

VÖB Online
M 514/02
vom 27. September 2002

Geldwäsche; Rechtsabteilung;
Vorstandssekretariat

M 493/02 vom 16.09.2002
M 469/02 vom 05.09.2002

Geldwäsche;
Kreditwesengesetz (KWG)

Bekämpfung der Geldwäsche
Automatisierter Abruf von Kontoinformationen / § 24 c KWG
Rundschreiben 17/2002 der BAFin
hier:

Sehr geehrte Damen und Herren,

mit den oben genannten Mitteilungen hatten wir Sie darüber informiert, dass die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) einen Entwurf der "Schnittstellenspezifikation BAFin – Kreditinstitute" als Anforderungskatalog für die technische und organisatorische Realisierung des Abrufverfahrens nach § 24c KWG vorgelegt hat. Gleichzeitig hatten wir Sie für den 2. Oktober 2002 zu einer Informationsveranstaltung über die materiellen und technischen Grundlagen des Abrufverfahrens eingeladen.

Mit dem als **Anlage** beigefügten Rundschreiben 17/2002 vom 26. September 2002 hat die BAFin die Schnittstellenspezifikation (Version 1.5) als **verbindliche Vorgabe** für das Abrufverfahren an die Kreditinstitute verteilt.

Aus dem Rundschreiben der BAFin sind folgende Punkte hervorzuheben:

- **Mitteilung an die BAFin bis zum 28. Oktober 2002**

Die Institute haben, sofern sie nicht einem Gemeinschaftsrechenzentrum angeschlossen sind, der BAFin bis zum 28. Oktober 2002 mitzuteilen, ob sie die für das Abrufverfahren vorzuhaltenden Daten selbst oder über einen

externen Dienstleister bereitzustellen beabsichtigen. Letzterenfalls ist der Dienstleister zu benennen. Diese Mitteilung ersetzt nicht die Anzeigepflichten nach § 25a Abs. 2 KWG.

Wie in der Einladung für die Informationsveranstaltung angegeben, ist geplant, die von der BAFin angesprochene Gemeinschaftslösung zur technischen Abwicklung des Kontenabrufverfahrens für interessierte VÖB-Mitgliedsinstitute über die VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen GmbH einzurichten. Institute, die sich dieser zentralen Abrufstelle anschließen wollen, können die entsprechende Mitteilung an VÖB-ZVD leiten und werden von dort an die BAFin gemeldet.

- **Arbeitsgruppe bei der BAFin**

Die technische Realisierungsphase der Abrufkomponente soll von einer noch zu bildenden Arbeitsgruppe, der auch Vertreter der kreditwirtschaftlichen Verbände angehören sollen, begleitet werden. Ziel dieser Arbeitsgruppe ist es, in der Praxis auftretende Fragen zur Umsetzung der Schnittstellenspezifikation in Zusammenarbeit mit der BAFin zu klären. Eine erste Sitzung dieser Arbeitsgruppe wird voraussichtlich Ende Oktober stattfinden. Diesbezüglich bitten wir Sie, uns über Fragen, die im Rahmen der technischen Realisierungsphase auftreten, zu informieren, da wir den VÖB in dieser AG vertreten werden.

- **Grundsätzliche Fragen zum Kontenabrufverfahren**

Über die Arbeitsgruppe hinaus sollen grundsätzliche Fragen zum Kontenabrufverfahren von den Instituten beim jeweiligen Verband eingereicht und vom Verband zusammengefasst an die BAFin weitergeleitet werden. Auch insoweit bitten wir Sie um Mitteilung etwaiger Problemfälle.

Wir weisen nochmals darauf hin, dass alle Institute das Abrufverfahren kraft Gesetzes zum **1. April 2003** einzurichten haben. Das Bundesministerium der Finanzen (BMF) wird von der in § 24c Abs. 7 KWG vorgesehenen Möglichkeit, Ausnahmen von der Verpflichtung zur Übermittlung im automatisierten Verfahren zuzulassen, voraussichtlich nur in sehr eng begrenztem Umfang Gebrauch machen. Insbesondere ist es sehr fraglich, ob eine generelle Ausnahme für bestimmte Institutsgruppen erreicht werden kann. Eine Ausnahmeregelung wird voraussichtlich allenfalls für einige wenige Kontoarten möglich sein. Diese Einschätzung beruht auf einem Gespräch, das am 26. September 2002 zwischen dem BMF und dem Zentralen Kreditausschuss stattgefunden hat. Das BMF wird sich hierzu in Kürze konkret äußern.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Bundesverband Öffentlicher Banken Deutschlands

Björn Christian Stein

Astrid Wagner

Anlage



Bundesanstalt für Finanzdienstleistungsaufsicht

POSTANSCHRIFT BAFin, Graurheindorfer Str. 108, 53117 Bonn

HAUSANSCHRIFT 53117 Bonn, Graurheindorfer Str. 108

REFERAT

BEARBEITET VON

TELEFON 0228 4108- (oder 4108-0)

FAX 0228 4108-1550

E-MAIL poststelle@bafin.de

INTERNET www.bafin.de

IVBB 01888 436-0

DATUM 26. September 2002

GESCHÄFTSZEICHEN **Z 12 - O 1918 - 30/02** (BEI ANTWORT BITTE ANGEBEN)

Rundschreiben 17/2002

An alle Kreditinstitute

in der Bundesrepublik Deutschland

Automatisierter Abruf von Kontoinformationen nach § 24c (neu) des Gesetzes über das Kreditwesen (KWG)

Anlage

Mit dem 4. Finanzmarktförderungsgesetz vom 21. Juni 2002 (BGBl. 2010 ff.) ist in das Gesetz über das Kreditwesen (KWG) die Regelung zum automatisierten Abruf von Kontoinformationen (§ 24c) neu aufgenommen worden. Bis zum Inkrafttreten des § 24c KWG am 1. April 2003 müssen die technischen Voraussetzungen für den Abruf von Kontoinformationen nach § 24c KWG durch die BAFin auf Seiten der Kreditinstitute und der BAFin realisiert werden.

Als Anlage übersende ich Ihnen das Schnittstellenkonzept für den Datenverkehr zwischen der BAFin und den Kreditinstituten bzw. den von diesen mit der Bereitstellung der Daten nach § 24c KWG beauftragten Rechenzentren. Die technische Realisierungsphase der Abrufkomponente soll von einer noch zu bildenden Arbeitsgruppe begleitet werden. Dieser Arbeitsgruppe sollen Vertreter von im Zentralen Kreditausschuss zusammengeschlossenen Verbänden, Vertreter verschiedener Rechenzentren und Vertreter der BAFin angehören.

Dienstszitz: 53117 Bonn, Graurheindorfer Straße 108; 53003 Bonn; Postfach 13 08
60439 Frankfurt am Main, Lurgiallee 12; 60391 Frankfurt am Main; Postfach 50 01 54

Ab Freitag, den 31.05.2002, sind die Dienstszitze Bonn und Frankfurt/M. der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin), unter folgenden Telefonnummern zu erreichen: 0228/4108-0 IVBB: 01888/436-0, FAX Bonn: 0228/4108-1550, FAX Frankfurt/M.: 0228/4108-123

Grundsätzliche Fragen zu dem Kontenabrufverfahren bitte ich Ihrem jeweiligen Regional- oder Spitzenverband einzureichen, damit dieser die Anfragen zusammengefasst an mich weiterleiten kann. Meine Antwort werde ich Ihnen auf demselben Wege zukommen lassen. In diesem Zusammenhang ist anzumerken, dass nach meinem Kenntnisstand in den einzelnen Verbänden Gemeinschaftslösungen zur technischen Abwicklung des Kontenabrufverfahrens angedacht sind. Kreditinstitute, die keinem Verband angeschlossen sind, richten bitte alle Anfragen im Rahmen des § 24c KWG direkt an die BAFin.

Ferner möchte ich Sie bitten, sofern Sie nicht einem Gemeinschaftsrechenzentrum angeschlossen sind, mir bis zum 28. Oktober 2002 mitzuteilen, ob Sie die nach § 24c KWG vorzuhaltenden Daten selbst oder über einen von Ihnen zu beauftragenden externen Dienstleister bereitzustellen beabsichtigen. Sollen die Daten von einem externen Dienstleister abgerufen werden, bitte ich, mir diesen Dienstleister zu benennen. Diese informatorische Mitteilung im Rahmen der Implementierung des Kontoabrufverfahrens ersetzt nicht die Anzeigepflichten gemäß § 25 a Abs. 2 KWG.

Für eventuelle Rückfragen steht Ihnen Herr RD Thomas Caspari (Tel. 02 28/41 08 - 12 80) zur Verfügung.

Im Auftrag

T h. C a s p a r i

Dieses Schreiben wurde elektronisch übersandt und enthält daher keine Unterschrift.

Verfahren zum automatisierten Abruf von Kontoinformationen

**Bundesanstalt für
Finanzdienstleistungsaufsicht
(BAFin)**

**Schnittstellenspezifikation
BAFin - Kreditinstitute**

Version 1.5

0. Rechtliche und organisatorische Angaben

Copyright © 2002 by BAFin.

Dieses Dokument dient zur Information der am Verfahren zum Auskunftersuchen gemäß § 24c KWG Beteiligten. Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung - gleich in welcher Form, ganz oder teilweise - sind nur mit vorheriger schriftlicher Zustimmung der Bundesanstalt für Finanzdienstleistungsaufsicht zulässig.

Dieses Dokument enthält neben Erläuterungen, Bewertungen und eigenen Erhebungen Beschreibungen von Herstellerprodukten, Schnittstellen und Konzepten, die auf entsprechenden Veröffentlichungen der jeweiligen Hersteller beruhen. Sofern in dem Dokument interne Informationen von Herstellern offen gelegt wurden, sind diese gekennzeichnet und unterliegen damit der besonderen Geheimhaltung.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenzeichen usw. in diesem Dokument berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen. Alle Marken und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Zeichenhalter.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

0.1 Inhaltsverzeichnis

1	Einleitung.....	6
1.1	Zielgruppe(n), Voraussetzungen.....	6
1.2	Quelle der Informationen.....	6
1.3	Bezugsdokumente.....	7
1.4	Glossar.....	8
1.5	Notation.....	9
2	Einführung.....	10
2.1	Rechtliche Grundlage.....	10
2.2	Gegenstand des Auskunftersuchens.....	10
2.3	Ablauf des Auskunftersuchens.....	10
2.4	Technische Struktur.....	11
2.5	Basisanforderungen an das Auskunftsverfahren.....	14
2.5.1	Sicherheitsniveau.....	14
2.5.2	Abfragelogik.....	15
2.5.3	Mengengerüst, Performanz und Verfügbarkeit.....	15
2.5.4	Mandantenfähige Abfragekomponenten.....	15
3	Datenübertragung zwischen BAFin und Verpflichteten (normativ).....	16
3.1	Netzverbindung zwischen BAFin und Verpflichteten.....	16
3.1.1	Zugang über Internet.....	16
3.1.2	Fallback-Zugang über ISDN Dial-In.....	17
3.2	Router Abfrage-Zugang.....	17
3.3	Firewall / VPN-Gateway Abfrage-Zugang.....	18
3.3.1	Firewall-Funktionalität.....	18
3.3.2	VPN-Funktionalität.....	18
3.4	Abfragekomponente.....	19
3.5	SSH-Daemon.....	20
4	Technische Abläufe (normativ).....	22
4.1	Abfrageverarbeitung.....	22
4.1.1	Empfang von Abfragen.....	22
4.1.2	Prüfung der Abfragekonsistenz.....	22
4.1.3	Versand der <i>Abfrage-Bestätigungs-Datei</i>	23
4.1.4	Selektion der gesuchten Kontoinformationen.....	24
4.1.5	Bereitstellung und Versand der Abfrage-Ergebnisse.....	26
4.1.6	Allgemeine Anforderungen an die Bearbeitung von Abfragen.....	27
4.2	Import der Kontoinformationen.....	27
4.3	Verwaltung der Kontoinformationen.....	28
4.3.1	Löschung historischer Kontoinformationen.....	28
4.3.2	Wechsel des DataCrypt-Schlüssels.....	28

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

5	Daten-Beschreibung (normativ).....	29
5.1	<i>Dateninhalte und –beziehungen</i>	29
5.1.1	Abzufragende Daten bei den Verpflichteten.....	29
5.1.2	Verwaltungsdaten in den Abfragekomponenten der Verpflichteten.....	31
5.1.3	Verwaltungsdaten für die Abfrage bei den Verpflichteten.....	32
5.1.4	Steuerungsdaten für die Abfrage bei den Verpflichteten (<i>Abfrage-Steuerungsdaten</i>)	33
5.1.5	Ergebnisdaten für Abfragen.....	33
5.2	<i>Technische Definition der Daten</i>	34
5.2.1	Technische Definition der Datenobjekte.....	34
5.2.2	Klassifikation gleichartiger Datenfelder	39
5.2.3	Formate der Datenfelder	41
5.3	<i>Verwendung der Daten für die Abfrage-Bearbeitung</i>	41
5.3.1	Input-Daten.....	41
5.3.2	Systemdaten.....	41
5.3.3	Output-Daten.....	42
6	Prozess-Beschreibung.....	43
6.1	<i>Rollen</i>	43
6.1.1	BAFin.....	43
6.1.2	Betreiber.....	43
6.1.3	Administrator Abfragekomponente des Verpflichteten.....	43
6.1.4	Technisch Verantwortlicher des Verpflichteten.....	44
6.1.5	b) Verfahrensverantwortlicher des Verpflichteten.....	44
6.1.6	Datenschutzbeauftragter des Verpflichteten.....	44
6.2	<i>Organisatorische Abläufe</i>	44
6.2.1	Einrichtung der System-Komponenten.....	44
6.2.2	Betrieb.....	44
6.2.3	Störungsbehebung.....	45
6.2.4	Wartung.....	45
7	Nicht funktionale Anforderungen (normativ).....	47
7.1	<i>Mengengerüst</i>	47
7.2	<i>Performanz</i>	47
7.3	<i>Datenaktualität</i>	47
7.4	<i>Verfügbarkeit</i>	47
7.5	<i>Sicherheitsanforderungen</i>	49
7.5.1	Zugriffsschutz.....	49
7.5.2	Datensicherheit.....	49
7.5.3	Datenkonsistenz.....	49
7.6	<i>Rechtliche Restriktionen</i>	49
7.7	<i>Systemarchitektur</i>	49
7.8	<i>Netzwerkarchitektur</i>	50
7.9	<i>Systemtests</i>	50
7.9.1	Integrationstest durch die BAFin.....	50
7.9.2	Tests im laufenden Betrieb durch die BAFin.....	50
7.9.3	Weitere Tests	50

