also sein:

Electronic-Banking ja, aber sicher!

Darüber hinaus gehen uns vermehrt Fragen von Kommunen zu, welche Electronic-Banking-Angebote der Kreditwirtschaft sich für den Einsatz in Kommunalverwaltungen eignen und wie sich die angebotenen Lösungen effizient im Verwaltungsbetrieb einsetzen lassen. In diesem Zusammenhang tauchen immer wieder Fragen zur Nutzung der elektronischen Kontoauszüge und zu den haushaltsrechtlichen Nachweis- und Aufbewahrungspflichten auf.

2 Rechtsgrundlagen

2.1 Abkommen der Kreditwirtschaft

Grundlage für die Kontoführung auf elektronischem Wege war ursprünglich ein Staatsvertrag zwischen den Ländern vom 18.03.1983 über Bildschirmtext (GVBl S. 537), der am 01.09.1983 in den Ländern Bayern, Berlin, Hessen, Nordrhein-Westfalen und Schleswig-Holstein und am

---

1 Die „fett“ gekennzeichneten Begriffe werden in Abschnitt 7 erläutert.

2 Die über das Internet erreichbaren Quellen haben wir in Abschnitt 8.1 aufgeführt.

3 Wir haben uns bemüht, richtige und vollständige Informationen zur Verfügung zu stellen. Alle Angaben wurden nach bestem Wissen und mit größtmöglicher Sorgfalt recherchiert und soweit wie möglich überprüft. Da uns die einzelnen Systeme aber nicht zu „Labortests“ zur Verfügung standen, übernehmen wir keine Garantie oder Haftung für die Fehlerfreiheit, Aktualität, Richtigkeit und Vollständigkeit der bereitgestellten Informationen.

01.09.1984 in den anderen Ländern in Kraft trat. Auf dieser Rechtsgrundlage schlossen die Spitzenverbände der Kreditwirtschaft zusammen mit der Bundespost damals das „Abkommen über Bildschirmtext“, das um ein BTX-Sicherheitskonzept sowie spezielle Bedingungen über die Nutzung von Bildschirmtext ergänzt wurde.[4] Darauf aufbauend vereinbarten die Spitzenverbände der deutschen Kreditwirtschaft im Jahr 1995 ein Abkommen über die Datenfernübertragung (**DFÜ**), das den elektronischen Datenaustausch zwischen den Kunden und Kreditinstituten neu regelte. Technische Basis dieses Abkommens war der dateiorientierte **BCS/FTAM**-Datenverkehr zwischen den Kunden und den Kreditinstituten.

Mit dem Siegeszug des Internets standen der Kreditwirtschaft und ihren Kunden inzwischen neue Dienste auf der Grundlage internationaler Standards zur Verfügung, die neue Möglichkeiten für die elektronische Kommunikation boten, zugleich aber wegen der Offenheit und Struktur des Internets neue Risiken bargen. Für die Übertragung von beleglosen Bankaufträgen und Zahlungsverkehrsdaten über das Internet definierte und veröffentlichte der Zentrale Kreditausschuss (**ZKA**) mit dem Homebanking Computer Interface (**HBCI**) einen neuen, vom Online-Diensteanbieter unabhängigen Übertragungsstandard. Dieser sollte die dialogorientierte Abwicklung von Bankgeschäften auch mit mehreren Kreditinstituten (multibankfähig) über eine einheitliche und standardisierte Schnittstelle ermöglichen.

Der Einsatz von Internet-Banking-Systemen und Zahlungsverkehrsprogrammen sowie der Austausch von Datenträgern mit Zahlungsverkehrsdaten orientiert sich im Bereich der deutschen Kreditwirtschaft an folgenden Abkommen:

– Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten – DFÜ –

  Abkommen, in Kraft getreten am 15.03.1995 und Änderungsvereinbarung zum DFÜ-Abkommen, in Kraft getreten am 01.01.2006, mit folgenden Anlagen

  - Anlage 1: Spezifikation für die **EBICS**-Anbindung
  - Anlage 2: Spezifikation für die FTAM-Anbindung (ist am 31.12.2010 entfallen)
  - Anlage 3: Spezifikation der Datenformate

– Homebanking-Abkommen, in Kraft getreten am 01.10.1997 (Grundlage für HBCI bzw. **FinTS**)

Um das bei einem Kreditinstitut geführte Girokonto auf elektronischem Wege nutzen zu können, ist auf Grundlage des Vertrages über die Girokontenführung der Abschluss einer zusätzlichen Vereinbarung[5] über die elektronische Kontoführung notwendig, die Art und Weise der Nutzung und Datenübermittlung (Internet, DFÜ oder DTA), die Authentifizierungsmerkmale (Kennung, Passwort, Key) sowie die für die Autorisierung der Aufträge erforderlichen Legitimationsmedien und -verfahren (**PIN/TAN** oder elektronische Signaturen) festlegt und der die entsprechenden AGB der Kreditinstitute (sog. Online-Banking-Bedingungen) zu Grunde liegen. Ei-

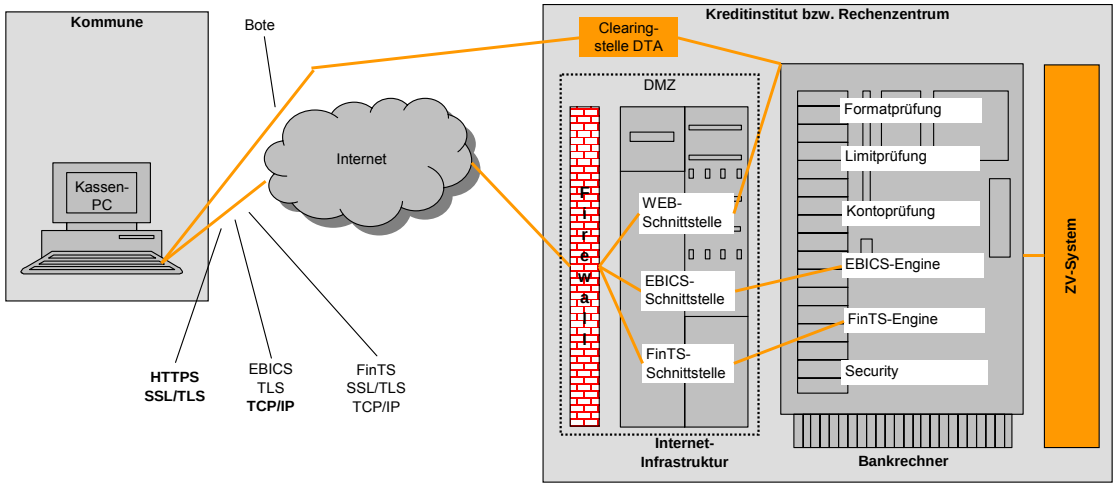
[4] vgl. CBL-Journal, Issue September 2002, Stefan Werner, „Rechtliche Aspekte von Zahlungssystemen im Internet”, CBL Web-Doc. 5/2002

[5] hierbei handelt es sich um eine in Ergänzung zum Girovertrag getroffene Nebenabrede, die den Kunden berechtigt, Erklärungen gegenüber dem Kreditinstitut online abzugeben – vgl. BGH, Urteil vom 12.12.2000, Az.: XI ZR 138/00

nen Überblick über die unterschiedlichen Nutzungsmöglichkeiten und Übertragungswege von elektronischen Zahlungsverkehrsdaten und Kontoinformationen soll die nachfolgende Abbildung veranschaulichen:

Übertragungswege von Zahlungsverkehrsdaten Abbildung 1

(in Anlehnung an EBICS Kompendium)



2.2 Gesetzliche Grundlagen

Mit Umsetzung der EG-Richtlinie für Zahlungsdienstleistungen (Richtlinie 2007/64/EG Payment Services Directive – EU-Zahlungsdiensterichtlinie) durch das „Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht“ (BGBl I 2009 S. 2355) veränderte sich mit Wirkung vom 31.10.2009 der Rechtsrahmen für den bargeldlosen Zahlungsverkehr erheblich. Die wesentlichen zivilrechtlichen Umsetzungsvorschriften (§§ 675 a bis 676 c BGB, Art. 248 EGBGB – vgl. BT-Drs.16/13669) brachten unter anderem folgende Änderungen, die auch den elektronischen Zahlungsverkehr über das **Online-Banking**, Homebanking oder den beleglosen Zahlungsverkehr durch Datenträgeraustausch betreffen:

– Neuregelung der Rechte und Pflichten von Zahlungsdienstleistern und Zahlungsdienstnutzern (z. B. entfallende Verpflichtung der Kreditinstitute zum Abgleich der Bankverbindungsdaten und Namen des Zahlungsempfängers bei allen Überweisungsaufträgen)

– einheitliche Regelungen für inländische und grenzüberschreitende Zahlungsinstrumente innerhalb der EU bzw. des EWR (z. B. Überweisungen, Lastschriften)

– Vereinheitlichung und Verkürzung der Ausführungs- und Wertstellungsfristen (z. B. müssen ab 01.01.2012 alle Zahlungsaufträge in Euro, unabhängig davon, ob es sich um inländische oder grenzüberschreitende Zahlungen handelt, innerhalb eines Geschäftstages ausgeführt werden)

Weitere gesetzliche Rahmenbedingungen für das Electronic-Banking sind im Telemediengesetz (TMG) und im Signaturgesetz (SigG) zu finden.

2.3 Haushaltsrecht

In den seit 01.01.2007 geltenden Kommunalhaushaltsverordnungen (Verordnungen über das Haushalts-, Kassen- und Rechnungswesen der Gemeinden, der Landkreise und der Bezirke nach den Grundsätzen der Kameralistik oder der doppelten kommunalen Buchführung – KommHV-Kameralistik/KommHV-Doppik) ist der Einsatz von elektronischen Zahlungsverkehrssystemen in § 37 Abs. 1 KommHV-Kameralistik sowie § 33 Abs. 1 KommHV-Doppik näher geregelt. Weitere Bestimmungen zum elektronischen Zahlungsverkehr sind in den Vorschriften über die Einrichtung und den Geschäftsgang der Kasse, zur Abwicklung des Zahlungsverkehrs (§ 43 Abs. 3 Satz 2 und § 47 KommHV-Kameralistik, § 39 Abs. 3 Satz 2 und § 43 KommHV-Doppik) und zu den haushaltrechtlich zulässigen Arten elektronischer Signaturen (§ 87 Nr. 12 KommHV-Kameralistik, § 98 Nr. 21 KommHV-Doppik) zu finden. Bei der Auswahl und beim Einsatz von elektronischen Zahlungsverkehrssystemen sind diese materiellrechtlichen Vorgaben entsprechend zu berücksichtigen.

2.4 EU-Zahlungsdiensterichtlinie/SEPA-Zahlungsinstrumente

Für eine noch nicht näher bestimmte Übergangszeit[6] können die Zahlungsdienstnutzer auch nach Inkrafttreten der neuen (harmonisierten) Regelungen Überweisungen und Lastschriften sowohl nach den alten nationalen Regelungen als auch nach den neuen Bestimmungen und Verfahren vornehmen. Die Kreditinstitute wurden dagegen mit der Umsetzung der EU-Zahlungsdiensterichtlinie verpflichtet, spätestens ab November 2010 für die **SEPA**-Basislastschriften erreichbar[7] zu sein. Die aktuell möglichen Varianten und deren Unterschiede soll die Abbildung auf der folgenden Seite darstellen:

[6] Die Europäische Kommission hat am 16.12.2010 einen Vorschlag für die Formulierung einer Verordnung zur Etablierung von Anforderungen an Überweisungen und Lastschriften in Euro und zur Anpassung der EU-Verordnung 924/2009 (EU-Verordnung zur SEPA-Migration) veröffentlicht. Der Vorschlag sieht das Abschalten der bestehenden nationalen Verfahren (Enddatum) für Überweisungen 12 Monate nach Inkrafttreten der EU-Verordnung und für Lastschriften 24 Monate nach Inkrafttreten der EU-Verordnung vor.
(Quelle: Bankenverband http://www.voeb.de/de/themen/zahlungsverkehr/sepa_migration/)

[7] Offizieller Starttermin für die SEPA-Lastschriften (Core und B2B) war der 02.11.2009; ab 02.11.2010 bestand für die Kreditwirtschaft die Verpflichtung, für die SEPA-Basislastschriften (Core) erreichbar zu sein.