Verfahren zum automatisierten Abruf von Kontoinformationen
Schnittstellenspezifikation BAFin - Kreditinstitute

8	Anhang.....	51
8.1	Document-Type-Definition (DTD).....	51
8.2	Aufrufschnittstelle des Moduls DataCrypt.....	53

0.2 Abbildungsverzeichnis

Abbildung 1:	Verlauf des Auskunftersuchens	11
Abbildung 2:	Architektur des Gesamtsystems	11
Abbildung 3:	Wechselwirkung der Abfragekomponente mit Fremdsystemen.	12
Abbildung 4:	Gliederung der Systeme beim Verpflichteten	12

0.3 Tabellenverzeichnis

Tabelle 1:	Selektion der abzufragenden Daten durch Anhaltsdaten.....	26
Tabelle 2:	XML-Document-Type-Definition (DTD)	53

1 Einleitung

Das Auskunftsverfahren gemäß § 24c KWG (im folgenden kurz: Auskunftsverfahren) realisiert ein Verfahren, mit dem die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) bei Kreditinstituten (im folgenden: Verpflichtete) Stammdaten der Konten und Depots sowie der zugehörigen Kunden auf elektronischem Weg abrufen kann.

Das vorliegende Dokument dient als Anforderungskatalog für die technische und organisatorische Realisierung des Auskunftsverfahrens gemäß § 24c KWG bei den Verpflichteten. Neben den technischen und organisatorischen Randbedingungen, die aus Art der Realisierung des Verfahrens bei der BAFin resultieren, werden insbesondere die Aspekte Datenschutz, IT-Sicherheit und Wirtschaftlichkeit berücksichtigt.

Das vorliegende Dokument stellt keine vollständige Spezifikation aller zur Realisierung des Verfahrens auf der Seite der Verpflichteten erforderlichen Maßnahmen dar. Vielmehr wurden die Anforderungen auf die notwendigen Bereiche beschränkt, um den Verpflichteten weitest gehende Flexibilität bei der Umsetzung zu gewähren. Es ist zulässig, dass mehrere Verpflichtete das Auskunftsverfahren mittels einer gemeinsamen, mandantenfähigen Abfragekomponente implementieren.

Das Dokument ist gegliedert in besonders gekennzeichnete, normative Abschnitte, welche die Anforderungen spezifizieren und informative Abschnitte, die zur Erläuterung dienen und Beispiele enthalten. In Kapitel 2 wird zunächst das Auskunftsverfahren und die Anforderungen an die Systeme der Verpflichteten erläutert. Kapitel 3 spezifiziert die Datenübertragung zwischen der BAFin und den Verpflichteten. Kapitel 4 enthält die Vorgaben für die vom Verpflichteten zu realisierenden technischen Abläufe. In Kapitel 5 werden die für den Verpflichteten relevanten Daten definiert. Kapitel 6 beschreibt die organisatorischen Prozesse bzw. Anforderungen soweit sie von der BAFin vorgegeben werden. Kapitel 7 enthält eine Zusammenstellung der nicht-funktionalen Anforderungen, wie z.B. Performanz, Verfügbarkeit und Zugriffsschutz. Der Anhang enthält konkrete Beispiele für technische Abläufe und Daten.

Die zur Implementierung direkt erforderlichen Teile des Dokuments (XML-DTD, Testdaten, Modul **DataCrypt**, etc.) sind in elektronischer Form bei der BAFin erhältlich.

1.1 Zielgruppe(n), Voraussetzungen

Zielgruppe sind die Personen, die mit der Implementierung der Abfragekomponente bei den Verpflichteten betraut sind. Es werden grundlegende Kenntnisse in XML, Netzwerktechnik (TCP/IP) und Verfahren der IT-Sicherheit (Firewall, Virtual-Private-Networks, Secure-Shell/Secure-Copy) vorausgesetzt.

1.2 Quelle der Informationen

Dieses Dokument basiert auf dem § 24c KWG [02.KWG§24c] und den für die Verpflichteten relevanten Informationen aus den Konzepten und Spezifikationen der Systeme, die bei der Bundesanstalt für Finanzdienstleistungsaufsicht das Auskunftsverfahren gemäß § 24c KWG realisieren. Darüber hinaus wurden Maßnahmen zur Sicherstellung von Datenschutz und IT-Sicherheit gemäß den Vorgaben des zuständigen Datenschutzbeauftragten und des Bundesamts für die Sicherheit in der Informationstechnik (BSI) integriert.

Verfahren zum automatisierten Abruf von Kontoinformationen

Schnittstellenspezifikation BAFin - Kreditinstitute

1.3 Bezugsdokumente

- [02.KWG§24c] § 24c automatisierter Abruf von Kontoinformationen (Fundstelle Bundesgesetzblatt Teil I Nr. 39; 2002; S. 2053f).
- [GWG§8-Abs.1] § 8 Abs. 1 Geldwäschegesetz.
- [02.GHB] IT-Grundschutzhandbuch; <http://www.bsi.de/gshb/deutsch/menue.htm>; BSI; Mai 2002.
- [02.SSH] Secure-Shell (SSH); <http://www.ietf.org/html.charters/secsh-charter.html>; IETF; 24.06.2002.
- [02.IPSec] IP Security Protocol (ipsec); <http://www.ietf.org/html.charters/ipsec-charter.html>; IETF; 16-05-2002.
RFC 2406: IP Encapsulating Security Payload; <http://www.ietf.org/rfc/rfc2406.txt>; IETF.
RFC 2402: IP Authentication Header; <http://www.ietf.org/rfc/rfc2402.txt>; IETF.
RFC 2408: Interpretation for ISAKMP Header; <http://www.ietf.org/rfc/rfc2408.txt>; IETF.
RFC 2409: The Internet Key Exchange (IKE); <http://www.ietf.org/rfc/rfc2409.txt>; IETF.
- [X509v3] X509v3;
<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.509>; International Telecommunication Union (ITU).
- [02.BSI.SINA] BSI-Projekt: Sichere Inter-Netzwerk Architektur (SINA); <http://www.bsi.bund.de/fachthem/sina/index.htm>; BSI; 2002

Verfahren zum automatisierten Abruf von Kontoinformationen
Schnittstellenspezifikation BAFin - Kreditinstitute

1.4 Glossar

4-Augenprinzip	Aktionen dürfen nur durch Kooperation von zwei verschiedenen Personen durchgeführt werden. Das 4-Augenprinzip kann technisch oder durch organisatorische Regelungen durchgesetzt werden.
Abfrage	Abruf von Kontoinformationen gemäß § 24c KWG durch die BAFin bei einem Verpflichteten. Die Abfragen an die Verpflichteten werden aus den Daten der - > Anfragen erstellt. Die Abfragekomponenten der Verpflichteten ermitteln das Abfrageergebnis und senden diese als Antwortdatei an die BAFin zurück.
Abfragekomponente	Komponente bei den Verpflichteten, welche die Abrufe entgegen nimmt, das Ergebnis ermittelt und als Antwortdatei an die BAFin sendet. Die Abfragekomponente enthält eine Kopie der für das Auskunftersuchen gemäß § 24c KWG relevanten Daten des Verpflichteten.
Abfrage-User	Technisches Benutzerkonto für die BAFin zum Abruf von Kontoinformationen per Secure-Copy.
Abfragevertraulichkeit	Abrufe dürfen den Verpflichteten gemäß § 24c KWG nicht zur Kenntnis gelangen.
Anhaltsdaten	Daten die vom Bedarfsträger zur Auswahl der für ihn relevanten Kontodatensätze im Rahmen der Anfrage angegeben werden (z.B. Kontonummer oder Name).
Auskunftersuchen	Auskunftersuchen gemäß § 24c KWG.
Auskunftssystem	Alle technischen Komponenten der BAFin, der Verpflichteten und der Bedarfsträger, die dediziert für das Auskunftersuchen gemäß § 24c KWG eingesetzt werden.
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKNr	Eindeutiges Identifizierungsmerkmal für alle Verpflichteten, das von der BAFin vergeben wird.
Base64-Transformation	Eindeutig umkehrbare Transformation zur Darstellung von Byte-Feldern ausschließlich mit druckbaren Zeichen.
Bedarfsträger	Bedarfsträger ist die BAFin, die gem. § 24c Abs. 2 KWG zum Abruf berechtigt ist. Mittelbare Bedarfsträger sind die in § 24c Abs. 3 Nr. 1-3 KWG genannten Behörden und Gerichte, für die die BAFin auf deren Ersuchen hin tätig ist.
Bündelabfrage	Mehrere in einer Abfrage-Datei zusammengefasste Abfragen. Diese werden in den Abfragekomponenten als separate Abfragen verarbeitet.
CLIP	Calling-Line-Identification-Presentation
DataCrypt	Software-Komponente zur Konvertierung und Verschlüsselung von Daten für die -> datenbanklogische Blackbox
Datenbanklogische Blackbox	Verfahren zur Sicherstellung der -> Abfragevertraulichkeit mittels Verschlüsselung von Kontoinformationen und Abfragen-Daten.
DMZ	Zwischennetz („demilitarisierte Zone“) eines Firewall-Systems
DSB	Datenschutzbeauftragter
DTD	Formale Spezifikation von XML-Datenformaten (Document-Type-Definition)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

Fallback-Dial-In	Einwahlzugang über ISDN bei der BAFin und den Verpflichteten, falls über das Internet keine Verbindung möglich.
Konto	Konto wird als Konto im Sinne des § 154 Abs. 2 AO verstanden. Deshalb fallen grundsätzlich auch Darlehens- und Kreditkonten unter den Begriff des Kontos.
Kontodatensatz	Datensatz, der die gemäß § 24c KWG vom Verpflichteten vorzuhaltenden Daten für ein Konto für einen Zeitpunkt enthält. Bei Kontoänderungen können zu einem Konto mehrere Kontodatensätze existieren, die sich bzgl. des Gültigkeitszeitraums unterscheiden.
KWG	Kreditwesengesetz
LAN-Interface	Netzwerkschnittstelle
NAT	Network-Address-Translation
TGZ-Archiv	mittels tar / gzip gepackte und komprimierte Dateien (Dateierweiterung „.tar.gz“ oder „.tgz“)
Verpflichteter	Verpflichteter im Rahmen des § 24c KWG (z.B. Banken, Kreditinstitute, Fondsgesellschaften)
VPN	Virtual-Private-Network
XML	Extensible Markup-Language
Zugangsnetz BAFin	Zwischennetz vom internen LAN-Interface des VPN-Gateways BAFin-Zugang zum externen LAN-Interface der Empfangskomponente.
Zugangsnetz Verpflichteter	Zwischennetz vom internen Interface des VPN-Gateways Abfrage-Zugang zum externen Interface der -> Abfragekomponente.

1.5 Notation

Besonders definierte Begriffe werden wie folgt dargestellt: **Begriff**.

Eindeutige Bezeichnungen (Identifikatoren) für Dateninhalte und -felder werden wie folgt dargestellt: *Datenfeldname*.

2 Einführung

2.1 Rechtliche Grundlage

Die rechtliche Grundlage für das Auskunftersuchen ist § 24c KWG [02.KWG§24c], der im Rahmen des 4. Finanzmarktförderungsgesetzes am 26.06.2002 im Bundesgesetzblatt veröffentlicht wurde. Eine Umsetzung des Verfahrens (d.h. Aufnahme des Betriebs) ist zum 01.04.2003 gefordert.

2.2 Gegenstand des Auskunftersuchens

Die Verpflichteten müssen gemäß § 24c KWG folgende Kontoinformationen für den selektiven Abruf durch die BAFin vorhalten:

- Verwaltungsdaten des Kontos/Depots: Identifikation des Kontos/Depots (z.B. Kontonummer), Tag der Einrichtung, Tag der Auflösung
- Identifikation von Kontoinhabern (ggf. mehrere): Name, Geburtsdatum
- Identifikation von Verfügungsberechtigten (ggf. mehrere): Name, Geburtsdatum
- Identifikation von abweichend wirtschaftlich Berechtigten (ggf. mehrere): Name, Anschrift

Es sind seitens der Verpflichteten nicht nur die jeweils aktuellen Daten, sondern auch historische Daten bis zu drei Jahre vorzuhalten. Änderungen der Kontoinformationen sind täglich für den Abruf bereitzustellen.

2.3 Ablauf des Auskunftersuchens

Sofern die BAFin nicht im eigenen aufsichtlichen Interesse, sondern auf Ersuchen eines mittelbaren Bedarfsträgers tätig ist, kann das Verfahren in folgende Schritte gegliedert werden:

- Die BAFin prüft, ob der Ersuchende für das Auskunftersuchen autorisiert ist. Ist dies der Fall, erfasst die BAFin die Anfragedaten und protokolliert die Anfrage.
- Die BAFin leitet die Anfrage des mittelbaren Bedarfsträgers als Abfrage an alle Verpflichteten weiter.
- Die Verpflichteten stellen jeweils diejenigen Kontodatensätze als Abfrage-Ergebnis zusammen, welche die in der Abfrage angegebenen Kriterien erfüllen und senden dieses Abfrage-Ergebnis an die BAFin zurück.
- Die BAFin sammelt die Abfrage-Ergebnisse aller Verpflichteter.
- Die BAFin protokolliert die Abfrage-Ergebnisse, stellt das Anfrage-Ergebnis zusammen und leitet dieses an den Ersuchenden weiter. Damit ist ein Auskunftersuchen abgeschlossen.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

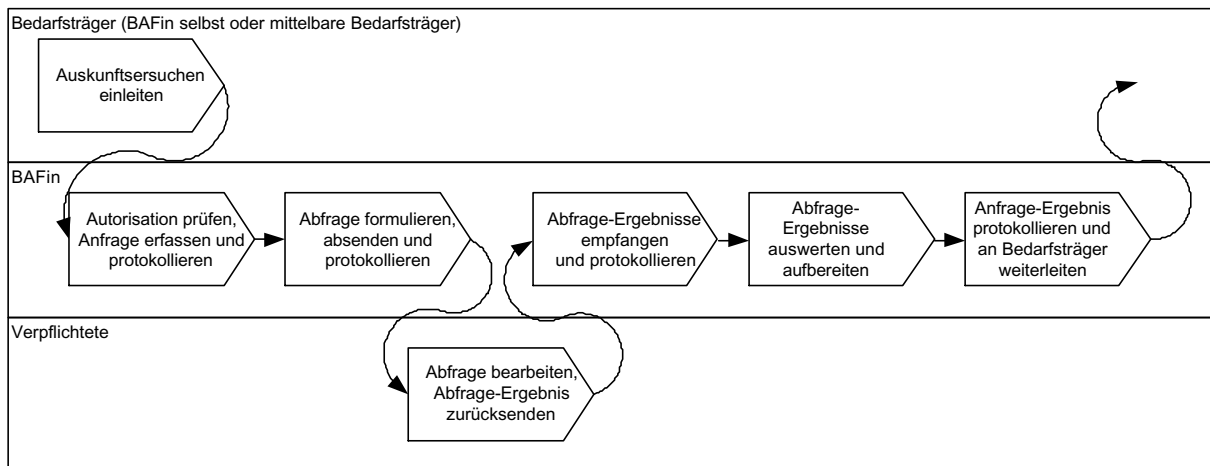


Abbildung 1: Verlauf des Auskunftsersuchens

2.4 Technische Struktur

Abbildung 2 gibt einen Überblick über die wesentlichen am Auskunftsverfahren beteiligten Systemkomponenten aus der Sicht des Verpflichteten.

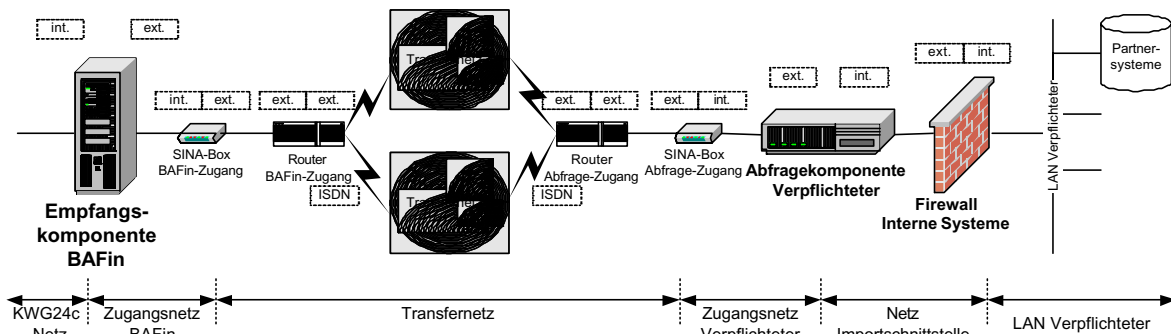


Abbildung 2: Architektur des Gesamtsystems

Abbildung 3 stellt die Wechselwirkung der Abfragekomponente mit Fremdsystemen dar. Fremdsysteme sind eine oder mehrere Stellen der BAFin sowie die Kundendatenbanken des jeweiligen Verpflichteten.

Als Medium für die verschlüsselte Übermittlung von Abfragen und Abfrage-Ergebnissen wird ein TCP/IP-Netz mit Virtual-Private-Network (VPN) verwendet. Der Zugang zu den Systemen der BAFin bzw. der Verpflichteten ist sowohl über Internet als auch über eine Einwahl möglich.

Zwischen der BAFin und den Verpflichteten werden die Daten in Form von XML-Dateien (*Abfrage-Datei*, *Antwort-Datei*) ausgetauscht. Das Verfahren zur Bereitstellung der Kontoinformationen für die Abfragekomponente kann im wesentlichen vom Verpflichteten festgelegt werden. Es sind lediglich bestimmte Anforderungen zur Realisierung der Abfrage-logik zu erfüllen.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

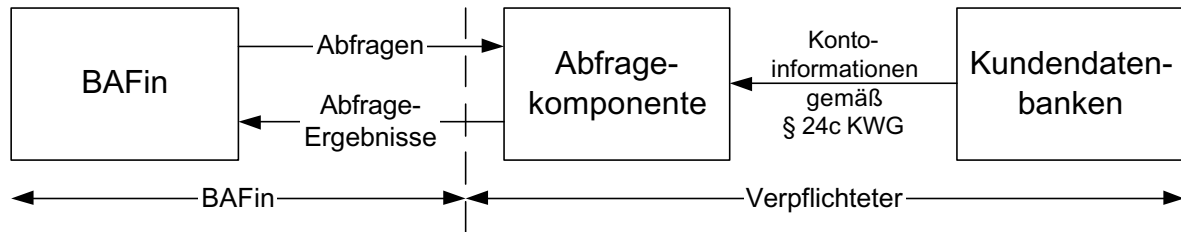


Abbildung 3: Wechselwirkung der Abfragekomponente mit Fremdsystemen.

Das vorliegende Dokument spezifiziert die Schnittstelle zwischen der Abfragekomponente des jeweiligen Verpflichteten und den Systemen der BAFin. Darüber hinaus werden soweit erforderlich Anforderungen an die Schnittstelle zwischen der Abfragekomponente und den Kundendatenbanken des Verpflichteten definiert.

Die im folgenden angegebene Gliederung der Systeme beim Verpflichteten (Abbildung 4) dient in erster Linie der strukturierten Beschreibung der Anforderungen und ist nicht als zwingende Vorgabe oder vollständige Beschreibung für die Realisierung gedacht. So ist es durchaus zulässig, Router, Firewall-System und VPN-Gateway in einer Komponente zu kombinieren.

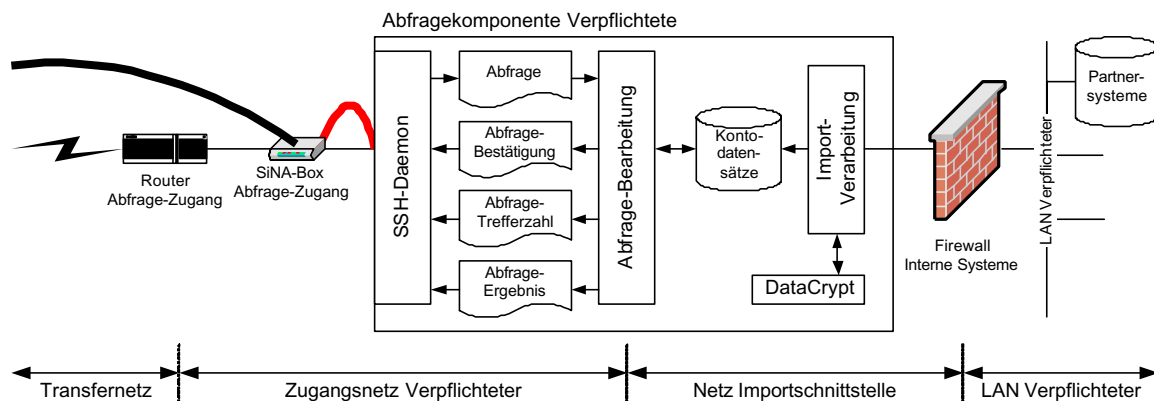


Abbildung 4: Gliederung der Systeme beim Verpflichteten

Erläuterungen zu den Abbildungen:

Transfernetz: Netz, über das der Transfer von *Abfrage-Dateien*, *Abfrage-Bestätigungs-Dateien* und *Abfrage-Ergebnis-Dateien* erfolgt. Dies kann entweder das Internet oder ein Transfernetz über ISDN-Einwahl sein.

Router Abfrage-Zugang: Router mit ISDN-Ein-/Auswahlfunktionalität über PPP/CHAP zur Verbindung von **Transfernetz-1** und **Transfernetz-2** mit dem **VPN-Gateway Abfrage-Zugang**.

Zugangsnetz Verpflichteter: Zwischennetz vom internen LAN-Interface (Netzwerkschnittstelle) des **VPN-Gateways Abfrage-Zugang** zum externen LAN-Interface der **Abfragekomponente**.

Firewall / VPN-Gateway Abfrage-Zugang: Netzwerkkomponente zur Beschränkung des Zugriffs auf die erforderlichen Protokolle (IPSec, SSH) und zur Realisierung eines VPN-Gateways zur Terminierung der IPSec-Verbindung mit den Systemen der BAFin. Die Verwendung eines VPNs trägt dem hohen Schutzbedarf beim Datentransfer über das Internet und externe ISDN-Verbindungen Rechnung.

Abfragekomponente: Dediziertes Server-System zur Speicherung aller gespiegelten Kontoinformationen gemäß § 24c KWG und zur Bearbeitung der Abfragen. Die Auslegung der Hard- und Software-Konfiguration der **Abfragekomponente** liegt weitgehend in der Verantwortung des

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

Verpflichteten.

SSH-Daemon: Dienst für den gesicherten Transfer von Dateien zwischen den Systemen der BAFin und der **Abfragekomponente** via Secure-Copy (SCP).

Abfrage-Datei: Datei im XML-Format zur Spezifikation einer Abfrage.

Abfrage-Bestätigungs-Datei: Datei im XML-Format zur Bestätigung, dass eine Abfrage korrekt von der **Abfrage-Bearbeitung** empfangen wurde und bearbeitet wird.

Abfrage-Trefferzahl-Datei: Datei im XML-Format zur Übermittlung der Anzahl der zu einer Abfrage gefundenen Kontodatensätze.

Abfrage-Ergebnis-Datei: Datei im XML-Format, welche die Ergebnisse einer Abfrage enthält.

Abfrage-Bearbeitung: Softwarekomponente, welche die *Abfrage-Dateien* auswertet, *Abfrage-Bestätigungs-Dateien* versendet, Abfragen gemäß der **Abfragelogik** (siehe Abschnitt 1.1.1) an die Datenbank mit den *Kontodatensätzen* stellt und die *Abfrage-Ergebnis-Dateien* aus dem Ergebnis der Abfrage erstellt und versendet.

Router BAFin-Zugang: Router mit ISDN-Ein-/Auswahlfunktionalität über PPP/CHAP zur Verbindung von **Transfernetz-1** und **Transfernetz-2** mit der **SINA-Box BAFin-Zugang**.

Zugangsnetz BAFin: Zwischennetz vom internen LAN-Interface der **SINA-Box BAFin-Zugang** zum externen LAN-Interface der **Empfangskomponente**.

SINA-Box BAFin-Zugang: Netzwerkkomponente zur Beschränkung des Zugriffs auf die erforderlichen Protokolle (IPSec, SSH) und zur Realisierung eines VPN-Gateways zur Terminierung der IPSec-Verbindung mit den Systemen der Verpflichteten.

KWG24c-Netz: Netz, in dem sich die interne Netzwerkschnittstelle der **Empfangskomponente** zu den Komponenten der Weiterverarbeitung der Abfrage-Ergebnisse befindet.

Empfangskomponente: Vereinfachte Darstellung der Systeme der BAFin für den Empfang und die Auswertung der Abfrage-Ergebnisse.

Kontodatensätze: Datenbank mit Datensätzen, welche die gemäß § 24c KWG abrufbaren Informationen über alle Konten des Verpflichteten als Kopie der Originaldaten in den **Partnersystemen** enthält.

Partnersysteme: Datenbanken des Verpflichteten mit den Originaldaten der gemäß § 24c KWG abrufbaren Informationen.

LAN Verpflichteter: Netzwerk des Verpflichteten, über das die *Kontodatensätze* in die **Abfragekomponente** importiert werden können.

Firewall Interne Systeme: Allgemeine Netzwerkkomponente zur Abschottung der internen Systeme des Verpflichteten gegen die **Abfragekomponente**. Die Auslegung der **Firewall Interne Systeme** liegt alleine in der Verantwortung des Verpflichteten.

Netz Importschnittstelle: Netz, in dem sich die Netzwerkschnittstelle der **Abfragekomponente** zum Import der *Kontodatensätze* sowie die entsprechende Schnittstelle der **Firewall Interne Systeme** befindet.

Import-Verarbeitung: Softwarekomponente, welche die zu importierenden *Kontodatensätze* geeignet für die Abfragelogik und die Datenbank der **Abfragekomponente** aufbereitet und über **DataCrypt** verschlüsselt.