Aktuell mögliche Überweisungs- und Lastschriftverfahren

Abbildung 2

(in Anlehnung an Genossenschaftsbank Unterallgäu eG)

Verfahren / Rahmenbedingungen	Verfahren vor Umsetzung EU-Zahlungsdiensterichtlinie		Verfahren nach Umsetzung EU-Zahlungsdiensterichtlinie	
Überweisung				
	Überweisungsauftrag		**SEPA-Überweisung**	
Interbankenverhältnis	Überweisungsabkommen		SEPA-Rulebooks	
Inkassoverhältnis (Gläubiger<->Kreditinstitut Gläubiger)	Zahlungsdiensterahmenvertrag + Gutschrift		Zahlungsdiensterahmenvertrag + Gutschrift	
Deckungsverhältnis (Schuldner<->Kreditinstitut Schuldner)	Zahlungsdiensterahmenvertrag + Weisung		Zahlungsdiensterahmenvertrag + Weisung	
Mandat	Überweisungsauftrag		Überweisungsauftrag	
Identifikation Inkassostelle	Kto/BLZ		IBAN[a]/BIC[b]	
Ausführung (Auftrag in Euro)	ET[c] + 3 (ET + 1)[d]		ET[c] + 3 (ET + 1)[d]	
Ablehnung Bank	grds. Nein[e]		grds. Nein[e]	
Widerruf Kunde	grds. Unwiderruflich[f]		grds. Unwiderruflich[f]	
Lastschrift				
	Einzugsermächtigung	**Abbuchungsauftrag**	**SEPA-Basislastschrift**	**SEPA-Firmenlastschrift**
Interbankenverhältnis	Lastschriftabkommen	Lastschriftabkommen	SEPA-Rulebooks	SEPA-Rulebooks
Inkassoverhältnis (Gläubiger<->Inkassostelle)	Zahlungsdiensterahmenvertrag + Lastschriftauftrag	Zahlungsdiensterahmenvertrag + Lastschriftauftrag	Zahlungsdiensterahmenvertrag + Lastschriftauftrag	Zahlungsdiensterahmenvertrag + Lastschriftauftrag
Deckungsverhältnis (Schuldner<->Zahlstelle)	Zahlungsdiensterahmenvertrag + nachträgl. Autorisierung	Zahlungsdiensterahmenvertrag + vorherige Autorisierung	Zahlungsdiensterahmenvertrag + vorherige Autorisierung	Zahlungsdiensterahmenvertrag + vorherige Autorisierung
Mandat	Einzugsermächtigung (Einwilligung ggü. Gläubiger + nachträgl. Genehmigung)	Abbuchungsauftrag (Einwilligung ggü. Gläubiger + Auftrag an Zahlstelle)	SEPA-Basislastschriftmandat (Einwilligung ggü. Gläubiger + Auftrag an Zahlstelle)	SEPA-Firmenlastschriftmandat (Einwilligung ggü. Gläubiger + Auftrag an Zahlstelle)
Mandatsprüfung	nein	ja	nein	ja
Identifikation Gläubiger	nein	nein	Gläubiger-ID (Creditor Identifier)	Gläubiger-ID (Creditor Identifier)
Identifikation Inkassostelle	Kto/BLZ	Kto/BLZ	IBAN/BIC	IBAN/BIC
Ausführung	Fälligkeit bei Sicht	Fälligkeit bei Sicht	FT[g] - 5 (FT - 2)[h]	FT - 1[i]
Rückgabefristen	Schuldner: grds. 6 Wochen	entfällt	Zahlstelle: FT + 5 (bankfachl. Gründe) Schuldner: FT + 8 Wochen (autorisierte) Schuldner: FT + 13 Wochen (nicht autorisierte)	Zahlstelle: FT + 2 (bankfachl. Gründe) Schuldner: keine (autorisierte) Schuldner: FT + 13 Wochen (nicht autorisierte)
Datenformat	DTAUS/DTAZV[j]	DTAUS/DTAZV	SEPA-XML[k]	SEPA-XML

[a] **IBAN** = International Bank Account Number
[b] **BIC** = Bank Identifier Code
[c] ET = Einreichungs- bzw. Zugangstag (= Geschäftstag vgl. § 675 n Abs. 1 Sätze 2 bis 4 BGB)
[d] gilt seit 01.11.2009, ab 01.01.2012 nur noch ET + 1 GT (vgl. § 675 s Abs. 1 Sätze 1 und 2 BGB)
[e] außer vertragl. Voraussetzungen liegen nicht vor oder Ausführung wäre rechtswidrig
[f] außer bei Daueraufträgen bis zum Geschäftstag vor Ausführung
[g] FT = Fälligkeitstag (= Due Date)
[h] Setzt gemäß § 675 s Abs. 2 BGB die rechtzeitige Bekanntgabe nach den SEPA-Regelwerken voraus; erstmalige Basis-Lastschriften müssen fünf Tage, darauf folgende Lastschriften mindestens zwei Tage vor Fälligkeit bei der Zahlstelle vorliegen.
[i] Einmalige, erstmalige oder Folgelastschriften müssen gemäß den SEPA-Regelwerken für die SEPA-Firmenlastschrift einen Tag vor Fälligkeit bei der Zahlstelle vorliegen.
[j] **DTAUS/DTAZV** = nationale Datenträgeraustausch-Formate für Inlands- und Auslandszahlungsverkehr
[k] SEPA-**XML** = Zahlungsverkehrsaufträge im Extensible Markup Language gemäß ISO 20022

Aus unserer Sicht würde die von zahlreichen Verbänden geforderte gesetzliche Umstellungserleichterung (z. B. Anerkennung der Lastschrift-Einzugsermächtigungen als SEPA-Basislastschriftmandat) möglicherweise einige Kritikpunkte entschärfen. Falls – wie nach derzeitigem Rechtsstand – die bestehenden Einzugsermächtigungen durch die so genannten SEPA-Mandate ersetzt werden müssen, wäre dies für die einzugsermächtigten Unternehmen, Institutionen und Kommunen (z. B. Einziehung von Steuern, Gebühren und Beiträgen) mit einem erheblichen Mehraufwand verbunden. An der lebhaft geführten Diskussion[8] zur langfristigen Beibehaltung der bisherigen (nationalen) Überweisungs- und Lastschriftverfahren und der umfangreichen Kritik an der Komplexität und der Praxistauglichkeit der neuen SEPA-Überweisungs- und Lastschriftverfahren, insbesondere im Hinblick auf die Einholung der neuen Lastschriftmandate und die Verwendung von IBAN und BIC anstelle der gewohnten (nationalen) Kontonummern und Bankleitzahlen, beteiligen wir uns nicht.

3 Überblick über die aktuellen Sicherungs- und Übertragungsverfahren

Bei den von der Kreditwirtschaft angebotenen Electronic-Banking-Lösungen werden die Zahlungsverkehrsdaten und Kontoinformationen heutzutage nahezu ausschließlich[9] über die fast überall verfügbaren Internet-Verbindungen übertragen, da das Internet mit seinen standardisierten Diensten, seiner Verfügbarkeit und Bandbreite den technischen Anforderungen der Banken, Sparkassen und deren Kunden besser gerecht werden konnte. Um jedoch eine reibungslose und sichere Kommunikation zwischen Kunden- und Bankrechner zu gewährleisten, sind institutsübergreifend einheitliche Schnittstellen sowie Sicherungs- und Übertragungsverfahren notwendig, die sowohl den Privat- als auch den Firmenkunden eine sichere und reibungslose Abwicklung der elektronischen Bankgeschäfte ermöglichen sollen. Da es sich beim Internet um ein unsicheres Weitverkehrsnetz handelt, waren die Anforderungen an die Qualität und Sicherheit der anwendungsspezifischen Authentifizierungs-, Autorisierungs-, Transport- und Verschlüsselungsverfahren besonders hoch. Im Laufe der Zeit entstand für den Privatkundenbereich ein nachrichten- bzw. transaktionsorientiertes und für den Firmenkundenbereich ein dateiorientiertes Sicherungs- und Übertragungsverfahren.

3.1 FinTS

Für die Anwender von Homebanking-Lösungen wurde vom ZKA im Jahre 1996 erstmals das Homebanking Computer Interface (HBCI) veröffentlicht. Bereits im Jahr 1997 wurde vom ZKA die technische Weiterentwicklung von HBCI als Financial Transaction Services (FinTS) veröffentlicht. FinTS ist nach mehreren Entwicklungsstufen nunmehr seit 2004 in der Version 4.0 verfügbar. In der aktuellen Version sind die Datenstrukturen ausschließlich in XML spezifiziert; sie unterstützt XML-Sigaturen und -Verschlüsselung, E-Mail/Push-Services oder verteilte Signaturen. FinTS wird aber nicht von allen Kreditinstituten und auch nicht immer in der aktuellsten Version unterstützt.[10]

---

[8] vgl. Verwaltungsinfos Bayerischer Landkreistag vom 11.01.2011, Az.: II-830-0/br, und vom 02.09.2010, Az.: II-830-0/br

[9] Beim Einsatz der FTAM-Lösungen waren ISDN-Telefon-Verbindungen üblich; die Kreditwirtschaft war aber nur noch bis 31.12.2010 verpflichtet, FTAM zu unterstützen.

[10] Ob und in welchem Umfang FinTS von den Kreditinstituten unterstützt wird, kann beim ZKA unter dem Link http://www.hbci-zka.de/institute/institut_auswahl.htm abgefragt werden.

Der ZKA beschreibt FinTS auf seiner Website wie folgt:

„FinTS ist ein Standard zur Vereinheitlichung der Schnittstelle zwischen dem Bankkunden - zum Beispiel repräsentiert durch seine Finanzverwaltungssoftware oder ein Internetportal - und einem oder mehreren Kreditinstituten in identischer Weise. Ziel ist dabei die Gewährleistung von Multibankfähigkeit.

Bestandteile von FinTS sind außer dem grundlegenden Übertragungsprotokoll die fachliche Spezifikation von mehr als 130 Geschäftsvorfällen und eine ausgefeilte Sicherheitstechnik. Seit der Version 4.0 ist FinTS komplett in XML spezifiziert und wird damit kompatibel zu anderen internationalen Finanzdatenstandards. Über flexible Rollenmodelle und unterschiedliche Kommunikationsmöglichkeiten wie E-Mail/Push-Services ermöglicht der Standard die Nutzung des Protokolls für alle elektronischen Vertriebswege.

Kernstück der Sicherheitstechnik ist das bewährte Home Banking Computer Interface (HBCI)-Verfahren, das auf Basis der Banken-Signaturkarte eine komfortable Absicherung der Auftragsdaten erlaubt. Aber auch TAN-basierte Verfahren wie chipTAN oder mobileTAN sind von der Protokollstruktur her unterstützt. Verteilte Signaturen erlauben eine zeitlich und örtlich unabhängige Freigabe von Aufträgen.