DataCrypt: Softwarekomponente, welche zu importierende *Kontodatensätze* in XML-Dateien gemäß einem von der BAFin vorgegebenen Verfahren verschlüsselt und von der BAFin zur Verfügung gestellt wird. **DataCrypt** dient zur Realisierung der **Abfragevertraulichkeit** für Verpflichtete mittels **datenbanklogischer Blackbox** (siehe Abschnitt 2.5.1).

2.5 Basisanforderungen an das Auskunftsverfahren

2.5.1 Sicherheitsniveau

Im allgemeinen wird für alle am Auskunftsverfahren beteiligten Systeme als Sicherheitsniveau mindestens eine Umsetzung des IT-Grundschutzhandbuches [02.GHB] gefordert. Für bestimmte Systemkomponenten und Funktionalitäten müssen stärkere Maßnahmen eingesetzt werden. Dies betrifft im Einzelnen:

- **Sicherer Datentransfer:** Da die Übertragung der Abfragen und der Abfrage-Ergebnisse prinzipiell über das Internet erfolgen darf, werden besondere Maßnahmen zur Sicherstellung von Vertraulichkeit und Authentizität der Daten getroffen (siehe auch § 24c KWG Absatz 6 Satz 1). Als wesentliche Maßnahme wird ein Virtual-Private-Network (VPN) auf der Basis des IPsec-Standards mit zertifikatsbasierter Authentifizierung eingesetzt. Darüber hinaus findet eine Ende-zu-Ende-Absicherung zwischen den Systemen der BAFin und der Abfragekomponente durch den Dateitransfer mittels Secure-Copy (scp) statt.
- **Zugangsschutz für die Systeme der Verpflichteten:** Als Zugangsschutz für die IT-Systeme des Verpflichteten wird für den Netzzugang eine dedizierte Firewall-Funktionalität vorgeschrieben. Die Abfragekomponente ist ebenfalls gegen unberechtigten Zugang und Zugriff zu schützen. Alle weiteren Maßnahmen für den Zugangsschutz (z.B. zu den internen IT-Systemen) liegen in der Verantwortung des Verpflichteten.
- **Abfragevertraulichkeit:** Gemäß § 24c KWG Absatz 1 Satz 4 dürfen Abrufe dem Verpflichteten nicht zur Kenntnis gelangen. Als technische Maßnahme wird für die Abfragekomponente eine **datenbanklogische Blackbox** spezifiziert: Sowohl die Inhalte der Kontoinformationen als auch die Inhalte der Abfragen werden verschlüsselt übertragen. Die Abfrage innerhalb der Datenbank der Abfragekomponente erfolgt ebenfalls an Hand der verschlüsselten Daten, so dass in der Abfragekomponente zu keinem Zeitpunkt während des Abrufs Abfragedaten oder Kontoinformationen im Klartext vorliegen. Zur Realisierung der **datenbanklogische Blackbox** stellt die BAFin den Verpflichteten das Modul **DataCrypt** für verschiedene Systemarchitekturen (MS Windows, Solaris, AIX, Linux, HP-UX) zur Verfügung. Alternative Maßnahmen wie Zugriffsbeschränkung auf Betriebssystemebene, Tools zur Betriebssystemhärtung und physikalische Blackbox wurden ausgeschlossen, da diese Maßnahmen entweder Sicherheitslücken aufweisen oder mit Problemen bzgl. Realisierung, Administrierbarkeit und Wartbarkeit sowie evtl. zusätzlichen Aufwände für eine Evaluierung der Abfragekomponenten verbunden sind. Der Verpflichtete muss durch die **Abfragevertraulichkeit** durch zusätzliche organisatorische Regelungen angemessen unterstützen.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

2.5.2 Abfragelogik

Mit **Abfragelogik** werden die technischen Abläufe bezeichnet, die bei einem Auskunftersuchen und einem gegebenen Datenbestand beim Verpflichteten eine Auswahl dieses Datenbestands (genauer: eine Auswahl der Kontodatensätze bestimmter natürlicher und juristischer Personen) als Ergebnis zurückliefern. Die Abfragelogik wird zum Teil bei der BAFin und zum Teil bei den Verpflichteten implementiert. Das vorliegende Dokument spezifiziert lediglich den Teil der Abfragelogik, der für die Verpflichteten relevant ist.

Vom Bedarfsträger werden exakt und vollständig spezifizierte Anhaltsdaten als Kriterien für die Selektion der Konto-Datensätze gefordert. Als Anhaltsdaten müssen wegen des Datenschutzes mindestens eine Kontonummer oder ein Name angegeben werden.

Eine unscharfe Suche wird lediglich zum Ausgleich verschiedenartiger technischer Darstellung (Groß- / Kleinschreibung, Abkürzungen, Synonyme, Sonderzeichen, Wortvertauschungen) eingesetzt. Bei der Abfrage können Parameter angegeben werden, welche die Abfragelogik hinsichtlich der Unschärfe beeinflussen. Teile der **Abfragelogik** werden bereits im Modul **DataCrypt** von der BAFin zur Verfügung gestellt (siehe Abschnitt 2.5.1).

Die maximale Anzahl der im Abfrage-Ergebnis zurückzugebenden Kontodatensätze wird ebenfalls bei der Abfrage angegeben. Falls die Anzahl der gefundenen Kontodatensätze diese maximale Anzahl übersteigt, werden keine Kontoinformationen an die BAFin gesendet. Es wird lediglich die Anzahl der Treffer übermittelt.

2.5.3 Mengengerüst, Performanz und Verfügbarkeit

Bei den Vorgaben für Mengengerüst, Performanz und Verfügbarkeit wurden insbesondere mögliche Anforderungen der Bedarfsträger sowie der übliche Geschäftsbetrieb der Verpflichteten berücksichtigt. Die Anforderungen sind bereits auf eine mögliche elektronische Einreichung durch Bedarfsträger sowie die damit zu erwartenden Mengengerüste ausgelegt. Dennoch kann es sein, dass die Anforderungen an die Verpflichteten im Laufe der Zeit angepasst werden müssen.

Da insbesondere das Mengengerüst von Verpflichtetem zu Verpflichtetem stark variiert, können in dem vorliegenden Dokument keine allgemein gültigen Vorschläge zur angemessenen Ausstattung der Systeme bei den Verpflichteten gemacht werden. Es wird davon ausgegangen, dass die Systeme der Verpflichteten ausreichend skalierbar konzipiert werden.

2.5.4 Mandantenfähige Abfragekomponenten

Es ist zulässig, dass mehrere Verpflichtete das Auskunftsverfahren mittels einer gemeinsamen, mandantenfähigen Abfragekomponente implementieren. Bei einer mandantenfähigen Abfragekomponente ist seitens der Verpflichteten (Mandanten) streng darauf zu achten, dass sowohl die Kontoinformationen als auch die Abfragen separat für jeden Mandanten behandelt werden. Welche Teile des Auskunftsverfahrens gemeinsam und welche für die Mandanten getrennt realisiert werden, wird im normativen Teil des vorliegenden Dokuments detailliert angegeben.

3 Datenübertragung zwischen BAFin und Verpflichteten (normativ)

3.1 Netzverbindung zwischen BAFin und Verpflichteten

- (1) Die BAFin übermittelt den Verpflichteten folgende technischen Parameter der bei den Verpflichteten zu realisierenden Netze:
 - a) Netzadresse und Netzmaske des **Zugangsnetzes Verpflichteter**
- (2) Die BAFin übermittelt den Verpflichteten folgende technischen Parameter der zugreifenden Stellen der BAFin:
 - a) Netzadresse und Netzmasken der **Zugangsnetze BAFin** bei den Stellen der BAFin
- (3) Die Netzverbindung erfolgt in der Regel über das Internet. Falls die Internetverbindung gestört ist, wird seitens der BAFin automatisch versucht, eine Verbindung über ISDN aufzubauen (Fallback-Zugang). Bei jedem Sendevorgang wird zunächst erneut versucht, die Internetverbindung aufzubauen.
- (4) Der Verpflichtete versucht jeweils zunächst eine Verbindung über das Internet aufzubauen. Nach einer konfigurierbare Anzahl Fehlversuchen versucht der Verpflichtete seinerseits über einen ISDN-Zugang (Fallback-Dial-In) eine Verbindung zur BAFin aufzubauen. Bei jedem Sendevorgang versucht der Verpflichtete zunächst erneut, die Internetverbindung aufzubauen, bevor er den Fallback-Dial-In-Zugang verwendet.
- (5) Die Übertragungskapazität der Netzwerk-Komponenten ist gemäß den Anforderungen an die Antwortzeit ausulegen.

3.1.1 Zugang über Internet

Für die primäre Netzverbindung zwischen BAFin und Verpflichtetem sind seitens des Verpflichteten folgende Anforderungen zu erfüllen:

- (1) Der Verpflichtete richtet einen permanenten Internetzugang für das Auskunftersuchen gemäß § 24c KWG ein. Hierfür kann auch ein bereits bestehender Internetzugang verwendet werden.
- (2) Der Verpflichtete legt folgende technischen Parameter fest und teilt sie der BAFin mit:
 - a) Öffentliche IP-Adresse des **Routers Abfrage-Zugang**.
 - b) Öffentliche IP-Adresse des **VPN-Gateways Abfrage-Zugang**.
- (3) Die BAFin übermittelt den Verpflichteten folgende technischen Parameter der zugreifenden Stellen der BAFin:
 - a) Öffentliche IP-Adressen der **Router BAFin-Zugang** bei den Stellen der BAFin.
 - b) Öffentliche IP-Adressen der **VPN-Gateways BAFin-Zugang** bei den Stellen der BAFin.
- (4) Für **mandantenfähige Abfragekomponenten** kann ein Internetzugang für alle Mandanten gemeinsam verwendet werden.

Verfahren zum automatisierten Abruf von Kontoinformationen

Schnittstellenspezifikation BAFin - Kreditinstitute

3.1.2 Fallback-Zugang über ISDN Dial-In

Für die sekundäre Netzverbindung (Fallback-Dial-In) zwischen BAFin und Verpflichtetem sind seitens des Verpflichteten folgende Anforderungen zu erfüllen:

- (1) Der Verpflichtete richtet einen ISDN-Zugang für das Auskunftersuchen gemäß § 24c KWG ein. Hierfür kann auch ein bereits bestehender ISDN-Zugang verwendet werden.
- (2) Der **Router Abfrage-Zugang** muss für Einwahl und Auswahl über ISDN mit folgenden Parametern konfiguriert sein:
 - a) Authentisierung mittels PPP/CHAP
 - b) Aktivierung des Merkmals CLIP (Calling-Line-Identification-Presentation)
- (3) Der Verpflichtete konfiguriert folgende technischen Parameter gemäß den Vorgaben der BAFin:
 - a) IP-Adresse für das ISDN-Interface des **Routers Abfrage-Zugang**
 - b) IP-Adressen der zugreifenden Stellen (ISDN-Interfaces der **Router BAFin-Zugang**)
 - a) CLIs (Rufnummern) der zugreifenden Stellen (**Router BAFin-Zugang**)
 - a) Benutzernamen und Passwörter für die Einwahl der BAFin beim Verpflichteten (**Router Abfrage-Zugang**)
 - b) Benutzernamen und Passwörter für die Einwahl des Verpflichteten bei den Stellen der BAFin (**Router BAFin-Zugang**)
 - c) Time-Out für Verbindungsaufbau
 - d) Time-Out für Einwahl über ISDN
- (4) Der Verpflichtete legt folgende technischen Parameter fest und teilt sie der BAFin mit:
 - a) CLIs (Rufnummern) für den **Router Abfrage-Zugang**
- (5) Der **Router Abfrage-Zugang** muss so konfiguriert werden, dass er den Verbindungsaufbau über das **Transfernetz-2** versucht, falls die Verbindung über **Transfernetz-1** nicht zustande kommt.
- (6) Für **mandantenfähige Abfragekomponenten** kann ein ISDN-Zugang für alle Mandanten gemeinsam verwendet werden.

3.2 Router Abfrage-Zugang

- (1) Am externen und internen LAN-Interface des **Routers Abfrage-Zugang** muss der Verpflichtete die öffentliche IP-Adresse des **Routers Abfrage-Zugang** (vgl. Abschnitt 3.1.1) konfigurieren.
- (2) Der **Router Abfrage-Zugang** muss folgende Zugriffsberechtigungen und –beschränkungen durchsetzen (Paketfilter-Funktionalität):
 - a) Zugriff (Inbound/Outbound) ausschließlich von den Stellen der BAFin
 - b) Zugriff (Inbound/Outbound) ausschließlich über die für IPSec/IKE und das Online-Management **Firewall / VPN Abfrage-Zugang** erforderlichen Protokolle
 - c) Zugriff auf den Router zur Administration ausschließlich über die lokale Konsole
 - d) Zugriff auf den Router für SNMP-Monitoring ausschließlich über interne Schnittstellen
 - e) alle anderen Zugriffe müssen verhindert werden
- (3) Für **mandantenfähige Abfragekomponenten** kann ein **Router Abfrage-Zugang** für alle Mandanten gemeinsam verwendet werden.

3.3 Firewall / VPN-Gateway Abfrage-Zugang

- (1) Für **mandantenfähige Abfragekomponenten** kann **Firewall / VPN-Gateway Abfrage-Zugang** für alle Mandanten gemeinsam verwendet werden.

3.3.1 Firewall-Funktionalität

Für **Firewall / VPN Abfrage-Zugang** werden die Zugriffsberechtigungen und –beschränkungen per Smart Card durch die BAFin vorgegeben.

Falls darüber hinaus weitere Firewalls / VPN-Gateways seitens des Verpflichteten eingesetzt werden, müssen diese hinsichtlich der Firewall-Funktionalität folgende Anforderungen erfüllen:

- (1) Es müssen folgende Zugriffsberechtigungen und –beschränkungen durchgesetzt werden:
- a) Zugriff **Transfernetz / VPN-Gateway Abfrage-Zugang** (Inbound/Outbound) ausschließlich von bzw. zu den Stellen der BAFin
 - b) Zugriff **Transfernetz / VPN-Gateway Abfrage-Zugang** (Inbound/Outbound) ausschließlich über die für IPSec/IKE und das zentrale Management des **VPN-Gateways Abfrage-Zugang** erforderlichen Protokolle
 - c) Zugriff **VPN-Gateway Abfrage-Zugang / Zugangsnetz Verpflichteter** (Inbound/Outbound) ausschließlich zwischen **VPN-Gateway Abfrage-Zugang** und **Abfragekomponente**
 - d) Zugriff **VPN-Gateway Abfrage-Zugang / Zugangsnetz Verpflichteter** (Inbound/Outbound) ausschließlich über das für Secure-Copy (scp) erforderliche Protokoll (TCP 22)
 - e) Zugriff zur Administration der Firewall-Funktionalität (nur von dedizierten Systemen über die erforderlichen Protokolle)
 - f) alle anderen Zugriffe müssen verhindert werden.
- (2) Der Administrationszugang muss durch ausreichend starke Authentisierungsmechanismen und ggf. Verschlüsselung abgesichert sein. Die erforderliche Stärke der Mechanismen wird vom Stand der Technik vorgegeben.

3.3.2 VPN-Funktionalität

Um eine Steuerung des VPNs durch die BAFin zu ermöglichen, werden das VPN-Protokoll, die zu verwendenden Parameter und Zugriffsberechtigungen und die Schlüssel zentral durch die BAFin vorgegeben. Hierfür setzt die BAFin SINA-Boxen und SINA Online-Management ein. Die Verteilung der Schlüssel und Zugriffsberechtigungen erfolgt via SmartCards. Die SINA-kompatiblen Boxen werden gemäß Firewall-Anforderungen konfiguriert.

- (1) Der Verpflichtete muss ein VPN-Gateway einsetzen, dass bzgl. folgender Eigenschaften kompatibel zu SINA [02.BSI.SINA] ist:
- a) VPN-Protokoll IPSec
 - b) Schlüssel- und Berechtigungsmanagement per SmartCard und SINA Online-Management
- (2) Auf Grund der Eigenschaften des VPN-Protokolls IPSec darf keine Network-Address-Translation (NAT) zwischen Internetzugang und dem VPN-Gateway erfolgen.
- (3) Der Verpflichtete legt folgende technischen Parameter fest und teilt sie der BAFin mit:
- a) IP-Adresse des **VPN-Gateways Abfrage-Zugang** im **Zugangsnetz Verpflichteter** (interne IP-Adresse)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (4) Die BAFin übermittelt den Verpflichteten per SmartCard folgende technischen Parameter des VPNs:
- a) öffentliche IP-Adresse des **VPN-Gateways Abfrage-Zugang** (vgl. Abschnitt 3.1.1)
 - b) IP-Adresse des **VPN-Gateways Abfrage-Zugang** im **Zugangsnetz Verpflichteter** (interne IP-Adresse)
 - a) Schlüsselmanagement mit Internet Key Exchange-Protokoll (IKE)
 - b) Authentifizierung mittels digitaler Zertifikate
 - c) Kryptographische Algorithmen (DSS / RSA, 3DES / AES, HMAC-SHA 1 / HMAC-RIPEMD 160)
 - d) Zugriffsberechtigungen und -beschränkungen bzgl. Source / Destination und der Netzwerk-Protokolle
- (5) Die Netzwerkverbindung zwischen **VPN-Gateway Abfrage-Zugang** und **Abfragekomponente** sind durch eine oder mehrere der folgenden Maßnahmen gegen unberechtigten Zugriff zu schützen:
- a) Verlegung ausschließlich in sicherer Umgebung (Rechenzentrum)
 - b) Verwendung eines separaten VPNs

3.4 Abfragekomponente

- (1) Für **mandantenfähige Abfragekomponenten** kann eine **Abfragekomponente** für alle Mandanten gemeinsam verwendet werden.

Für die **Abfragekomponente** sind hinsichtlich der Datenübertragung seitens des Verpflichteten folgende Anforderungen zu erfüllen:

- (2) Die **Abfragekomponente** muss korrekt in die beteiligten Netze routen
- (3) Die **Abfragekomponente** darf nicht zwischen den verschiedenen Netzen routen
- (4) Die **Abfragekomponente** muss hinsichtlich externer Zugriffe wie folgt gehärtet werden (Netzhärtung):
 - a) Deaktivierung aller nicht erforderlichen Dienste
 - b) Entfernen aller nicht erforderlichen Software-Komponenten
 - c) Verwenden von dedizierten Benutzerkonten für die verschiedenen Funktionen (Administration, Import, Zugriff BAFin)
 - d) Administratoren müssen sich namentlich einloggen (Nachweisbarkeit)
 - e) Entfernen aller nicht erforderlichen Zugriffsberechtigungen für die Benutzer
 - f) Entfernen aller nicht erforderlichen Benutzerkonten
- (5) Der Verpflichtete legt folgende technischen Parameter fest und teilt sie der BAFin mit:
 - a) IP-Adresse der **Abfragekomponente** im **Zugangsnetz Verpflichteter** (externe IP-Adresse)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (6) Die BAFin übermittelt den Verpflichteten folgende technischen Parameter der zugreifenden Stellen der BAFin:
- a) Benutzernamen und Passwörter der Stellen der BAFin für den Zugriff auf die **Abfragekomponente**. Für **mandantenfähige Abfragekomponenten** wird je Mandant und je Stelle der BAFin ein eigenes Benutzerkonto **Abfrage-User** benötigt.
 - b) IP-Adressen der **Empfangskomponenten** bei den Stellen der BAFin
 - c) Benutzernamen und Passwörter für den Zugriff auf die **Empfangskomponenten** bei den Stellen der BAFin
- (7) Der Verpflichtete konfiguriert folgende technischen Parameter gemäß den Vorgaben der BAFin:
- a) Benutzernamen und Passwörter für den Zugriff der Stellen der BAFin auf die **Abfragekomponente**
 - b) IP-Adressen der **Empfangskomponenten** der Stellen der BAFin in den **Zugangsnetzen BAFin** (externe IP-Adressen)
 - c) Benutzernamen und Passwörter für den Zugriff des Verpflichteten auf die **Empfangskomponenten** bei den Stellen der BAFin
- (8) Die Benutzerkonten für den Zugriff der BAFin auf die **Abfragekomponente** müssen folgende Anforderungen erfüllen:
- a) Der Benutzer darf keine Berechtigung haben, eine Login-Shell zu öffnen
 - b) Der Benutzer darf ausschließlich die Berechtigung haben, Dateien in seinem Home-Verzeichnis abzulegen und zu löschen
 - c) Jeder Benutzer muss ein eigenes Home-Verzeichnis besitzen.
- Für die **Abfragekomponente** stellt die BAFin die Erfüllung folgender Anforderungen sicher:
- (9) Jede Stelle der BAFin greift über ein separates Benutzerkonto auf die **Abfragekomponente** zu.
- (10) Für den Import der Kontoinformationen in die **Abfragekomponente** muss ein dediziertes technisches Benutzerkonto gemäß folgenden Anforderungen eingerichtet werden:
- a) Der Benutzer darf keine Berechtigung haben, eine Login-Shell zu öffnen
 - b) Der Benutzer darf ausschließlich die Berechtigung haben, Import-Dateien an die **Abfragekomponente** zu übermitteln

3.5 SSH-Daemon

Für den **SSH-Daemon** sind hinsichtlich der Datenübertragung seitens des Verpflichteten folgende Anforderungen zu erfüllen:

- (1) Der SSH-Dienst darf keine Authentisierung per Benutzername/Passwort akzeptieren.
- (2) Der Verpflichtete erzeugt und konfiguriert folgende Schlüsselpaare und teilt den öffentlichen Teil der BAFin mit:
 - a) Host-Schlüsselpaar für die **Abfragekomponente**
 - b) Benutzer-Schlüsselpaare für den Zugang des Verpflichteten zu den **Empfangskomponenten**. Für **mandantenfähige Abfragekomponenten** wird je Mandant ein eigenes Benutzer-Schlüsselpaar für den Zugang des Verpflichteten benötigt.
- (3) Der private Schlüssel für den Zugang des Verpflichteten zu den **Empfangskomponenten** muss angemessen gegen unberechtigten Zugriff geschützt werden (Passphrase und/oder sonstige Zugriffsbeschränkungen)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (4) Die BAFin erzeugt folgende Schlüsselpaare und übermittelt den öffentlichen Teil dem Verpflichteten:
 - a) Host-Schlüsselpaar für die **Empfangskomponenten**
 - b) Benutzer-Schlüsselpaare für den Zugang der BAFin zu der **Abfragekomponente**. Für **mandantenfähige Abfragekomponenten** wird je Mandant ein eigenes Benutzer-Schlüsselpaar für den Zugang der BAFin benötigt.
- (5) Der Verpflichtete konfiguriert folgende technischen Parameter gemäß den Vorgaben der BAFin:
 - a) Öffentlicher Teil des Host-Schlüsselpaares für die **Empfangskomponenten**
 - b) Öffentlicher Teil der Benutzer-Schlüsselpaare für den Zugang der BAFin zu der **Abfragekomponente**
- (6) Es wird dem Verpflichteten empfohlen, folgende Information zu protokollieren:
 - a) Datum, Uhrzeit und Dateiname der per scp an die **Empfangskomponenten** übertragenen Dateien

4 Technische Abläufe (normativ)

In diesem Kapitel werden die für den Verpflichteten relevanten technische Abläufe erläutert und die entsprechenden Anforderungen definiert. Hierbei wird auf *Datennamen* Bezug genommen, die in Kapitel 5 spezifiziert werden.

4.1 Abfrageverarbeitung

Abfragen müssen wie folgt durch die **Abfragekomponente** verarbeitet werden.

4.1.1 Empfang von Abfragen

Die abfragende Stelle der BAFin legt Abfragen als *Abfrage-Datei* per Dateitransfer mittels Secure-Copy (scp) im Home-Verzeichnis des **Abfrage-User** auf der **Abfragekomponente** ab.

- (1) Die **Abfrage-Bearbeitung** muss fortlaufend prüfen, ob neue *Abfrage-Dateien* in den Home-Verzeichnissen der **Abfrage-User** abgelegt wurden und diese unverzüglich weiter verarbeiten.
- (2) Falls die BAFin *Abfrage-Dateien* als TGZ-Archiv (mittels tar / gzip gepackte und komprimierte Dateien) ablegt, muss die **Abfragekomponente** in der Lage sein, diese zu entpacken. TGZ-Archive werden durch die Dateierweiterung „.tar.gz“ oder „.tgz“ kenntlich gemacht.

4.1.2 Prüfung der Abfragekonsistenz

- (1) Die **Abfrage-Bearbeitung** muss abgelegte *Abfrage-Dateien* hinsichtlich der Konsistenz der enthaltenen Abfrage bzw. Abfragen analysieren:
 - a) Stimmt die in der Abfrage übermittelte *Verpflichteten-ID* nicht mit der des Verpflichteten überein, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Übermittlungsfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* der Text „Falsche Verpflichteten-ID“ einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
 - b) Gehört die in der Abfrage übermittelte *Abfragestellen-ID* nicht zum **Abfrage-User**, in dessen Home-Verzeichnis die *Abfrage-Dateien* abgelegt wurden, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Übermittlungsfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* der Text „Falsche Abfragestellen-ID“ einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
 - c) Falls die Felder der *Abfrage-Anhaltsdaten* keiner sinnvollen Kombination gemäß Abschnitt 5.2.1.2 entsprechen, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Inhaltsfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* der Text „Kombination der Anhaltsdaten nicht sinnvoll“ einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
 - d) Falls die Felder der *Abfrage-Anhaltsdaten* keiner zulässigen Kombination gemäß Abschnitt 5.2.1.2 entsprechen, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Inhaltsfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* der Text „Kombination der Anhaltsdaten nicht zulässig“ einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
 - e) Falls die *Abfrage-Steuerungsdaten* unzulässige Parameter enthalten (z.B. *Abfrage-maximale-Anzahl-Kontodatensätze* ist kleiner als 0), dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Parameterfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* ein erläuternder Text einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- f) Falls die in den *Abfrage-Verwaltungsdaten* angegebene *Abfrage-Key-ID* von der *Daten-Key-ID* der **Abfragekomponente** verschieden ist, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Schlüsselfehler“ zu setzen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
- g) Falls die **Abfragekomponente** Abfragen nur mit Verzögerung weiter verarbeiten kann (z.B. auf Grund von Wartungsarbeiten), dann ist für diese Abfragen in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Temporärer Systemfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* eine ausführliche Begründung einzutragen. Die Abfrage wird durch die **Abfragekomponente** zu einem späteren Zeitpunkt weiter bearbeitet.
- h) Falls eine Abfrage durch die **Abfragekomponente** nicht analysiert werden konnte, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Syntaxfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* eine ausführliche Beschreibung einzutragen. Alle weiteren Felder zu der Abfrage in der *Abfrage-Bestätigungs-Datei* sind nur zu setzen, falls die entsprechenden Daten bekannt sind. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
- i) Falls die *Abfrage-Datei* als Ganzes durch die **Abfragekomponente** nicht analysiert werden konnte, dann ist in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Syntaxfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* eine ausführliche Beschreibung einzutragen. Alle weiteren Felder der *Abfrage-Bestätigungs-Datei* sind nur zu setzen, falls die entsprechenden Daten bekannt sind. Die *Abfrage-Datei* wird durch die **Abfragekomponente** nicht weiter bearbeitet.
- j) Falls die **Abfragekomponente** eine Abfrage auf Grund eines sonstigen Fehlers nicht weiter verarbeiten kann, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Permanenter Systemfehler“ zu setzen und in der *Abfrage-Fehlerbeschreibung* eine ausführliche Beschreibung einzutragen. Die Abfrage wird durch die **Abfragekomponente** nicht weiter bearbeitet.
- k) Falls die Konsistenzprüfung für eine Abfrage positiv verlaufen ist, dann ist für diese Abfrage in der *Abfrage-Bestätigungs-Datei* der *Abfrage-Fehlercode* „Kein Fehler“ zu setzen. Die Abfrage wird durch die **Abfragekomponente** weiter bearbeitet.