FinTS wird zurzeit von ca. 2.000 Kreditinstituten unterstützt und kontinuierlich fortgeschrieben. So wird zum Beispiel auch der neue SEPA-Zahlungsverkehr unterstützt.“

3.2 EBICS

Als Nachfolger für das bei Firmenkunden bewährte, technisch aber überholte BCS/FTAM-Sicherungs- und Übertragungsverfahren regte der ZKA im Jahre 2003 die Erweiterung des DFÜ-Abkommens um eine internetbasierende Variante an, die als Electronic-Banking Internet Communication Standard (EBICS) bezeichnet wird. Damit war es auf Basis des DFÜ-Abkommens möglich, auch Kunden mit hohem Zahlungsverkehrsaufkommen einen einheitlichen und multibankfähigen Bankenstandard auf Basis von Internetdiensten bereitzustellen. Seit 01.01.2008 besteht die bankseitige Verpflichtung zur Unterstützung von EBICS, d. h. alle Kreditinstitute in Deutschland sind mit diesem einheitlichen Standard erreichbar. EBICS wurde von Anfang an in XML spezifiziert, unterstützt alle elektronisch angebotenen Zahlungsverkehrsdienste und räumlich verteilte Signaturen.

EBICS wird vom ZKA wie folgt beschrieben:

„Die im Zentralen Kreditausschuss zusammengeschlossenen Spitzenverbände des Kreditgewerbes haben Änderungen an den technischen Anlagen des DFÜ-Abkommens beschlossen. Ziel ist die Weiterentwicklung von EBICS als attraktiver Electronic-Banking-Standard für Kunden des deutschen und europäischen Kreditgewerbes.

Die Schnittstellenspezifikation zum ‚Abkommen über die Datenfernübertragung zwischen Kunde und Kreditinstitut' (DFÜ-Abkommen) beschreibt die sichere Kommunikation zwischen Kunden und Kreditinstituten. Dabei erfüllt insbesondere der seit 1. Januar 2008 für alle deutschen Kreditinstitute verbindliche ‚Electronic Banking Internet Communication Standard' (EBICS) auf hohem Sicherheitsniveau die aktuellen Anforderungen an eine moderne, schnelle und flexible Kommunikation über das Internet. Die bankseitige Verpflichtung zur Unterstützung des Vorgängerstandards FTAM entfällt zum 31. Dezember 2010.

Die Vorteile des EBICS-Standard sind die sichere Datenübertragung über das Internet, ein modernes Schlüsselmanagement und die verteilte elektronische Unterschrift (VEU). Die vollständige Spezifikation sowie die XML-Schemata sind unter www.ebics.org hinterlegt."

3.3 Vergleich FinTS/EBICS

Um den Kommunen die Entscheidungsfindung bei der Auswahl des für die örtlichen Verhältnisse am besten geeigneten Sicherungs- und Übertragungsverfahrens zu erleichtern, haben wir in der nachfolgenden Abbildung die Leistungsmerkmale der beiden von der Kreditwirtschaft angebotenen Sicherungs- und Übertragungsverfahren dargestellt:

Abbildung 3

Vergleich der Sicherungs- und Übertragungsverfahren

Merkmal \ Verfahren	FinTS (HBCI)	EBICS
Transportwege und Sicherungsverfahren		
- Übertragungsweg	Internet	Internet
- Transportprotokoll	TCP/IP, HTTPS[a)]	HTTPS
- Verschlüsselungsprotokoll (auf Transportebene)	SSL	SSL/TLS
- Verschlüsselungsprotokoll (auf Anwendungsebene)		ZKA-Verschlüsselung
- Sicherungsverfahren	PIN/TAN, Kennung/Schlüsseldatei, PIN/Chipkarte	PIN/Schlüsseldatei, PIN/Chipkarte
- Schnittstelle Anwendung	XML (ab V 4.0)	XML
- Signaturerstellungseinheiten	DDV-Chipkarte und ZKA-Banken-Signaturkarte	ZKA-Banken-Signaturkarte
Sicherheitsmerkmale		
- Authentifizierung	Kennung/PIN	PIN/Schlüsseldatei oder PIN/Chipkarte[b)]
- Autorisierung/Legitimation	PIN/TAN oder PIN/Schlüsseldatei oder PIN/Chipkarte	PIN/Schlüsseldatei oder PIN/Chipkarte[b)]
- Berechtigungen (mit Bank vereinbarte Befugnis)	E/A/B[c)]	E/A/B/T[c)]
- Mehrfachunterschriften	ja	ja
- Zeitlich und räumlich verteilte Unterschriften	ja[d)]	ja
- Reine Transportunterschrift	nein	ja
- Segmentierung[e)]	nein	ja
- Recovery	nein	ja
Aufträge/Geschäftsvorfälle Zahlungsverkehr		
- Umsatzabfrage (z.B. Tages-Umsätze SWIFT MT940)	ja	ja
- Kontoauszug (PDF-Format)	ja	nein[f)]
- Überweisung (national)	ja	ja
- Überweisung (SEPA)	ja	ja
- Terminüberweisung	ja	ja
- Daueraufträge	ja	Anlage
- Lastschrift (Einzugsermächtigung)	ja	ja
- Lastschrift (Abbuchungsauftrag)	ja	ja
- Lastschrift (SEPA-Basislastschrift)	ja	ja
- Lastschrift (SEPA-Firmenlastschrift)	ja	ja
- Auslandszahlung (SWIFT, Fränkl-Transfer)	nein	ja
- Auslandszahlung-EURO (SEPA)	ja	ja
Limits		
- Multibankfähig (Konten bei mehreren Banken)	ja mit Einschränkungen[g)]	ja
- Unterstützung durch Kreditinstitute	größtenteils	vollständig
- Datensätze pro Sammelüberweisung	500 bzw. 999 pro Sammelüberweisung[h)]	unbegrenzt
- Definition eigener (nationaler) Geschäftsvorfälle	ja	nein
- Aufbewahrungsdauer Umsätze	mindestens 180 Tage[i)]	mindestens 180 Tage[i)]

a) Das ehemals verfügbare Protokoll T-Online-Classic ist nicht mehr relevant.
b) mit Authentifizierungs- bzw. Autorisierungssignatur
c) E = Einzel-Verfügungsberechtigung; A = gemeinsame Verfügungsberechtigung; B = Mitzeichnungsberechtigung; T = Transportberechtigung
d) wird erst ab FinTS V 4.0 mit HBCI-Signaturkarte unterstützt
e) Merkmal nur im Massenzahlungsverkehr von Bedeutung
f) in aktuellen Spezifikationen vorgesehen, aber wegen fehlender gesetzlicher Regelung noch nicht näher definiert
g) pro Bank ist für jede unterschriftsberechtigte Person ein Sicherungsmedium (PIN/TAN-Liste oder Chipkarte) notwendig
h) Abhängig vom jeweiligen Service-Rechenzentrum; manche Kreditinstitute bieten automatische Splitting-Funktionen an, sodass mit FinTS gegebenenfalls auch mehr Datensätze mit einer Transaktion oder dem DTA-Geschäftsvorfall übertragen werden können.
i) Ist vom Service-Rechenzentrum abhängig: bei FinTS beträgt die Aufbewahrungsdauer im Service Rechenzentrum in der Regel 180 oder 360 Tage.

4 Überblick Electronic-Banking-Lösungen

4.1 Verwendung und Einsatz

Beim Einsatz von Electronic-Banking-Systemen werden die vom Kunden erfassten Zahlungsverkehrsdaten und sonstigen Geschäftsvorfälle entweder sofort, mit Abschluss der Eingabe im Internet-Banking-Portal, oder separat, mit einer entsprechenden Funktion der Zahlungsverkehrsprogramme, per Datenfernübertragung an das Kreditinstitut bzw. dessen Service-Rechenzentrum zur Ausführung übertragen. Gelegentlich erfolgt die Übermittlung der Zahlungsverkehrsdaten auch noch per Datenträger (Diskette oder CD). Die vom Kreditinstitut bereitgestellten Informationen über die dort geführten Girokonten (z. B. Umsätze, Salden, Zinsen, Entgelte oder Rechnungsabschlüsse) werden entweder direkt im Online-Dialog angezeigt (Internet-Browser) oder ebenfalls per Datenfernübertragung an das beim Kunden installierte Zahlungsverkehrsprogramm übertragen.

Soweit wir dies beurteilen können, werden bei den bayerischen Kommunen aller Größenklassen seit Jahren Electronic-Banking-Systeme für die Abwicklung des bargeld- und beleglosen Zahlungsverkehrs sowie für die Kontoführung verwendet. In erster Linie setzen die Kommunen dabei die für Firmenkunden gedachten Zahlungsverkehrsprogramme (z. B. SFIRM32, VR-NetWorld, ProfiCash, COTEL, StarMoney Business, WinData)[11] ein. Eher seltener anzutreffen sind im kommunalen Bereich browserbasierte Internet-Banking-Lösungen. Einige Kommunen nutzen zwischenzeitlich auch die Vorteile der (weitgehend) automatisierten Ist-Buchung bzw. automatisierten Kontierung auf Grundlage der elektronisch übermittelten und maschinell verarbeitbaren Kontoauszugsdaten, die allgemein als elektronischer Kontoauszug (ELKA)[12] bezeichnet werden. Eine seit Jahrzehnten ebenfalls erfolgreich genutzte Möglichkeit des Electronic-Banking soll in diesem Zusammenhang nicht unerwähnt bleiben. Es ist dies die Übertragung von Zahlungsverkehrsdaten über Service-Rechenzentren (z. B. monatliche Lohn- und Gehaltsauszahlungen über das AKDB-Rechenzentrum). Auf diese Variante[13] wollen wir aber im Rahmen dieses Beitrags nicht näher eingehen, da wir in diesem Beitrag die vor Ort eingesetzten Lösungen im Fokus haben.

Aus unserer Sicht vereinfachen und erleichtern die Online-Banking-Programme zahlreiche Verwaltungsprozesse in der Kasse und bieten den Kassenmitarbeitern unter anderem folgende Vorteile:

– aktuelle und schnelle Auskunft über Kontobewegungen und -stände

– vielfältige Such-, Auswertungs- und Filtermöglichkeiten über die auf den Girokonten nachgewiesenen Buchungen

– schnelle und einfache Übertragung der von automatisierten Verfahren bereitgestellten Zahlungsverkehrsdateien im DTAUS- bzw. DTAZV-Format an die kontoführenden Institute

---

11 Diese Auflistung möglicher Produkte erhebt weder einen Anspruch auf Vollständigkeit noch stellt die gewählte Reihenfolge eine Aussage in Bezug auf deren Qualität dar.

12 Die Bezeichnung als elektronischer Kontoauszug ist unseres Erachtens nicht ganz korrekt – vgl. Ausführungen in Abschnitt 5.

13 Kommuniziert ein Kunde nicht direkt mit seinem Kreditinstitut und schaltet stattdessen einen IT-Dienstleister, das so genannte Service-Rechenzentrum, in die Kommunikation ein, so gilt die „Vereinbarung über Richtlinien zur Beteiligung von Service-Rechenzentren am beleglosen Datenaustausch per Datenfernübertragung (DFÜ)“.