4.1.3 Versand der *Abfrage-Bestätigungs-Datei*

- (1) Nach Prüfung der Abfragekonsistenz sendet die **Abfrage-Bearbeitung** unverzüglich (vgl. Abschnitt 7.2 **Bestätigungszeit**) eine *Abfrage-Bestätigungs-Datei* mit den *Abfrage-Verwaltungsdaten*, den *Abfrage-Steuerungsdaten* und der *Abfrage-Empfangsbestätigung* (*Abfrage-Fehlercode* und *Abfrage-Fehlerbeschreibung*) zu allen in der *Abfrage-Datei* enthaltenen Abfragen via Secure-Copy an die **Empfangskomponente** der abfragenden Stelle.
- (2) Der Name für die *Abfrage-Bestätigungs-Datei* ist gemäß Abschnitt 5.2.1 festzulegen.
- (3) Die **Abfragekomponente** muss die *Abfrage-Bestätigungs-Datei* als TGZ-Archiv versenden.
- (4) Falls die Netzwerkverbindung zum Versand der *Abfrage-Bestätigungs-Datei* nicht sofort zustande kommt, muss die **Abfragekomponente** den Versand so oft weiter versuchen, bis er erfolgreich war. Hierfür ist eine konfigurierbare Retry-Zeit (Default-Wert: 1 Minute) einzurichten.
- (5) Falls die Netzwerkverbindung zum Versand der *Abfrage-Bestätigungs-Datei* nach einer konfigurierbaren Anzahl von Versand-Versuchen (Default-Wert: 10) nicht zustande kommt, muss die **Abfragekomponente** den Administrator des Verpflichteten darüber benachrichtigen.
- (6) Wenn die *Abfrage-Bestätigungs-Datei* erfolgreich versendet wurde, dann erhöht die **Abfragekomponente** den *Abfragezähler* um den Wert 1.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (7) Alle Dateien und Daten zu Abfragen, die auf Grund einer nicht bestandenen Konsistenzprüfung nicht weiter verarbeitet werden, sind nach Versand der *Abfrage-Bestätigungs-Datei* durch die **Abfragekomponente**, ggf. nach erfolgter Fehleranalyse, zu löschen. Die Fehleranalyse hat unverzüglich zu erfolgen. Für eine weitergehende Fehleranalyse dürfen nur Dateien gespeichert werden, aus denen die eigentlichen Daten der Abfrage entfernt wurden.

4.1.4 Selektion der gesuchten Kontoinformationen

- (1) Nach Empfang einer *Abfrage-Datei* muss die **Abfrage-Bearbeitung** unverzüglich die Kontoinformationen gemäß den in der *Abfrage-Datei* enthaltenen *Abfrage-Anhaltsdaten* auswerten und das Ergebnis der Abfragen an die BAFin übermitteln (vgl. Abschnitt 7.2 **Antwortzeit**).

Für die Selektion der **passenden** Kontoinformationen muss die **Abfrage-Bearbeitung** nach folgender *Abfragelogik* vorgehen:

- (2) Damit ein *Kontodatenatz* auf Grund gegebener *Abfrage-Anhaltsdaten* selektiert wird, muss zu jedem angegebenen Anhaltsdatenfeld mindestens ein Kontodatenfeld (bzw. eine Kombination von Kontodatenfeldern) gemäß Tabelle 1 existieren, dessen Inhalt zum Inhalt des Anhaltsdatenfeldes **passt**.
- (3) Der Inhalt eines Kontodatenfeldes oder einer Kombination von Kontodatenfeldern **passt** genau dann zum Inhalt des Anhaltsdatenfeldes, wenn der **normalisierte Inhalt** des Anhaltsdatenfeldes gemäß einer Vergleichsoperation vollständig oder mit einem **wesentlichen Anteil** des **normalisierten Inhalts** des Kontodatenfeldes (bzw. der Kombination von Kontodatenfeldern) übereinstimmt.

Die BAFin bereitet die *Abfrage-Anhaltsdaten* analog zu den importierten Kontoinformationen durch **Normalisierung**, **Token-Separierung** und Verschlüsselung auf. Die Vergleichsoperationen finden in der **Abfragekomponente** auf beiderseits gleichartig **normalisierten** und verschlüsselten, ggf. in **Tokenlisten** separierten, Daten statt und erfordern daher keine Entschlüsselung in der **Abfragekomponente**.

- (4) Vergleichsoperation für *Datumfelder*: Die **Datum-Normalisierung** findet im Modul **DataCrypt** statt. Damit der Inhalt des Anhaltsdatenfeldes zu dem des Kontodatenfeldes **passt** müssen die **normalisierten** und verschlüsselten Inhalte identisch sein.
- (5) Vergleichsoperation für die Felder *Konto-Nummer* und *Auswahl-Konto-Nummer*: Die **Kontonummern-Normalisierung** findet im Modul **DataCrypt** statt. Damit der Inhalt des Feldes *Auswahl-Konto-Nummer* zu dem des Feldes *Konto-Nummer* **passt** müssen die **normalisierten** und verschlüsselten Inhalte identisch sein.
- (6) Vergleichsoperation für ein *Auswahl-Namensfeld* und gemäß Tabelle 1 relevante *Namensfelder*:
- Im Modul **DataCrypt** werden die Inhalte **normalisiert** und aus den **normalisierten Inhalten** für jedes Feld **Tokenlisten** (Listen der separierten Einzelwörter) mit einzeln verschlüsselten **Token** erzeugt. Für *Namensfelder* erfolgt diese Verarbeitung beim Import, für *Auswahl-Namensfelder* beim Erzeugen der Abfrage durch die BAFin.
 - Die **Tokenliste** des *Auswahl-Namensfeldes* ist die **Auswahl-Tokenliste**.
 - Falls gemäß *Auswahl-Namensfeld* und Tabelle 1 mehrere *Namensfelder* relevant sind, werden die **Tokenlisten** zu einer **Vergleichs-Tokenliste** zusammengefasst (Bilden der Vereinigungsmenge; Beispiel: {„MICHAEL“, „MARKUS“}, {„SCHULTZE“, „MAIER“} - > {„MICHAEL“, „MARKUS“, „SCHULTZE“, „MAIER“}). Falls nur ein *Namensfeld* relevant ist, besteht die **Vergleichs-Tokenliste** nur aus der **Tokenliste** des *Namensfeldes*.

Verfahren zum automatisierten Abruf von Kontoinformationen
Schnittstellenspezifikation BAFin - Kreditinstitute

- d) Falls die **Auswahl-Tokenliste** keine Untermenge (Teilmenge) der **Vergleichs-Tokenliste** ist, dann passt der Inhalt des *Auswahl-Namensfeldes* nicht zum Inhalt der relevanten *Namensfelder*. Der Vergleich wird abgebrochen, der *Kontodatensatz* wird nicht selektiert. Ansonsten wird wie folgt fortgefahren:
- e) Bilden der **Schnitt-Tokenliste** als Schnittmenge aus **Auswahl-Tokenliste** und **Vergleichs-Tokenliste** (Beispiel: {„MICHAEL“, „SCHULTZE“, „MAIER“}, {„MICHAEL“, „MARKUS“, „SCHULTZE“, „MAIER“} -> {„MICHAEL“, „SCHULTZE“, „MAIER“}).
- f) Berechnung des **Übereinstimmungsmaßes** als Relation der Kardinalität (Anzahl der enthaltenen **Token**) der **Schnitt-Tokenliste** zur Kardinalität der **Vergleichs-Tokenliste** (für das angegebene Beispiel ist das **Übereinstimmungsmaß** $3/4 = 75\%$).
- g) Der Inhalt eines *Auswahl-Namensfeldes* **passt** zum Inhalt der relevanten *Namensfelder*, wenn das ermittelte **Übereinstimmungsmaß** größer oder gleich einem in den *Abfrage-Steuerungsdaten* vorgegebenen **minimalen Übereinstimmungsmaß** (*Abfrage-minimale-Übereinstimmung-Namen*) ist.

Anhaltsdatenfeld / Kontodatenfelder in denen gesucht wird	Konto-Nummer	Einrichtungsdatum	Auflösungsdatum	Inhaber-Nachname	Inhaber-Vorname	Inhaber-Geburtsdatum	VB-Nachname	VB-Vorname	VB-Geburtsdatum	WB-Nachname	WB-Vorname	WB-Anschrift
<i>Auswahl-Konto-Nummer</i>	X											
<i>Auswahl-Einrichtungsdatum</i>		X										
<i>Auswahl-Auflösungsdatum</i>			X									
<i>Auswahl-Inhaber-Name</i>				X	X							
<i>Auswahl-Inhaber-Nachname</i>				X								
<i>Auswahl-Inhaber-Vorname</i>					X							
<i>Auswahl-Inhaber-Geburtsdatum</i>						X						
<i>Auswahl-VB-Name</i>							X	X				
<i>Auswahl-VB-Nachname</i>							X					
<i>Auswahl-VB-Vorname</i>								X				
<i>Auswahl-VB-Geburtsdatum</i>									X			

Verfahren zum automatisierten Abruf von Kontoinformationen
Schnittstellenspezifikation BAFin - Kreditinstitute

Anhaltsdatenfeld / Kontodatenfelder in denen gesucht wird	Konto-Nummer	Einrichtungsdatum	Auflösungsdatum	Inhaber-Nachname	Inhaber-Vorname	Inhaber-Geburtsdatum	VB-Nachname	VB-Vorname	VB-Geburtsdatum	WB-Nachname	WB-Vorname	WB-Anschrift
Auswahl-WB-Name										X	X	
Auswahl-WB-Nachname										X		
Auswahl-WB-Vorname											X	
Auswahl-WB-Anschrift												X
Auswahl-Name				X	X		X	X		X	X	
Auswahl-Nachname				X			X			X		
Auswahl-Vorname					X			X			X	
Auswahl-Geburtsdatum						X			X			

Tabelle 1: Selektion der abzufragenden Daten durch Anhaltsdaten

4.1.5 Bereitstellung und Versand der Abfrage-Ergebnisse

- (1) Für jede in der *Abfrage-Datei* angegebene Abfrage sind eine eigene *Abfrage-Trefferzahl-Datei* und ggf. eine eigene *Abfrage-Ergebnis-Datei* zu erzeugen.
- (2) Nach Selektion der in einer Abfrage gesuchten Kontoinformationen erzeugt die **Abfrage-Bearbeitung** unverzüglich (vgl. Abschnitt 7.2 **Antwortzeit**) eine *Abfrage-Trefferzahl-Datei* und sendet diese via Secure-Copy an die **Empfangskomponente** der abfragenden Stelle.
- (3) Der Name für die *Abfrage-Trefferzahl-Datei* ist gemäß Abschnitt 5.2.1 festzulegen.
- (4) Die **Abfragekomponente** muss die *Abfrage-Trefferzahl-Datei* als TGZ-Archiv versenden.
- (5) Falls die Netzwerkverbindung zum Versand der *Abfrage-Trefferzahl-Datei* nicht sofort zustande kommt, muss die **Abfragekomponente** den Versand so oft weiter versuchen, bis er erfolgreich war. Hierfür ist eine konfigurierbare Retry-Zeit (Default-Wert: 1 Minute) einzurichten.
- (6) Falls die Netzwerkverbindung zum Versand der *Abfrage-Trefferzahl-Datei* nach einer konfigurierbaren Anzahl von Versand-Versuchen (Default-Wert: 10) nicht zustande kommt, muss die **Abfragekomponente** den Administrator des Verpflichteten darüber benachrichtigen.
- (7) Falls keine zur Abfrage **passenden** Kontoinformationen gefunden wurden, dann ist die *Abfrage-Trefferzahl* = 0 und es wird keine *Abfrage-Ergebnis-Datei* erzeugt.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (8) Falls der Wert an gefundenen Treffern über dem Wert *Anfrage-maximale-Anzahl-Kontodatensätze* aus den *Abfrage-Steuerungsdaten* liegt, dann wird keine *Abfrage-Ergebnis-Datei* erzeugt.
- (9) Falls zur Abfrage **passende** Kontoinformationen gefunden wurden und der Wert an gefundenen Treffern den Wert *Anfrage-maximale-Anzahl-Kontodatensätze* nicht überschreitet, dann muss die **Abfragekomponente** eine *Abfrage-Ergebnis-Datei* erzeugen und im Home-Verzeichnis des **Abfrage-Users** als TGZ-Archiv ablegen.
- (10) Der Name für die *Abfrage-Ergebnis-Datei* ist gemäß Abschnitt 5.2.1 festzulegen.
- (11) Nach dem erfolgreichen Versenden der *Abfrage-Trefferzahl-Datei* sind durch die **Abfragekomponente** alle Dateien und Daten zu der Abfrage bis auf die zu *Abfrage-Ergebnis-Datei* löschen. Die zugehörige *Abfrage-Datei* ist spätestens nach dem Bearbeiten der letzten Abfrage zu löschen.