– Prüfung von Zahlungsverkehrsdateien auf Integrität und Vollständigkeit

– einfache Erfassung von Überweisungen und Lastschriften

– Verwaltung der Kontoverbindungsdaten von Zahlungsempfängern und -schuldnern

– automatisierte Buchung von elektronisch übermittelten Umsatzdaten über entsprechende Zusatzprogramme oder Schnittstellen zu den Online-Banking-Lösungen

4.2 Gefährdungspotenziale

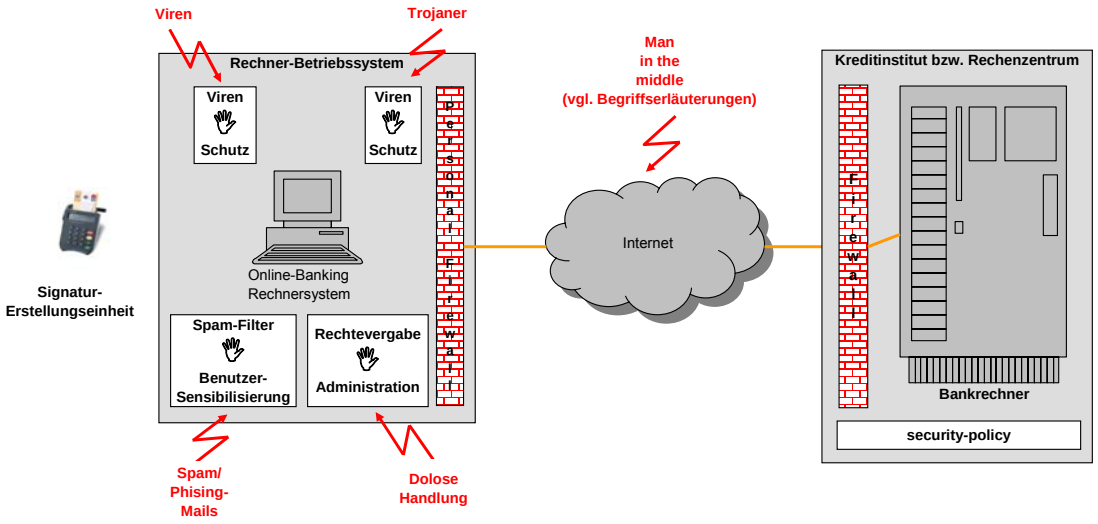
Online-Banking-PC sind, wie alle anderen Endgeräte, mit denen Internetdienste genutzt werden, potenzielles Ziel von Angriffen. An dieser Bedrohungslage wird sich wohl auch im Laufe der nächsten Jahre nichts ändern, wie die einschlägigen Statistiken eindrucksvoll belegen. Um diesen Gefahren wirksam zu begegnen, sind organisatorische (z. B. Schulung und Aufklärung der Benutzer, Dienstanweisung), aber auch einige, eigentlich selbstverständliche, technische Maßnahmen (z. B. zentrale und lokale Firewall, Virenschutz, eingeschränkte Benutzerrechte) notwendig, um erfolgreiche Angriffe zu verhindern oder zumindest zu erschweren.

Gefahren drohen aber nicht nur von außen, sondern auch von innen. Die in den letzten Jahren bekannt gewordenen dolosen Handlungen zeigen, dass es vereinzelt Mitarbeiter in der öffentlichen Verwaltung gibt, die sich in rechtswidriger Weise bereichern wollten. Bei der nachträglichen Betrachtung dieser Fälle hat sich oftmals gezeigt, dass diese Taten schneller entdeckt oder möglicherweise sogar verhindert hätten werden können, wenn die haushaltsrechtlichen Vorschriften beachtet und nicht nur als „formaler Kram“ abgetan worden wären. Wir wollen die Gefährdung von innen auch nicht überbewerten; dies würde der Loyalität und Vertrauenswürdigkeit der Bediensteten der öffentlichen Verwaltung nicht gerecht. Nachdem aber sämtliche der uns bekannten Unterschlagungsfälle von Innentätern begangen wurden, meinen wir, dass dieses Risiko gerade bei den organisatorischen Maßnahmen im Bereich der Kasse (z. B. Funktionstrennung, Vier-Augen-Prinzip, differenzierte Rechtevergabe nach dem Minimalprinzip) angemessen berücksichtigt werden sollte.

Die nachfolgende Abbildung soll nochmals die Gefährdungspotenziale veranschaulichen:

Der Online-Banking-PC als Ziel unterschiedlichster Angriffe

Abbildung 4
(in Anlehnung an FinTS V 4.0 Kompendium)



Wir wollen an dieser Stelle keinesfalls unnötig dramatisieren. Die Maxime in Bezug auf den Einsatz von Electronic-Banking-Lösungen sollte eher lauten:

„Gefahr erkannt, Gefahr gebannt“

4.3 Prüfungserfahrungen

Im Rahmen unserer überörtlichen Kassen- und Rechnungsprüfungen mussten wir immer wieder Feststellungen zu den Online-Banking-Vereinbarungen mit den Kreditinstituten, zur Konfiguration und zum Betrieb der eingesetzten Zahlungsverkehrsprogramme treffen. Zum einen wurden von den Kommunen grundlegende haushaltsrechtliche Bestimmungen, die der inneren Kassensicherheit dienen, nicht beachtet. Zum anderen betrafen unsere Prüfungsbemerkungen organisatorische und technische Mängel, die wir vor dem Hintergrund der oben beschriebenen Gefährdungspotenziale aufgegriffen haben, um einem Missbrauch der Online-Banking-Programme vorzubeugen und um die Vertraulichkeit, Verfügbarkeit und Integrität der IT sowie der gespeicherten und/oder übertragenen Daten zu gewährleisten.

Nachfolgend wollen wir die Kritikpunkte und Problembereiche aufgrund unserer Prüfungserfahrungen stichpunktartig darstellen:

– Einzel-Verfügungsberechtigung über die für das Online-Banking freigeschalteten Girokonten und fehlendes Vier-Augen-Prinzip bei elektronischen Überweisungen und Lastschriften

– fehlende Trennung der Fachaufgaben (Kasse) von der Administration der Hard- und Software

– keine Kontrolle von Zahlungsverkehrsdaten durch die Kasse, die in anderen Fachbereichen erstellt werden (z. B. Zahlungsverkehrsdateien im DTAUS-Format für Sozial- und Jugendhilfeauszahlungen)

– offenliegende und leicht einsehbare TAN- oder iTAN-Listen

– Schadprogramme (Viren, Trojaner und sonstige Malware) auf Rechnersystemen mit Zahlungsverkehrsprogrammen

– fehlender Virenscanner, nicht aktueller Virenscanner oder deaktivierte Firewall

– administrative Rechte (lokale oder Domänen-Admin-Rechte) der lokalen oder Domänen-Benutzerkonten

– Verwendung von Sammel-Benutzerkonten durch mehrere Anwender

– Weitergabe von Autorisierungsmedien und -informationen (Passworte, Signaturmedien, PIN) an Kolleginnen und Kollegen

Angesichts dieser Prüfungserfahrungen und der in Abschnitt 4.2 skizzierten Gefährdungspotenziale möchten wir in den nachfolgenden Ausführungen die jeweiligen Systeme sowie deren Vor- und Nachteile beschreiben und Empfehlungen zum sicheren, verantwortungsvollen und ordnungsgemäßen Einsatz von Online-Banking-Programmen geben.

4.4 Internet-Banking

Auf der Grundlage von Standard-Internetdiensten bietet die Kreditwirtschaft ihren Kunden schon seit einigen Jahren Internet-Banking-Portale an, die – unabhängig von den Öffnungszeiten – eine komfortable Kontoführung und die beleglose Einreichung von Zahlungsaufträgen von zu Hause bzw. vom Büro aus ermöglichen. Das Internet-Angebot der Kreditinstitute wendet sich vorrangig an private Nutzer, wird aber inzwischen auch von kleineren Kommunen oder Firmen mit geringem Zahlungsverkehr und wenigen Kontoverbindungen genutzt. Manche Kreditinstitute bieten zwischenzeitlich sogar spezielle Internet-Banking-Lösungen für Geschäftskunden mit erweitertem Leistungsumfang an. Für die Nutzung der Internetportale ist nur ein mit dem Internet verbundenes Endgerät (PC oder Terminal) und eines der gängigen Internet-Browser-Programme (z. B. MS Internet-Explorer, Firefox, Opera etc.) notwendig, weshalb dafür gelegentlich auch der Begriff „browsergestütztes Online-Banking“ verwendet wird. Die Verbindung zu den Internet-Banking-Portalen findet in der Regel auf der Grundlage von verschlüsselten Verbindungen über HTTPS/SSL statt. Als Autorisierungs- oder Legitimationsmedien werden PIN/TAN-Lösungen[14], HBCI-Signaturen oder neuerdings qualifizierte elektronische Signaturen verwendet, bei denen die Schlüsseldateien und Zertifikate auf USB-Speichersticks oder Smartcards[15] gespeichert sind. Die Sicherheit der Internet-Banking-Lösungen hängt unseres Erachtens sehr stark von der so genannten Endpoint-Security, also der lokalen Rechnerkonfiguration, der Wirksamkeit der technischen Schutzmaßnahmen (Virenscanner, Firewall, Patch-Stand Betriebssystem und Browser) und dem aufmerksamen und verantwortungsbewussten Umgang des Benutzers mit den am Arbeitsplatz verfügbaren Internetdiensten sowie den Authentifizierungsdaten (Benutzerkennung/Passwort) und Legitimationsmedien der Online-Banking-Lösungen ab.

[14] Meistens in Form von gedruckten TAN- oder iTAN-Listen; ChipTAN- oder mobileTAN-Verfahren haben wir noch nicht angetroffen.

[15] Für deren Einsatz sind allerdings ein Browser-Plugin und ein entsprechendes Lesegerät notwendig.

Als problematisch beim browsergestützten Online-Banking erachten wir, dass es in den letzten Jahren immer wieder zu massiven Angriffen von Internetkriminellen auf die Anwender solcher Lösungen kam, die bei entsprechend gutgläubigen und unbedarften Personen, nicht zuletzt aufgrund der dabei angewandten perfiden Methoden (z. B. **Phishing** und **Pharming**-Attacken), teilweise auch erfolgreich waren.[16] Wegen der fortschreitenden technischen Möglichkeiten, die zum Ausforschen, Manipulieren oder Fernsteuern fremder Rechnersysteme verfügbar sind[17], aber auch wegen der im geschäftlichen Umfeld (Aufgabenerledigung durch mehrere Personen, Vier-Augen-Prinzip bei Zahlungsaufträgen, Vertretungsregelungen) nur sehr schwer zu realisierenden Geheimhaltung der persönlichen TAN- oder iTAN-Listen, eignen sich Lösungen mit dieser Ausprägung unseres Erachtens nur bedingt für den kommunalen Bereich.[18]

Gleichwohl wollen wir mit diesem Beitrag keineswegs der Nutzung von browsergestützten Online-Banking-Lösungen eine grundsätzliche Absage erteilen. Die Kreditwirtschaft bietet inzwischen Lösungen mit verbesserten Autorisierungs-, Sicherungs- und Übertragungsverfahren (z. B. EBICS) an, die sich unseres Erachtens durchaus so konfigurieren und einsetzen lassen, dass sie aus heutiger Sicht als ausreichend sicher betrachtet werden können. Die meisten browsergestützten Online-Banking-Lösungen werden aus organisatorischen Gründen, vor allem wegen des auf den Privatanwender ausgerichteten Funktionsumfangs (z. B. hinsichtlich der damit möglichen Geschäftsvorfälle oder Auswertungen) und der verfahrensimmanenten Beschränkungen (z. B. maximale Anzahl der bei einer Transaktion übertragbaren Datensätze, Art und Umfang der möglichen Geschäftsvorfälle, keine Multibanking-Fähigkeiten), derzeit wohl nur für kleinere Kommunen mit geringem Zahlungsaufkommen und wenigen Kontoverbindungen in Betracht kommen. Allerdings ist zu erwarten, dass nicht nur die Sicherheit, sondern auch der Leistungsumfang der Online-Portal-Lösungen weiter zunimmt und diese künftig auch eine Lösungsalternative für mittlere und größere Kommunen sein können.

4.5 Zahlungsverkehrsprogramme

Den Firmenkunden, aber auch den Kommunen mit mittlerem oder größerem Zahlungsaufkommen werden von der Kreditwirtschaft in der Regel Online-Banking-Programme[19] angeboten, die den professionellen Anwendern eine bedarfsgerechte und möglichst effiziente Abwicklung der elektronischen Kontoführung (Zahlungsverkehr und Kontoinformationen) ermöglichen sollen. Diese Angebote unterscheiden sich im Allgemeinen von den Internet-Banking-Lösungen[20] durch ihren größeren Funktionsumfang, unterstützen auch den elektronischen Zahlungsverkehr und die Kontoführung mit mehreren Kreditinstituten[21], bieten bessere Auswertungs- und Filter-

---

16 vgl. u. a. BKA-Pressemitteilungen vom 06.09.2010 (http://www.bka.de/pressemitteilungen/2010/pm100906.html) und vom 28.07.2010 (http://www.bka.de/pressemitteilungen/2010/pm100728.html), BKA-Präsident Jörg Ziercke in Zeit-Online vom 01.09.2010 (http://www.zeit.de/digital/datenschutz/2010-09/online-banking-angriffe)

17 ZEUS und andere Trojaner, vgl. http://www.spiegel.de/netzwelt/web/0,1518,708911,00.html

18 Vgl. Handelsblatt etc.; ChipTAN und mobileTAN-Lösungen kommen unseres Erachtens im kommunalen Umfeld wegen der speziellen Anforderungen (Doppel-Unterschrift, Vertretungsregelungen, Substitut Unterschrift durch elektronische Signaturen) nicht in Betracht.

19 Von den Verwaltungen und der Kreditwirtschaft werden die beiden Begriffe Online-Banking-Programme und Zahlungsverkehrsprogramme synonym verwendet.

20 Mit der zunehmenden Leistungsfähigkeit der Internet-Banking Business-Lösungen verschwimmen diese Grenzen.

21 so genannte Multibankfähigkeit

möglichkeiten sowie Schnittstellen zu ERP[22]-Systemen und HKR[23]-Verfahren und zeichnen sich durch eine leistungsfähigere Benutzer- und Rechteverwaltung aus. Da die kontobezogenen Umsatzinformationen auf den Rechnersystemen des Kontoinhabers gespeichert sind, lassen sich mit diesen Programmen die haushaltsrechtlichen Nachweis- und Aufbewahrungsanforderungen (vgl. § 71 Abs. 1, § 82 Abs. 2 KommHV-Kameralistik oder § 67 Abs. 1, § 69 Abs. 2 KommHV-Doppik) leichter erfüllen.

Zudem bieten dedizierte Zahlungsverkehrsprogramme gegenüber den Internet-Banking-Systemen einen entscheidenden Vorteil. Sie sind aufgrund ihres Lösungskonzepts (Offline-Erfassung mit anschließender Online-Übertragung der Zahlungsverkehrsdaten oder sonstiger Aufträge) sowie den anwendungsspezifischen Sicherungs- und Übertragungsverfahren (FinTS oder EBICS) gegen Phishing- und Pharming-Attacken immun. Leider kann bei der zunehmenden Raffinesse und Spezialisierung der Schadprogramme (z. B. Trojaner ZEUS, Spy Eye oder URLzone) nicht ausgeschlossen werden, dass auch hierbei die Autorisierungs- und Legitimationsdaten ausgespäht[24] oder die damit gesicherten Zahlungsverkehrsdaten beim Kunden selbst oder beim Übertragungsvorgang manipuliert werden. Insoweit sollte auch bei den zunächst sicher erscheinenden Sicherungs- und Übertragungsverfahren die Sicherheit des Endgeräts im Auge behalten werden. Im Hinblick auf unsere Prüfungserfahrungen sollte der Online-Banking-PC nicht als „Surf-Arbeitsplatz“ für Azubis oder Praktikanten eingesetzt werden.

4.6 Vergleich der eBanking-Alternativen

Wegen der Vielfalt der von der Kreditwirtschaft angebotenen eBanking-Lösungen haben wir uns im Rahmen dieses Beitrags im Wesentlichen auf den für die Kommunen so wichtigen elektronischen Zahlungsverkehr konzentriert. Es ist uns klar, dass heutzutage über den elektronischen Zahlungsverkehr hinaus weit mehr Bankprodukte oder Geschäftsprozesse (z. B. eBrokerage) auf elektronischem Wege abgewickelt werden können. Wir haben uns aber auf typische Lösungen beschränkt, wie sie von den eBanking-Beratern der Banken und Sparkassen üblicherweise den bayerischen Kommunen angeboten werden.

Die Abbildung auf der folgenden Seite soll die Unterschiede der typischen eBanking-Lösungen nochmals auf einen Blick verdeutlichen:

[22] Enterprise Resource Planning

[23] Haushalts-, Kassen- und Rechnungswesen

[24] Ein solches Ausspähen kann nur mit vom Betriebssystem des PC unabhängigen Geräten und Prozessen (sog. sichere Signaturerstellungseinheiten) erreicht werden.

Vergleich der eBanking-Lösungen

Abbildung 5

Verfahren / Merkmale	Internet-Banking		Zahlungsverkehrsprogramme mit FinTS (HBCI)			Zahlungsverkehrsprogramme mit EBICS	
	Private	Business	PIN/TAN	Schlüsseldatei	Chipkarte	Schlüsseldatei	Chipkarte
Einsatzbedingungen							
- Benutzer-Interface	Internet-Portal		Zahlungsverkehrssoftware			Zahlungsverkehrssoftware	
- Nutzungsvoraussetzung	Browserinstallation		Installation Software			Installation Software	
- Übertragungsweg	Internet (TCP/IP, HTTPS(SSL), EBICS[a])		Internet (TCP/IP, SSL/TLS, FinTS/HBCI ab V 3.0)			Internet (TCP/IP, TLS, EBICS)	
Sicherheitsmerkmale							
- Authentifizierung	Kennung/PIN oder Kennung/Key oder Chipkarte/PIN		Kennung/Passwort			Kennung/Passwort	
- Autorisierung/Legitimation	PIN/TAN oder Chipkarte/PIN		PIN/TAN	PIN/Datei	Chipkarte/PIN	Kennung/PIN	Chipkarte/PIN
- Berechtigungen (mit Bank vereinbarte Befugnis)	E/A/B	E/A/B	E/A/B			E/A/B/T	
- Mehrfachunterschriften	nein	ja	ja			ja	
- Zeitlich und räumlich verteilte Unterschriften	nein	ja[b]	ja[c]			ja	
Geschäftsvorfälle							
- Umsatzabfrage	ja	ja	ja			ja	
- Kontoauszug (PDF-Format)	ja	ja	ja			ja	
- Überweisung (national)	ja	ja	ja			ja	
- Überweisung (SEPA)	ja	ja	ja			ja	
- Terminüberweisung	ja	ja	ja			ja	
- Daueraufträge	ja	ja	ja			Anlage	
- Lastschrift (Einzugsermächtigung)	nein	ja	ja			ja	
- Lastschrift (Abbuchungsauftrag)	nein	ja	ja			ja	
- Lastschrift (SEPA-Basislastschrift)	nein	ja	ja			ja	
- Lastschrift (SEPA-Firmenlastschrift)	nein	ja	ja			ja	
- Auslandszahlung (SWIFT, Fränkli-Transfer)	nein	nein	nein			ja	
- Auslandszahlung-EURO (SEPA)	ja	ja	ja			ja	
Schnittstellen							
- Datenimport		DTA	DTA, CSV, MT940, MT942			DTA, CSV, MT940, MT942, ISO 20222	
- Datenexport		CSV/MT940	DTA, CSV, MT940			DTA, CSV, MT940	
Limits							
- Multibankfähig (Konten bei mehreren Banken)	nein	nein	ja mit Einschr.[d]			ja	
- Mehrere Konten bei einer Bank	ja	ja	ja			ja	
- Datensätze pro Sammelüberweisung	<= 10	<= 500	500 bzw. 999 pro Sammelüberweisung			unbegrenzt	
- Aufbewahrungsdauer Umsätze	90 bis 120 Tg	90 bis 120 Tg	unbegrenzt			unbegrenzt	
Beurteilung							
- Sicherheitsniveau[e]	2 - 5[f]	2 - 5	4	3[g]	1	2	1
- Eignung für Kommune	nein	ja, mit Chipkarte/Pin[h]	nein	nein	ja	nein	ja
- Funktionsumfang	niedrig bis mittel	mittel	mittel			hoch	
- Zahlungsverkehrsaufkommen	niedrig	niedrig	mittel			hoch	
- Zielgruppe	Private	kleine Unternehmen	mittlere Unternehmen			große Unternehmen	

[a] auf der Basis von EBICS werden inzwischen auch multibankfähige Online-Portal-Lösungen angeboten (z.B. Travic-Port der SIZ)
[b] nur mit Banken-Signaturkarte
[c] wird erst ab FinTS V 4.0 unterstützt
[d] Pro Bank ist bei FinTS für jede unterschriftsberechtigte Person je eine PIN/TAN-Liste, eine Schlüsseldatei oder eine Chipkarte erforderlich.
[e] nach Art, Umfang und Stärke der Sicherheitsmaßnahmen und unter Berücksichtigung der bekannten Angriffsszenarien
(Signatur mit Banken-Signaturkarte = 1; EBICS-Signatur mit Schlüsseldatei = 2; HBCI-Signatur mit Schlüsseldatei = 3; HBCI-PIN/TAN = 4; SSL-PIN/TAN = 5)
[f] abhängig vom gewählten Authentifizierungsinstrument
[g] Bewertung gilt nur für FinTS/HBCI 3.0 und höher (vgl. Uni-Tübingen - Trojanersichere Online Accounts)
[h] sofern der PC nach den Empfehlungen der Kreditwirtschaft abgesichert ist

Die signaturbasierenden Varianten, bei denen sowohl die persönlichen und öffentlichen Signaturschlüssel als auch die Zertifikatsinformationen auf so genannten Smartcards gespeichert sind, haben wir aus folgenden Gründen besser bewertet:

– Nach den haushaltsrechtlichen Vorschriften kann die Schriftform bei Überweisungs- und Lastschriftaufträgen nur durch elektronische Signaturen ersetzt werden (vgl. § 43 Abs. 3 Satz 2 KommHV-Kameralisitik, § 39 Abs. 3 Satz 2 KommHV-Doppik).

– Die Authentizität und Integrität der signierten Zahlungsverkehrsdaten wird durch die verwendeten elektronischen Zertifikate, Hash- und Verschlüsselungsverfahren nachprüfbar sichergestellt.

– Die von der Kreditwirtschaft empfohlenen Signaturerstellungseinheiten (Lesegeräte der Sicherheitsklasse 3 oder Bank-Secoder) lassen eine vom Rechnersystem und dessen Sicherheit unabhängige Erzeugung der elektronischen Signaturen zu.

– Die 2-Faktor Autorisierung bzw. Legitimation der Zahlungsaufträge mit Smartcard und PIN setzt den Besitz der Chipkarte und das Wissen über die zugehörige PIN voraus.