Die *Abfrage-Ergebnis-Datei* wird aktiv von der abfragenden Stelle der BAFin aus dem Home-Verzeichnis des **Abfrage-Users** abgeholt und danach gelöscht. Lediglich im Falle einer Störung können *Abfrage-Ergebnis-Datei* im Home-Verzeichnis des **Abfrage-Users** verbleiben.

4.1.6 Allgemeine Anforderungen an die Bearbeitung von Abfragen

- (1) Abfragen, die in der **Abfragekomponente** bearbeitet werden, dürfen auch bei einem Totalausfall der **Abfragekomponente** nicht verloren gehen.
- (2) Die **Abfragekomponente** löscht täglich diejenigen *Abfrage-Ergebnis-Dateien* aus den Home-Verzeichnissen der **Abfrage-User**, die älter sind als eine konfigurierbare Zeitdauer (Default-Vorgabe der BAFin: 14 Tage).

4.2 Import der Kontoinformationen

- (1) Die **Abfragekomponente** muss die zu importierenden *Import-Kontodatenatz-Datei* mit Hilfe des Moduls **DataCrypt** in eine *Abruf-Kontodatenatz-Datei* konvertieren: Dabei ist jeweils der aktuelle durch die BAFin vorgegebene Schlüssel zu verwenden.

Das Modul **DataCrypt** führt bei der Konvertierung folgende Schritte aus:

- Berechnung eines kryptographischen Hashwerts aus dem jeweiligen Kontodatenatz und speichern des Hashwerts im Feld *Datenatz-Hash*.
- Normalisieren und Verschlüsseln des Feldes *Konto-Nummer* in das Feld *Index-Konto-Nummer*.
- Normalisieren und Extrahieren der **Tokenlisten** aus den *Namensfeldern*. Verschlüsseln und Speichern der einzelnen **Token** in den *Index-Namensfeldern*.
- Verschlüsseln der einzelnen Felder des *Kontodatenatzes*. Das Feld *Datenatz-Gültigkeitsende*, das der internen Verwaltung der Datenätze in der Datenbank dient, wird zusätzlich unverschlüsselt als *Datenatz-Gültigkeitsende_plain* im jeweiligen Datenatz gespeichert.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (2) Die **Abfragekomponente** importiert die *Abruf-Kontodatenätze* aus einer *Abruf-Kontodatenatz-Datei* folgendermaßen in die Datenbank:
 - a) Import der Felder des *Abruf-Kontodatenatzes* als Datensatz in die Datenbank.
 - b) Indizieren der verschlüsselten *Datumfelder* des importierten *Abruf-Kontodatenatzes*.
 - c) Indizieren des normalisierten und verschlüsselten Feldes *Index-Konto-Nummer*.
 - d) Indizieren der einzelnen verschlüsselten **Token** aus den **Tokenlisten** der *Index-Namensfelder* in jeweils einen Index pro *Index-Namensfeld* als Verweis auf die zugehörigen Datensätze. Es ist zu beachten, dass bei der Löschung historischer Kontoinformationen nach der Aufbewahrungsfrist auch alle zugehörigen Indizes gelöscht werden müssen.
- (3) Während des Imports neuer Kontoinformationen müssen die alten Kontoinformationen jederzeit für Abfragen verfügbar sein.
- (4) Nach jedem Import der Kontoinformationen sind folgende Informationen für die *Abfrage-Ergebnisstatistiken* vorzuhalten:
 - a) Gesamte Anzahl der bereitgehaltenen Kontodatenätze (*Gesamt-Anzahl-Kontodatenätze*)
 - b) Zeitpunkt der letzten Aktualisierung der bereitgehaltenen Kontodatenätze (*Datenaktualisierungszeitpunkt*)
 - c) Art der letzten Aktualisierung der bereitgehaltenen Kontodatenätze (Full-Load/Incremental-Load, *Datenaktualisierungsart*)
 - d) Die Kennung des bei der Verschlüsselung der importierten Kontodatenätze verwendeten Schlüssels *Daten-Key-ID*

4.3 Verwaltung der Kontoinformationen

4.3.1 Löschung historischer Kontoinformationen

- (1) Die **Abfragekomponente** muss täglich historische Kontoinformationen löschen, die älter als die in § 24c KWG vorgeschriebene Aufbewahrungsfrist (3 Jahre) sind. Relevant für die Löschung ist das *Datenatz-Gültigkeitsende* für geänderte Kontodaten und das *Auflösungsdatum* für den gesamten Kontodatenatz. Es ist zu beachten, dass bei der Löschung historischer Kontoinformationen nach der Aufbewahrungsfrist auch alle zugehörigen Index-Einträge gelöscht werden müssen. Dies betrifft insbesondere geänderte Kontodaten.

4.3.2 Wechsel des DataCrypt-Schlüssels

- (1) Falls die BAFin einen neuen Schlüssel für das Modul **DataCrypt** vorgibt, sind zu dem vorgegebenen Termin die Kontoinformationen in der **Abfragekomponente** mit dem neuen Schlüssel verschlüsselt vorzuhalten. Für die Migration auf einen neuen Schlüssel gibt es zwei Möglichkeiten:
 - a) Vollständiges Neuladen der Kontoinformationen
 - b) Umverschlüsselung mittels **DataCrypt**: Die Kontoinformationen sind aus der Datenbank der **Abfragekomponente** als *Abruf-Kontodatenatz-Datei* zu exportieren. Diese kann mittels **DataCrypt** vom alten auf den neuen Schlüssel umverschlüsselt und dann erneut geladen werden.

5 Daten-Beschreibung (normativ)

5.1 Dateninhalte und –beziehungen

Im folgenden werden die für das technische Auskunftsverfahren wesentlichen Daten bzgl. der Inhalte und der zwischen diesen bestehenden Beziehungen definiert.

5.1.1 Abzufragende Daten bei den Verpflichteten

(1) Aus dem § 24c KWG [02.KWG§24c] ergeben sich folgende Daten, die je Konto/Depot von den Kreditinstituten zur Abfrage vorgehalten werden müssen:

- Verwaltungsdaten des Kontos/Depots:
 - Identifikation des Kontos/Depots
 - Tag der Einrichtung
 - Tag der Auflösung
- Identifikation Kontoinhaber (ggf. mehrere):
 - Name
 - Geburtstag
- Identifikation von Verfügungsberechtigten (ggf. mehrere):
 - Name
 - Geburtstag
- Identifikation von abweichend wirtschaftlich Berechtigten (ggf. mehrere):
 - Name
 - Anschrift

Es sind seitens der Verpflichteten nicht nur die jeweils aktuellen Daten, sondern auch historische Daten bis zu drei Jahre vorzuhalten. Daher werden diese Daten zusätzlich bezüglich des Gültigkeitszeitraums qualifiziert. Bei jeder Änderung der Kontodaten ist ein separater Kontodatensatz zu erstellen und gemäß dem Gültigkeitszeitraum zu qualifizieren. Daher können bei Kontoänderungen zu einem Konto mehrere Kontodatensätze existieren, die sich bzgl. des Gültigkeitszeitraums unterscheiden. Insbesondere muss gelten, dass die Gültigkeitszeiträume dieser Datensätze disjunkt sind (siehe Abschnitt 5.1.2.2).

Im folgenden werden die abzufragenden Daten bei den Verpflichteten bzgl. der Inhalte näher beschrieben und in einzelne Datenfelder aufgeteilt.

5.1.1.1 Verwaltungsdaten des Kontos/Depots

5.1.1.1.1 Identifikation des Kontos/Depots (*Konto-Nummer*)

(1) Die *Konto-Nummer* muss bei dem jeweiligen Verpflichteten als gemeinsame Identifikation aller dieses Konto betreffenden Vorgänge verwendet werden.

5.1.1.1.2 Tag der Errichtung (*Errichtungsdatum*)

(2) *Errichtungsdatum* ist der Tag der Kontoeröffnung.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

5.1.1.1.3 Tag der Auflösung (*Auflösungsdatum*)

- (3) *Auflösungsdatum* ist der Tag der Kontolöschung in den technischen Systemen des Verpflichteten.

5.1.1.2 Identifikation Kontoinhaber

- (1) Jedes Konto kann einen oder mehrere Inhaber aufweisen.
- (2) Name (bzw. eindeutige Bezeichnung) des Inhabers (*Inhaber-Name*): Der *Inhaber-Name* soll einerseits eine möglichst vollständige, genaue und eindeutige Festlegung der (natürlichen oder juristischen) Person ermöglichen.
- (3) Mit *Inhaber-Name* ist bei natürlichen Personen die Zusammenstellung aus dem Nachnamen (ggf. inkl. akademischer Titel und Namenszusätzen wie „von“) und den Vornamen (gemäß Ausweisdokumenten) gemeint. Nicht im Namen enthalten sind Geburtsnamen, Künstlernamen, religiöse Namen und Adelstitel.
- (4) Mit *Inhaber-Name* ist bei juristischen Personen eine amtlich registrierte Bezeichnung (z.B. Firmenname im Handelsregistereintrag o.ä.) gemeint. Bei der Schreibweise dieser Bezeichnung in den IT-Systemen des Verpflichteten wird davon ausgegangen, dass sie im wesentlichen vollständig und korrekt ist, jedoch gelegentlich Abkürzungen enthalten kann.
- (5) Geburtstag des Inhabers (*Inhaber-Geburtsdatum*): Mit *Inhaber-Geburtsdatum* ist bei natürlichen Personen das Geburtsdatum gemeint, dass in den Ausweisdokumenten des Inhabers amtlich dokumentiert ist. Bei juristischen Personen ist das *Inhaber-Geburtsdatum* nicht relevant und muss daher vom Verpflichteten nicht zurückgeliefert werden.

5.1.1.3 Identifikation von Verfügungsberechtigten

- (1) Jedes Konto kann beliebig viele Verfügungsberechtigte aufweisen.
- (2) Verfügungsberechtigte sind diejenigen (natürlichen oder juristischen) Personen, die zwar verfügungsberechtigt, aber keine Inhaber sind.
- (3) Name (bzw. eindeutige Bezeichnung) des Verfügungsberechtigten (*VB-Name*): Für *VB-Name* gelten die gleichen Randbedingungen wie für *Inhaber-Name*.
- (4) Geburtstag des Verfügungsberechtigten (*VB-Geburtsdatum*): Für *VB-Geburtsdatum* gelten die gleichen Randbedingungen wie für *Inhaber-Geburtsdatum*.

5.1.1.4 Identifikation von abweichend wirtschaftlich Berechtigten

- (1) Jedes Konto kann beliebig viele abweichend wirtschaftlich Berechtigte aufweisen.
- (2) Für abweichend wirtschaftlich Berechtigte sind Name und Anschrift vom Verpflichteten zu erheben ([GWG§8-Abs.1]).
- (3) Name (bzw. eindeutige Bezeichnung) des wirtschaftlich Berechtigten (*WB-Name*): Für *WB-Name* werden die gleichen Randbedingungen empfohlen wie für *Inhaber-Name*. Vom Verpflichteten sind bei natürlichen Personen mindestens der Nachname (ggf. inkl. akademischer Titel und Namenszusätzen wie „von“) und der Vorname anzugeben.
- (4) Anschrift des wirtschaftlich Berechtigten (*WB-Anschrift*): *WB-Anschrift* soll eine möglichst vollständige, genaue und eindeutige Festlegung der (natürlichen oder juristischen) Person ermöglichen. Diese Identifikation soll auch über einen längeren Zeitraum hinweg möglich sein.
- (5) Mit *WB-Anschrift* ist bei natürlichen Personen die Zusammenstellung aus Staat, Postleitzahl (Plz), Ort, Straße und Hausnummer des Hauptwohnsitzes gemeint. Zusätzlich können Informationen zu Gebäuden, Zimmernummern, „wohnhaft bei“ enthalten sein.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (6) Mit *WB-Anschrift* ist bei juristischen Personen die Zusammenstellung aus Staat, Postleitzahl (Plz), Ort, Straße und Hausnummer des Hauptsitzes gemeint.

5.1.2 Verwaltungsdaten in den Abfragekomponenten der Verpflichteten

5.1.2.1 Identifikation des Verpflichteten (*Verpflichteten-ID*)

- (1) Zur eindeutigen Identifikation der Verpflichteten (*Verpflichteten-ID*) wird die BAKNr verwendet. Die BAKNr wird von der BAFin als eindeutiges Identifizierungsmerkmal für alle Verpflichteten vergeben. Nach dem Untergang eines Verpflichteten wird dessen BAKNr nicht wieder verwendet.

5.1.2.2 Gültigkeitszeiträume für Kontodatensätze (*Datensatz-Gültigkeit*)

Die *Datensatz-Gültigkeit* dient zur Unterscheidung historischer Daten.

- (1) Die *Datensatz-Gültigkeit* beinhaltet das erste Datum (*Datensatz-Gültigkeitsbeginn*) und das letzte Datum (*Datensatz-Gültigkeitsende*), an dem ein Kontodatensatz gültig ist.
- (2) Unmittelbar vor dem *Datensatz-Gültigkeitsbeginn* gilt entweder ein früherer Kontodatensatz (bei geänderten Kontodaten) oder das Konto wurde neu eingerichtet. In letzterem Fall ist der *Datensatz-Gültigkeitsbeginn* gleich dem *Einrichtungsdatum*.
- (3) Unmittelbar nach dem *Datensatz-Gültigkeitsende* gilt entweder ein neuer Kontodatensatz (bei geänderten Kontodaten) oder das Konto wurde gelöscht. In letzterem Fall ist das *Datensatz-Gültigkeitsende* gleich dem *Auflösungsdatum*.
- (4) Die *Datensatz-Gültigkeit* dient den Verpflichteten dazu, historische Daten nach Ablauf der Aufbewahrungsfrist selektieren und löschen zu können. Relevant für die Löschung ist das *Datensatz-Gültigkeitsende* für geänderte Kontodaten und das *Auflösungsdatum* für den gesamten Kontodatensatz.
- (5) Die *Datensatz-Gültigkeit* ist vom Verpflichteten in den *Abfrage-Ergebnissen* zurückzugeben.