Die oftmals noch anzutreffenden PIN/TAN- oder PIN/iTAN-Sicherungsverfahren auf Basis gedruckter Listen haben wir bewusst nicht mehr in die vorstehende Aufstellung und Bewertung einbezogen, da wir diese weder für zeitgemäß noch für ausreichend sicher erachten. Wir dürfen in diesem Zusammenhang auf eine Aussage des ZKA in seiner aktuellen Broschüre[25] mit dem Titel „ZKA-KOMPENDIUM ONLINE-BANKING-SICHERHEIT“, Stand 09.11.2009, verweisen:

„Das PIN/TAN-Verfahren bietet seit einigen Jahren keinen passenden Schutz mehr gegen die immer besser werdenden Angriffe. Daher kümmert sich der Zentrale Kreditausschuss seit Jahren um die Weiterentwicklung solcher Sicherheitsmaßnahmen und hat sich auch auf einige grundlegende Verfahren geeinigt, die bei vielen Banken und Sparkassen zum Einsatz kommen und das Sicherheitsniveau im Vergleich zum klassischen PIN/TAN Verfahren anheben können.“

Daneben finden wir unsere Ansicht auch in diversen Presseberichten[26] bestätigt.

4.7 Datenträgeraustausch

Die älteste Form des Electronic-Banking ist das im Jahre 1976 eingeführte Verfahren zum Datenträgeraustausch mit den kontoführenden Kreditinstituten bzw. deren Service-Rechenzentren. Dementsprechend erscheinen die Spezifikationen der für den Datenträgeraustausch zugelassenen Speichermedien (z. B. 5 ¼-Zoll oder 8-Zoll-Disketten) nicht mehr ganz zeitgemäß. Der Datenträgeraustausch ist streng genommen kein medienbruchfreies elektronisches Verfahren, da neben dem Datenträger auch der so genannte Datenträgerbegleitzettel (enthält unter

[25] Diese Broschüre kann beim ZKA unter dem Link http://www.hbci-zka.de/dokumente/diverse/ZKA Kompendium Online-Banking-Sicherheit V1.0 final version.pdf heruntergeladen werden.

[26] vgl. https://www.kartensicherheit.de/ww/de/pub/oeffentlich/sicher_bezahlen/kartenzahlung_im_internet/chipkartenleser_internet/secoder.php, http://www.banktip.de/News/22132/Sicheres-Onlinebanking-mTAN-oder-Secoder.html, http://www.heise.de/ct/artikel/Zahl-oder-Karte-291676.html

anderem als Sicherungsmaßnahme die Summe der Datensätze, Bankleitzahlen, Kontonummern und Beträge sowie die Unterschriften der Verfügungsberechtigten) eingereicht werden muss. In der Praxis stellen aber sowohl die zugelassenen Speichermedien als auch der Datenträgerbegleitzettel keine besonders hochwertigen Schutzmaßnahmen dar, zumal die für den Datenträgeraustausch generierten Zahlungsverkehrsdateien[27] in der Regel auch mit den Zahlungsverkehrsprogrammen editiert oder mit Internet- oder Online-Banking-Lösungen per DFÜ an die Kreditinstitute bzw. deren Service-Rechenzentren übertragen werden können. Über den Datenträgeraustausch bzw. die DTAUS- und DTAZV-Dateiformate lässt sich sowohl der beleglose Massen- als auch der Individualzahlungsverkehr abwickeln. Mit dem zunehmenden Einsatz von Internet- oder Online-Banking-Programmen ist der Datenträgeraustausch in der Praxis allerdings immer seltener anzutreffen. Da die verwendeten Speichermedien (in der Regel werden 3 ½-Zoll-Disketten eingesetzt) jederzeit gelesen oder überschrieben werden können und die vorher erwähnten Kontrollsummen keinen wirksamen Schutz vor Manipulationen[28] bieten, müssen sowohl die sichere Aufbewahrung als auch der sichere Transport der Medien zum Kreditinstitut durch entsprechende organisatorische Maßnahmen gewährleistet sein. Sowohl aus organisatorischer als auch aus technischer Sicht ist die Online-Übertragung der elektronisch signierten Zahlungsverkehrsdaten mit den Transport- und Übertragungsprotokollen HTTPS, FinTS oder EBICS unseres Erachtens deutlich sicherer.

4.8 Zusammenfassung

Bei der Abwicklung von Geschäften über das Internet sollte die Sicherheit grundsätzlich an erster Stelle stehen. Dies gilt in besonderem Maße für das Online-Banking. Insoweit stand diese Maxime auch bei unseren Überlegungen und Wertungen immer im Vordergrund.

Aufgrund vorstehender Ausführungen empfehlen wir, bei Auswahl und Einsatz von Internet-Banking-Lösungen bzw. Zahlungsverkehrsprogrammen auf Folgendes zu achten:

– Einsatz von signaturbasierenden Authentifizierungs- und Autorisierungsverfahren, bei denen sichere Signaturerstellungseinheiten[29] (z. B. Banken-Signaturkarten, Lesegeräte der Sicherheitsklasse 2 und höher oder die sog. Bank-Secoder[30]) verwendet werden; dies bedeutet, dass in Kommunalkassen weder TAN- oder iTAN-Listen[31] noch ChipTAN-Verfahren, TAN-Generatoren oder mobileTAN-Verfahren[32] eingesetzt werden sollten.

---

27 DTAUS-Format für Inlandszahlungsverkehr; DTAZV für Auslandszahlungsverkehr; vgl. Begriffserläuterungen

28 Hinzu kommt, dass das DTAUS- oder DTAZV-Format mit vielen Programmen lesbar ist und die so gespeicherten Daten leicht editiert werden können.

29 Aus diesem Grund dürfen Signaturschlüssel oder andere Kryptodaten (z. B. Signaturdatei) nicht auf internen oder externen Speichermedien (z. B. USB-Speichermedien) gespeichert werden, die dauerhaft oder temporär mit dem Endgerät verbunden und von dessen Betriebssystem kontrolliert werden.

30 Empfohlen werden Lesegeräte der Sicherheitsklasse 3 oder Bank-Secoder, da diese dem Benutzer die zu signierenden Daten anzeigen („what you see, is what you sign“).

31 Diese Legitimationsmedien scheiden schon aus Gründen der internen und externen Kassensicherheit aus.

32 Die ChipTAN- oder mobileTAN-Verfahren sowie die TAN-Generatoren sind aus Sicht der externen Kassensicherheit derzeit zwar als ausreichend sicher anzusehen, kommen jedoch aufgrund § 43 Abs. 3 Satz 2 KommHV-Kameralistik bzw. § 39 Abs. 3 Satz 2 KommHV-Doppik für die Kommunen nicht in Betracht, da sie keine elektronischen Signaturen erzeugen; außerdem weisen wir darauf hin, dass das mobileTAN-Verfahren offenbar schon erfolgreich durch eine mehrstufige Attacke eines speziell konfigurierten ZEUS-Trojaners und einer Phishing-SMS angegriffen wurde (vgl. www.heise.de/security/meldung/Banking-Trojaner-ZeuS-nimmt-SMS-TAN-Verfahren-ins-Visier-1096613.html).

– keine Einzel-Verfügungsberechtigungen (sog. E-Unterschrift) über die Konten[33], sondern Umsetzung des haushaltsrechtlich vorgeschriebenen „Vier-Augen-Prinzips“ durch eine sinnvolle Kombination von gemeinsamen Verfügungsberechtigungen (sog. A-Unterschriften) und Mitzeichnungsberechtigungen (sog. B-Unterschriften) gegebenenfalls ergänzt mit Transportberechtigungen (sog. T-Unterschriften)

– Absicherung der Endgeräte gegenüber Schadprogrammen nach den jeweils aktuellen Empfehlungen der Kreditwirtschaft[34] und des BSI[35]. Hierzu sind die Kunden auch nach den AGB der Kreditwirtschaft verpflichtet.

– regelmäßige Kontrolle der in den Zahlungsverkehrsprogrammen nachgewiesenen Salden und Umsätze anhand der gedruckten oder elektronisch signierten Kontoauszüge

Die Kommunen müssen daher, abhängig von den örtlichen Sicherheitsbedürfnissen[36] und Leistungsanforderungen, den haushaltsrechtlichen Nachweis- und Aufbewahrungspflichten sowie den technischen und organisatorischen Rahmenbedingungen, für sich selbst entscheiden, welche Online-Banking-Lösung sich letztendlich am besten für die Abwicklung des Zahlungsverkehrs und die Kontoführung eignet.

5 Aufbewahrung und Beweiskraft elektronischer Kontoauszüge

In seiner Broschüre „Elektronische Kontoauszüge – Informationen für Privatkunden“[37] charakterisiert der Bankenverband das Wesen des Kontoauszugs wie folgt:

„*Mit dem Kontoauszug stellt die Bank dem Kunden Informationen über die Umsätze auf seinem Girokonto und den daraus resultierenden Kontostand zur Verfügung. Davon zu unterscheiden ist der meist am Quartalsende erstellte Rechnungsabschluss, in dem die Ein- und Ausgänge auf dem Girokonto saldiert und eventuelle Soll- und Habenzinsen sowie die mit der Bank vereinbarten Kontoführungsentgelte abgerechnet werden.“*

Rechtsgrundlage für die Erstellung von Kontoauszügen sind die in Art. 248 §§ 7 bis 10 EGBGB geregelten Informationspflichten der Kreditinstitute und die AGB der Banken und Sparkassen. Da der Kontoauszug, wie vom Bankenverband erläutert, mehrere Funktionen erfüllt (z. B. als Rechnung über steuerpflichtige Bankumsätze, als Abrechnung über umsatzsteuerfreie Bankleistungen oder als Nachweis von Buchungsvorgängen), wird in den AGB der Banken und Sparkassen ausdrücklich zwischen Rechnungsabschlüssen und sonstigen Kontoauszügen unterschieden. Ob die im **SWIFT** MT940-Format oder einem anderen Format an ein Zahlungs-

---

33 Dies gilt sowohl für die beleggebundenen als auch für die beleglosen Zahlungsverkehrsaufträge.

34 vgl. unter anderem Broschüre Bankenverband „Wege zum Online Banking, Mai 2008, Fiducia – Sicherheit beim Online-Banking (http://www.fiducia.de/Presse/verbraucherthemen/Sicheres_Online_Banking.html)

35 vgl. BSI Online-Banking Sicherheitstipps (https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/OnlineBanking/Sicherheitstipps/sicherheitstipps_node.html)

36 die idealerweise in einer so genannten security-policy nachvollziehbar festgelegt sind

37 Die Broschüre „Elektronische Kontoauszüge – Informationen für Privatkunden“, 2. Auflage, Juli 2009, steht unter dem Link https://www.bankenverband.de/publikationen/ods/elektronische-kontoauszuge/01-br0709_Elektronische-Kontoauszuege.pdf/download zum Download zur Verfügung.

verkehrsprogramm übermittelten kontobezogenen Daten (z. B. Tages-Kontoumsätze, Salden, Avise etc.) als Kontoauszug angesehen werden können, hängt von den jeweiligen Vereinbarungen der Kreditinstitute mit den Kunden und deren Inhalt ab.[38] Insoweit können die über FinTS oder EBICS übertragenen Kontoinformationen wohl nicht in jedem Fall mit dem papiergebundenen, am Bankdrucker ausgegebenen Kontoauszug oder den von den Kreditinstituten im PDF-Format übermittelten elektronischen Kontoauszügen gleichgesetzt werden.

In der Vergangenheit gab es darüber hinaus immer wieder Diskussionen zur steuerrechtlichen Verbindlichkeit der elektronischen Kontoauszüge. Mehrfach vertraten die Finanzbehörden[39] in der Vergangenheit die Auffassung, dass nur Steuerzahler ohne Buchführungs- und Aufzeichnungspflichten nach §§ 145 ff. AO mit einem Ausdruck der elektronisch übermittelten Kontoauszugsdaten ihren Nachweispflichten gegenüber den Finanzbehörden entsprechen können. In Bezug auf die buchführungspflichtigen Unternehmen sahen die Finanzbehörden die elektronischen Kontoauszüge dagegen als „originär digitale Daten“ an, die – sofern sie steuerrelevant sind – den Anforderungen nach den §§ 145 ff. AO, den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)[40] und den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)[41] unterliegen, nach denen die Buchführungspflichtigen neben der maschinellen Auswertbarkeit auch die Authentizität und Integrität der digitalen Daten gewährleisten müssen, was aber mit den eingesetzten Verfahren regelmäßig nicht möglich sei.[42]

Wir hatten uns bislang mit Blick auf die Grundsätze ordnungsgemäßer Verwaltungsbuchführung (vgl. § 61 KommHV-Kameralistik, § 57 KommHV-Doppik) dieser von den Finanzbehörden vertretenen Auffassung angeschlossen. Zudem war aus unserer Sicht aufgrund der Import-, Export- oder Löschfunktionen der vor Ort eingesetzten Online-Banking-Programme weder die Vollständigkeit noch die Integrität der in den Online-Banking-Programmen gespeicherten Daten sichergestellt. Wir haben deshalb im Interesse der Nachvollziehbarkeit, Vollständigkeit und Sicherheit der Buchführung gefordert, die papiergebundenen Kontoauszüge regelmäßig mit den Salden der Online-Banking-Programme abzugleichen.

Mit Schreiben vom 28.07.2010, Az.: S 0317.1.1 – 3/1 St 42, hat das Bayerische Landesamt für Steuern (LfSt)[43] nun erneut zu diesem Problem Stellung genommen und dargestellt, unter welchen Voraussetzungen die an Buchführungs- und Aufzeichnungspflichtige im Sinne der §§ 145 ff. AO übermittelten elektronischen Kontoauszüge als rechtsverbindlich angesehen

---

38 In den uns vorliegenden AGB zur Nutzung der Online-Banking-Anwendung „Elektronischer Kontoauszug“ wurde beispielsweise für die Rechtsverbindlichkeit der an die Online-Banking-Software übertragenen Daten gefordert, dass bei der Visualisierung der Daten der Name des Instituts und des Kontoinhabers sowie der Hinweis auf den Rechnungsabschluss und die damit verbundenen Rechtsfolgen (Genehmigungsfiktion) auf dem elektronischen Kontoauszug sichtbar sind und die maximale Anzahl von 14 Verwendungszweckzeilen je Umsatz von der Software dargestellt wird; ebenso muss sich auch aus den elektronischen Kontoauszügen der alte und neue Kontostand und die laufende Nummer des jeweiligen Auszugs zweifelsfrei und revisionssicher ergeben.

39 Vgl. Schreiben der OFD München vom 06.08.2004, Az.: S 0317 – 34 St 324, Verfügung der OFD Koblenz vom 30.11.2005, Az.: S 0315 A, Verfügung der OFD Münster vom 17.05.2005 (Kurzinformation Nr. 18/2005); lt. Broschüre des Bankenverbandes vertrat auch das BMF mit Schreiben vom 17.03.2006 diese Rechtsauffassung.

40 vgl. BMF Schreiben vom 07.11.1995, Az.: IV A 8 - S 0316 - 52/95, BStBl 1995 I S. 738

41 vgl. BMF Schreiben vom 16.07.2001, Az.: IV D 2 - S 0316 - 136/01, BStBl 2001 I S. 415

42 vgl. dazu die ausführlichen Erläuterungen in den Nrn. 10 ff. der Broschüre des Bankenverbandes, a. a. O.

43 vgl. AO-Kartei BY § 147 AO Karte 3

werden können. Bei den selbst aufbewahrten elektronischen Kontoauszügen setzt dies voraus, dass die übermittelten und gespeicherten Daten

– auf maschinell auswertbaren Datenträgern archiviert werden (§ 147 Abs. 2 und 5 AO sowie Tz. VIII/b Nr. 2 des BMF-Schreibens vom 07.11.1995, a. a. O.),

– die Authentizität und Integrität der Daten durch elektronische Signaturen sichergestellt ist und

– bei der Aufbewahrung und Speicherung sowohl die Grundsätze ordnungsgemäßer Buchführung (GoB) als auch die GoBS beachtet werden.

Wir schließen uns der vom LfSt vertretenen Rechtsauffassung an und werden bei unseren künftigen überörtlichen Prüfungen die nach diesen steuerrechtlichen Grundsätzen aufbewahrten elektronischen Kontoauszüge (z. B. mit qualifizierten Signaturen versehene PDF-Dateien) als verbindlich akzeptieren. An unseren Empfehlungen zum regelmäßigen Abgleich der auf den papiergebundenen oder den elektronisch signierten Kontoauszügen nachgewiesenen Umsätze und Salden mit denjenigen der Zahlungsverkehrsprogramme halten wir allerdings nach wie vor fest, weisen aber zugleich darauf hin, dass auch Programme, die der Abwicklung des Zahlungsverkehrs dienen, seit 01.01.2007 ohnehin den haushaltsrechtlichen Anforderungen an automatisierte Verfahren unterliegen. Demzufolge sind Eingriffe in solche Programme grundsätzlich untersagt und müssen, falls diese unumgänglich sind, entsprechend dokumentiert werden (vgl. § 37 Abs. 1 Nr. 8 KommHV-Kameralistik, § 33 Abs. 1 Nr. 8 KommHV-Doppik).

6 Verzicht auf Schriftform bei elektronisch signierten Überweisungs- und Lastschriftaufträgen

Nach den aktuell geltenden haushaltsrechtlichen Vorschriften sind Überweisungs- und Abbuchungsaufträge, Einzugsermächtigungen und Schecks von zwei Beschäftigten zu unterzeichnen. Beim Einsatz automatisierter Verfahren können die Unterschriften durch qualifizierte elektronische Signaturen im Sinne von § 2 Nr. 3 SigG oder fortgeschrittene elektronische Signaturen im Sinne von § 2 Nr. 2 SigG mit besonderen Merkmalen, die in der AFS-HKR[44] näher definiert sind, ersetzt werden (vgl. § 87 Nr. 12 KommHV-Kameralistik bzw. § 98 Nr. 21 KommHV-Doppik). Da es sich bei den in Online-Banking-Verfahren eingesetzten Signaturen überwiegend um fortgeschrittene elektronische Signaturen im Sinne von § 2 Nr. 2 SigG ohne die geforderten besonderen Merkmale handelt, haben wir im Hinblick auf die haushaltsrechtlichen Regelungen empfohlen, die automatisch generierten Transaktionsprotokolle ausdrucken und diese von den am Legitimations- bzw. Freigabevorgang beteiligten Bediensteten unterzeichnen zu lassen.

Werden allerdings für die elektronische Signatur der Zahlungsverkehrsaufträge die von der Kreditwirtschaft empfohlenen sicheren Signaturerstellungseinheiten[45] (z. B. vom ZKA zugelassene Banken-Signaturkarten in Verbindung mit Lesegeräten der Sicherheitsklasse 3 bzw. Secoder) verwendet, bestehen in technischer Hinsicht (Ausprägung und Qualität der elektroni-

[44] Anforderungen an den Einsatz fortgeschrittener Signaturen im Haushalts-, Kassen- und Rechnungswesen der Bayerischen Kommunen

[45] Die oftmals als Speichermedium für die Schlüsseldatei verwendeten Wechselmedien (z. B. normale USB-Sticks, CD-R oder CD-RW) fallen nicht darunter.

schen Signatur) keine Unterschiede zur haushaltsrechtlich zugelassenen fortgeschrittenen Signatur. Unseres Erachtens kann in diesen Fällen auf den zusätzlichen Ausdruck und die Unterzeichnung des Transaktionsprotokolls verzichtet werden. Letzteres gilt ohnehin, wenn die Zahlungsverkehrsdaten mit qualifizierten Signaturen im Sinne von § 2 Nr. 3 SigG signiert werden. In beiden Fällen muss natürlich durch organisatorische Maßnahmen sichergestellt sein, dass die persönlichen Chipkarten nur von den Signaturschlüsselinhabern selbst verwendet werden.

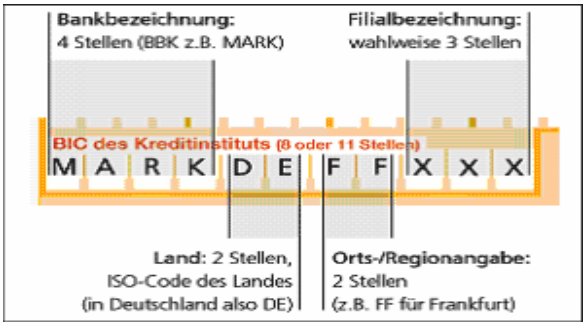
7 Begriffserläuterungen

– **BCS** (**B**anking **C**ommunication **S**tandard)

In den letzten 10 bis 15 Jahren etablierter Kommunikations-Standard des deutschen Kreditgewebes für Electronic-Banking, bei dem nach festen Regeln verschiedene Verfahren verknüpft werden, um eine sichere Übertragung zu gewährleisten

– **BIC (B**ank **I**dentifier **C**ode)

Standardisierte, internationale Bankleitzahl eines Kreditinstituts mit folgendem Aufbau:



(Quelle: Deutsche Bundesbank)

– **DFÜ** (**D**aten**f**ern**ü**bertragung)

Allgemeine Bezeichnung für die Datenübertragung zwischen Rechnersystemen. Beim Electronic-Banking steht der Begriff für den Datenaustausch zwischen den Kreditinstituten und ihren Kunden, um diesen die Abwicklung von Bankgeschäften im Wege der Datenfernübertragung mittels Filetransfer mit allen Kreditinstituten multibankfähig zu ermöglichen (vgl. DFÜ-Abkommen).

– **DTAUS** (Datenträgeraustausch-Format Inlandszahlungsverkehr)

Datenträgeraustausch-Format der deutschen Kreditwirtschaft für den Inlandszahlungsverkehr, das in Anlage 3 „Spezifikation der Datenformate“ des DFÜ-Abkommens näher beschrieben und spezifiziert ist

– **DTAZV** (Datenträgeraustausch-Format Auslandszahlungsverkehr)

Datenträgeraustausch-Format der deutschen Kreditwirtschaft für den Auslandszahlungsverkehr, das in Anlage 3 „Spezifikation der Datenformate“ des DFÜ-Abkommens näher beschrieben und spezifiziert ist

– **EBICS** (**E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard)

Standardisiertes Sicherungs- und Übertragungsverfahren, das für die multibankfähige und sichere Kommunikation über das Internet zwischen Kunde und Bank erforderlich ist

– **Electronic-Banking-Systeme**

Sammelbegriff für die elektronische Kommunikation der Banken mit ihren Kunden. Darunter werden im Rahmen dieses Beitrags Internet-Banking-Portale, Online-Banking bzw. Zahlungsverkehrsprogramme sowie die beleglose (elektronische) Übermittlung von Zahlungsverkehrsdaten verstanden.

– **FinTS** (**Fin**ancial **T**ransaction **S**ervices)

Offenes, standardisiertes Sicherungs- und Übertragungsverfahren, das eine sichere Übertragung von Aufträgen (sog. Geschäftsvorfällen) und Zahlungsverkehrsdaten zwischen dem Bankkunden und einem oder mehreren Kreditinstituten über eine einheitliche Schnittstelle gewährleisten soll. Ziel ist dabei die Gewährleistung von Multibankfähigkeit. FinTS ist die Weiterentwicklung des 1996 erstmals vom ZKA veröffentlichten Online-Banking Standards HBCI, der im so genannten Homebanking-Abkommen der deutschen Kreditwirtschaft näher geregelt und spezifiziert ist.

– **FTAM** (**F**ile **T**ransfer and **A**ccess **M**anagement)

Standardisiertes, auf dem OSI-Modell beruhendes Datenkommunikations-Protokoll für den Dateitransfer mit erweitertem Funktionsumfang

– **HBCI** (**H**ome**b**anking **C**omputer **I**nterface)

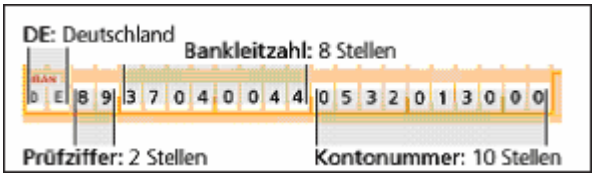
HBCI wurde im Auftrag der deutschen Kreditwirtschaft als internetfähiges Kommunikationsverfahren für die beim Kunden installierten Homebanking-Programme entwickelt und wird zwischenzeitlich als FinTS-Standard fortgeführt (vgl. FinTS).

– **HTTPS** (**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure)

Protokoll, das der sicheren Übertragung von Daten über (unsichere) Weitverkehrsnetze (z. B. das Internet) dient. Die Sicherheit wird erstens durch eine Authentifizierung zwischen dem Webserver und dem Internet-Browser und zweitens durch eine starke Verschlüsselung der Nutzdaten erreicht.

– **IBAN (I**nternational **B**ank **A**ccount **N**umber)

Standardisierte, internationale Bank-/Kontonummer für nationale und grenzüberschreitende Zahlungen mit folgendem Aufbau:



(Quelle: Deutsche Bundesbank)

– **Man in the Middle**

Bei einem Man-in-the-Middle-Angriff schleicht sich ein Dritter unbemerkt in eine Kommunikation zwischen zwei oder mehreren Partnern ein, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. (Quelle: BSI-Grundschutz-Kataloge)

– **Online-Banking**

Urspünglich für das BTX-Banking verwendeter Begriff; wird heute synonym für Internet-Banking-Portale oder Zahlungsverkehrsprogramme verwendet

– **Pharming**

Eine Fortentwicklung des klassischen Phishings. Pharming ist eine Fälschung der Zuordnung von Namen zu IP-Adressen (unter Windows z. B. durch Manipulation der „hosts“-Datei oder deren Suchpfad), um Anfragen auf gefälschte Webseiten umzuleiten. Der Nutzer landet so auf einem manipulierten Server eines Phishers, obwohl er im Browser, die richtige URL z. B. von Hand eingegeben hat. Pharming ist auch unter dem Begriff Domain-Spoofing bekannt.
(Quelle: BSI für Bürger)

– **Phishing**

Kunstwort, das sich aus „password“ und „fishing“ zusammensetzt. Es bezeichnet einen Trick, um mit Hilfe von gefälschten E-Mails an vertrauliche Daten zu gelangen. Eine Phishing-E-Mail gibt vor, von einem vertrauenswürdigen Absender (z. B. einer Bank) zu stammen. Der Empfänger wird stets gebeten, über einen Link oder ein Formular vertrauliche Daten wie z. B. die Kreditkartennummer, Kontodaten oder Passwörter einzugeben, die vom Absender dann genutzt werden, um den Empfänger finanziell zu schädigen. (Quelle: BSI für Bürger)

– **PIN** (**P**ersönliche **I**dentifikations-**N**ummer)

Ist vergleichbar mit einem Passwort; wird gemeinsam mit einer TAN für die Autorisierung von Bank-Transaktionen verwendet

– **SEPA** (**S**ingle **E**uro **P**ayments **A**rea)

SEPA steht für den einheitlichen Euro-Zahlungsverkehrsraum, in dem alle Zahlungen wie inländische Zahlungen behandelt werden. Seit dem Start von SEPA im Januar 2008 wird nicht mehr zwischen nationalen und grenzüberschreitenden Zahlungen unterschieden. SEPA dient der Verwirklichung eines einheitlichen Binnenmarktes im bargeldlosen Zahlungsverkehr.

– **SSL** (**S**ecure **S**ockets **L**ayer)

Zertifikatsbasierendes Verschlüsselungsprotokoll, das der sicheren Datenübertragung im Internet dient. Seit der Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht.
(Quelle: www.wikipedia.de)

– **SWIFT** (**S**ociety for **W**orldwide **I**nterbank **F**inancial **T**elecommunication)

Ist eine belgische Gesellschaft, die ein Telekommunikationsnetz (SWIFT-Netz) für den schnellen, sicheren, zuverlässigen und standardisierten Nachrichtenaustausch zwischen den Mitgliedern betreibt. SWIFT besteht derzeit aus mehr als 9.000 Banken, Sicherheitsinstitutionen und Firmenkunden in 209 Ländern.

– **TAN** (**T**rans**a**ktions**n**ummer)

Wird gemeinsam mit der PIN für die Autorisierung von Bank-Transaktionen (z. B. Überweisungen) verwendet. Jede TAN kann nur einmal verwendet werden. Die Bank sendet in der Regel dem Kunden eine Anzahl TANs auf dem Postweg zu. (Quelle: BSI für Bürger)

– **TCP/IP (T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol)

Netzwerk-Übertragungsprotokoll auf Schicht 3 (Network-Layer) und 4 (Transport-Layer) des OSI-Referenzmodells. TCP/IP ermöglicht den Datenaustausch über die Grenzen lokaler Netzwerke hinaus und eignet sich daher sehr gut für die Übertragung von Daten über das Internet oder vergleichbare Netze. (Quelle: www.wikipedia.de)

Eine nähere Beschreibung findet sich in Abschnitt 8 unseres Beitrags zum Thema „Firewallsysteme – Ein elementarer Teil der Sicherheit in der Informationstechnik (IT). Wozu werden sie benötigt, was können sie und wie werden sie eingesetzt?“ im Geschäftsbericht für das Jahr 2002, S. 33 ff.

– **TLS (T**ransport **L**ayer **S**ecurity**)**

Nachfolger des SSL-Verschlüsselungsprotokolls; dient der Verschlüsselung der Nutzdaten und ist ebenfalls zertifikatsbasierend (Quelle: www.wikipedia.de)

– **XML** (E**x**tensible **M**arkup **L**anguage)

Ist eine Computersprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdaten und dient der Beschreibung sowie dem Austausch von komplexen Datenstrukturen. XML wird unter anderem für den plattform- und implementationsunabhängigen Austausch von Daten zwischen Computersystemen eingesetzt, insbesondere über das Internet.

– **ZKA** (**Z**entraler **K**redit**a**usschuss)

Im Zentralen Kreditausschuss sind seit 1932 die fünf Spitzenverbände der deutschen Kreditwirtschaft (Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V., Bundesverband deutscher Banken e. V., Bundesverband Öffentlicher Banken Deutschlands e. V., Deutscher Sparkassen- und Giroverband e. V. und Verband deutscher Pfandbriefbanken e. V. – hervorgegangen aus dem Verband deutscher Hypothekenbanken e. V.) zusammengeschlossen. (Quelle: ZKA)

8 Quellen

8.1 Online-Quellen

(Stand: 25.01.2011)

Zentraler Kreditausschuss – Informationen zum Zahlungsverkehr und Electronic Banking
www.zka-online.de/zka/zahlungsverkehr/electronic-banking.html

Zentraler Kreditausschuss – Informationen zum FinTS-Standard und FinTS-Kompendium
www.hbci-zka.de

Zentraler Kreditausschuss – Informationen zu EBICS und EBICS-Kompendium
www.ebics.de

Bundesamt für Sicherheit in der Informationstechnik – IT-Grundschutz-Kataloge und BSI für den Bürger – So funktioniert Online-Banking
www.bsi.bund.de und www.bsi-fuer-buerger.de

Bankenverband – Fachinformationen zur Bank- und Informationstechnologie und diverse Broschüren
www.bankenverband.de/themen/fachinformationen/Bank- und Informationstechnologie

Bundesbank – Informationen zu SEPA
www.bundesbank.de/zahlungsverkehr/zahlungsverkehr_sepa.php

European Payments Council – Aktuelle Informationen zu SEPA (leider überwiegend nur in Englisch)
www.europeanpaymentscouncil.eu/index.cfm

Informatikzentrum der Sparkassen-Organisation GmbH – Informationen zum eBanking
www.siz.de/ebanking/standards/ebics.html

PPI Aktiengesellschaft Informationstechnologie
www.ppi.de/aktuelles/news/archiv/2008/september/23/artikel/ebics-kompendium-electronic-banking-internet-communication-standard/

Vorträge Prof. Dr. Georg Bitter „Neues Zahlungsverkehrsrecht“ am 30.06.2010 an der deutschen Richterakademie in Trier und am 30.08.2010 bei der Handelskammer Bremen
www.bankrecht.uni-mannheim.de/lehrstuhlinhaber/vortraege/index.html

Zahlungsverkehr-FAQ von Christian Bartsch und Stefan Krieg – Sehr informative (private) Website mit Informationen zu zahlreichen Zahlungsverkehrsfragen
www.zahlungsverkehrsfragen.de

Stadtsparkasse München – Informationen zum Electronic Banking für Firmenkunden
http://www.sskm.de/sskmwww/sskmwww_prod/sskmwww/firmenkunden/e_services/e_banking/index.jsp

Genossenschaftsbank Unterallgäu eG – Informationen zum Online-Banking und zu SEPA
www.genobank-unterallgaeu.de

Volksbank Freiburg eG – Informationen zum Online-Banking
www.volksbank-freiburg.de

Raiffeisenbank Aschaffenburg eG – Informationen zum Electronic Banking
www.raiba-aburg.de

Informationen zu Terminals, Karten und Zahlverfahren
www.terminaldirekt.de

Frankfurter Allgemeine Zeitung – „Onlinebanking – Höchste Sicherheit noch immer nicht Standard“
www.faz.net

Universität Tübingen, Lehrstuhl Technische Informatik, Bernd Borchert, „Trojanersichere Online Accounts“
www-ti.informatik.uni-tuebingen.de/~borchert/Troja/

PC-Welt – Ratgeber Online-Banking mTAN, HBCI und FinTS
www.pcwelt.de/ratgeber/mTAN-HBCI-und-FinTS-Ratgeber-Online-Banking-436788.html

PC-Welt – Ratgeber Sicherheit beim Online-Banking
www.pcwelt.de/news/Ratgeber-Sicherheit-beim-Online-Banking-285116.html

Deutsche Telekom AG T-Online – Online-Banking-Sicherheit im Überblick
computer.t-online.de/sicheres-online-banking-itan-chiptan-und-mtan-im-ueberblick/id_43312802/index

8.2 Literatur-Quellen

Wirtschaftslehre des Kreditwesens, Grill/Perczynski, Bildungsverlag EINS, 40. Auflage, Stand 01.05.2006, ISBN 3-441-00303-9

Electronic Banking, Stefan Werner, Bank-Verlag Medien GmbH, 1. Ausgabe, Stand 2009, ISBN 978-3-86556-209-8

Belegloser Zahlungsverkehr, Johannes Hergersberg, Deutscher Sparkassen Verlag GmbH, Stand 1998

FinTS V 4.0 Kompendium, Financial Transaction Service, Der Einstieg in die neue Welt des Online-Banking, Six Sigma EDV-Konzepte, Kurt Haubner, Stand 2004

EBICS-Kompendium V 3, Electronic Banking Internet Communication Standard, Michael Lembke, PPI Financial Systems GmbH, Stand 17.06.2009