5.1.2.3 Status Abfrage-Datenbank

- (1) Folgende Statusdaten über die vom Verpflichteten zum Abruf bereitgehaltenen Kontodatensätze sind der BAFin in jedem Abfrageergebnis mit dem jeweils aktuellen Wert mitzuteilen:
- a) Zähler, der für jeden Verpflichteten individuell die erfolgten Abfragen zählt (*Abfragezähler*). Erfolgt ist eine Abfrage dann, wenn die Abfragekomponente des Verpflichteten eine *Abfrage-Bestätigungs-Datei* als Antwort zu einer *Abfrage-Datei* zurück gesendet hat.
 - b) Versionsnummer des technischen Abfrageverfahrens (*Abfrage-Versionsparameter*)
 - c) Gesamte Anzahl der bereitgehaltenen Kontodatensätze (*Gesamt-Anzahl-Kontodatensätze*)
 - d) Zeitpunkt der letzten Aktualisierung der bereitgehaltenen Kontodatensätze (*Datenaktualisierungszeitpunkt*)
 - e) Art der letzten Aktualisierung der bereitgehaltenen Kontodatensätze (Full-Load/Incremental-Load, *Datenaktualisierungsart*)

Die genannten Daten dienen der BAFin zu fortlaufenden Plausibilitätskontrollen und ermöglichen der BAFin ein frühzeitiges Erkennen von Inkonsistenzen.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

5.1.3 Verwaltungsdaten für die Abfrage bei den Verpflichteten

- (1) Jeder Abfrage wird durch die BAFin eine eindeutige *Abfragekennung* zugeordnet. Die BAFin stellt sicher, dass sich *Abfragekennungen* in dem Zeitraum, in dem Protokolldaten aufbewahrt werden müssen (maximal 24 Monate), nicht wiederholen.
- (2) Abfrage-Fehler sind durch die Abfragekomponente wie folgt zu klassifizieren (*Abfrage-Fehlercode*) und zu beschreiben (*Abfrage-Fehlerbeschreibung*):
 - a) „Kein Fehler“: Abfrage wird durch die Abfragekomponente des Verpflichteten weiter bearbeitet.
 - b) „Syntaxfehler“: *Abfrage-Datei* konnte durch die Abfragekomponente des Verpflichteten nicht analysiert werden und wird daher nicht weiter bearbeitet. Nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.
 - c) „Übermittlungsfehler“: Die *Abfrage-Datei* wurde entweder an den falschen Verpflichteten oder von der falschen Stelle der BAFin gesendet. Die Abfrage wird durch die Abfragekomponente des Verpflichteten nicht weiter bearbeitet. Eine nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.
 - d) „Inhaltsfehler“: In der *Abfrage-Datei* wird eine unzulässige Abfrage spezifiziert. Die Abfrage wird durch die Abfragekomponente des Verpflichteten nicht weiter bearbeitet. Nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.
 - e) „Parameterfehler“: In der *Abfrage-Datei* werden unzulässige *Abfrage-Steuerungsdaten* angegeben (z.B. *Abfrage-maximale-Anzahl-Kontodatensätze* ist kleiner als 0). Die Abfrage wird durch die Abfragekomponente des Verpflichteten nicht weiter bearbeitet. Nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.
 - f) „Schlüsselfehler“: Für die Erzeugung der *Abfrage-Datei* wurde ein anderer Schlüssel *Abfrage-Key-ID* verwendet, als für den Import der Daten in die Abfragekomponente des Verpflichteten. Die Abfrage wird durch die Abfragekomponente des Verpflichteten nicht weiter bearbeitet. Der Schlüssel *Daten-Key-ID*, der für den Import der Daten verwendet wurde, wird in der *Abfrage-Ergebnisstatistik* angegeben.
 - g) „Temporärer Systemfehler“: Abfrage wird durch die Abfragekomponente des Verpflichteten zu einem späteren Zeitpunkt weiter bearbeitet. Nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.
 - h) „Permanenter Systemfehler“: Abfrage kann durch die Abfragekomponente des Verpflichteten nicht weiter bearbeitet werden. Nähere Beschreibung erfolgt in *Abfrage-Fehlerbeschreibung*.

Die *Abfrage-Fehlerbeschreibung* ermöglicht den Verpflichteten, eine frei formulierte textuelle Präzisierung oder Erläuterung des Fehlers anzugeben.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

5.1.4 Steuerungsdaten für die Abfrage bei den Verpflichteten (*Abfrage-Steuerungsdaten*)

- (1) Zur Steuerung der Abfragen bzgl. Datentransfer und Abfragelogik werden in den Abfragen der BAFin folgende *Abfrage-Steuerungsdaten* übertragen:
 - a) Versionsnummer des technischen Abfrageverfahrens (*Abfrage-Version*)
 - b) Kennung der abfragenden Stelle der BAFin (*Abfragestellen-ID*)
 - c) Maximale Anzahl der Kontodatensätze, die vom Verpflichteten in der *Abfrage-Ergebnis-Datei* zurückgegeben werden sollen (*Abfrage-maximale-Anzahl-Kontodatensätze*). Falls die Anzahl der passenden Kontodatensätze *Abfrage-maximale-Anzahl-Kontodatensätze* übersteigt, werden keine Kontodatensätze sondern lediglich die Anzahl der Treffer zurückgegeben.
 - d) Minimales Maß der Übereinstimmung zwischen Anhaltsdaten und zu suchenden Kontodatensätzen (*Abfrage-minimale-Übereinstimmung-Namen*).
- (2) Die *Abfrage-Steuerungsdaten* sind immer in den *Abfrage-Bestätigungen* und den *Abfrage-Ergebnis-Dateien* zurück zu übertragen.
- (3) Zur Steuerung der Abfragen bzgl. Datentransfer und Abfragelogik sind durch den Verpflichteten in der **Abfragekomponente** folgende *Abfrage-Parameterdaten* vorzuhalten:
 - a) Versionsnummer des technischen Abfrageverfahrens (*Abfrage-Versionsparameter*)
 - b) Die Kennung des bei der Verschlüsselung der importierten Kontodatensätze verwendeten Schlüssels *Daten-Key-ID*

Die *Abfrage-Version* unterstützt die robuste Anpassung des Abfrageverfahrens bei den Verpflichteten für den Fall technischer Modifikationen.

Evtl. können zukünftig verschiedene Stellen der BAFin bei den Verpflichteten abfragen. Um die Versendung der Abfrage-Ergebnisse steuern zu können wird vorsorglich die *Abfragestellen-ID* eingeführt.

Abfrage-maximale-Anzahl-Kontodatensätze und *Abfrage-minimale-Übereinstimmung-Namen* dienen dazu, den Abruf nicht benötigter oder offensichtlich nicht plausibler Daten von vornherein zu vermeiden. Durch die Einführung dieser Parameter können die Abfragen flexibel von der BAFin gesteuert werden.

Der *Abfrage-Versionsparameter* ermöglicht es der BAFin festzustellen, auf welchem Versionsstand die Abfragekomponenten der Verpflichteten sind.

5.1.5 Ergebnisdaten für Abfragen

- (1) Ergebnisdaten für Abfragen sind wie folgt definiert:
 - a) Anzahl der anhand der Abfrage gefundenen Kontodatensätze (*Abfrage-Trefferzahl*).
 - b) Anzahl der vom Verpflichteten im Ergebnis übermittelten Abfrage Kontodatensätze (*Abfrage-Anzahl-Kontodatensätze*). Diese kann von *Abfrage-Trefferzahl* abweichen (z.B. wenn ein Schwellwert überschritten wurde).
 - c) *Ergebnis-Kontodatensätze* mit den abzurufenden Daten als *Abfrage-Ergebnisdaten*

5.2 Technische Definition der Daten

Im folgenden werden die für das technische Auskunftsverfahren wesentlichen Daten bzgl. der technischen Darstellung spezifiziert. Zu den XML-Dateien stellt die BAFin eine Document-Type-Definition (DTD) und Beispiel-Dateien zur Verfügung.

5.2.1 Technische Definition der Datenobjekte

5.2.1.1 *Kontodatensatz, Abruf-Kontodatensatz, Ergebnis-Kontodatensatz, Import-Kontodatensatz-Datei, Abruf-Kontodatensatz-Datei*

(1) Ein *Kontodatensatz* besteht aus folgenden Daten:

- *Konto-Nummer*
- *Einrichtungsdatum*
- *Auflösungsdatum*
- *Kontostammdatensätze* (evtl. mehrere)
 - *Inhaber* (evtl. mehrere)
 - *Inhaber-Nachname*
 - *Inhaber-Vorname*
 - *Inhaber-Geburtsdatum*
 - *VB* (evtl. mehrere)
 - *VB-Nachname*
 - *VB-Vorname*
 - *VB-Geburtsdatum*
 - *WB* (evtl. mehrere)
 - *WB-Nachname*
 - *WB-Vorname*
 - *WB-Anschrift*
 - *Datensatz-Gültigkeitsbeginn*
 - *Datensatz-Gültigkeitsende*

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

(2) Ein Import-Kontodatensatz ist ein Kontodatensatz, der aus den Quelldatenbanken des Verpflichteten in die Datenbank der Abfragekomponente zu importieren ist. Er besteht aus folgenden Daten:

- Kontodatensatz
- Verpflichteten-ID

Die Verpflichteten-ID ist speziell für die Realisierung mandantenfähiger Abfragekomponenten relevant.

(3) Ein *Abruf-Kontodatensatz* ist ein für die Vergleichsoperationen der Abfragelogik vorbereiteter *Kontodatensatz mit verschlüsselten Feldinhalten*. Er besteht aus folgenden Daten:

- *Konto-Nummer*
- *Index-Konto-Nummer*
- *Verpflichteten-Id*
- *Einrichtungsdatum*
- *Auflösungsdatum*
- *Kontostammdatensätze* (evtl. mehrere)
 - *Inhaber* (evtl. mehrere)
 - *Inhaber-Nachname*
 - *Index-Inhaber-Nachname*
 - *Inhaber-Vorname*
 - *Index-Inhaber-Vorname*
 - *Inhaber-Geburtsdatum*
 - *VB* (evtl. mehrere)
 - *VB-Nachname*
 - *Index-VB-Nachname*
 - *VB-Vorname*
 - *Index-VB-Vorname*
 - *VB-Geburtsdatum*
 - *WB* (evtl. mehrere)
 - *WB-Nachname*
 - *Index-WB-Nachname*
 - *WB-Vorname*
 - *Index-WB-Vorname*
 - *WB-Anschrift*
 - *Index-WB-Anschrift*
 - *Datensatz-Gültigkeitsbeginn*
 - *Datensatz-Gültigkeitsende*

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- *Datensatz-Gültigkeitsende_plain*
- *Datensatz-Hash*

Datensatz-Gültigkeitsende_plain wird unverschlüsselt in den Abruf-Kontodatensätzen gespeichert. Es ist für die Löschung historischer Daten nach der Aufbewahrungsfrist erforderlich.

- (4) Ein *Ergebnis-Kontodatenatz* ist ein aus der Datenbank der Abfragekomponente abgerufener *Kontodatenatz* mit verschlüsselten Feldern. Er besteht aus folgenden Daten:
 - *Kontodatenatz*
 - *Datensatz-Hash*
- (5) Die *Import-Kontodatenatz-Datei* fasst die zu importierenden *Kontodatenätze* als XML-Datei zusammen. Die *Import-Kontodatenatz-Datei* kann direkt als Input für **DataCrypt** verwendet werden.
- (6) Die *Abruf-Kontodatenatz-Datei* fasst die *Abruf-Kontodatenätze* als Output von **DataCrypt** als XML-Datei zusammen. Die *Abruf-Kontodatenatz-Datei* kann für den Import in die Datenbank der **Abfragekomponente** verwendet werden.

5.2.1.2 Abfrage-Dateien, Konsistenz der Abfrage-Anhaltsdaten

- (1) Die von der BAFin an einen Verpflichteten gesendete *Abfrage-Datei* fasst die *Abfrage-Musterdaten* und die *Abfrage-Verwaltungsdaten* des Verpflichteten für beliebig viele Abfragen als eine XML-Datei zusammen.
- (2) Der Dateiname einer *Abfrage-Datei* wird wie folgt gebildet: „QRY_<Verpflichteten-ID>_<Abfrage-Zähler>.xml“ (Beispiel: „QRY_0815_4711.xml“).
- (3) Als Kombinationen der Felder der *Abfrage-Anhaltsdaten* sind nur diejenigen sinnvoll, die für jedes Kontodatenfeld maximal eine Vorgabe machen.

Beispiele:

- {*Auswahl-Nachname, Auswahl-Vorname*}: sinnvoll
 - {*Auswahl-Name, Auswahl-Nachname, Auswahl-Vorname*}: nicht sinnvoll
 - {*Auswahl-Name, Auswahl-VB-Name, Auswahl-WB-Name*}: nicht sinnvoll
- (4) Die minimal vorzugebenden Anhaltsdatenfelder werden auf Grund des Datenschutzes wie folgt vorgegeben: Mindestens sind entweder ein Namensfeld (*Auswahl-Inhaber-Nachname, Auswahl-Inhaber-Name, Auswahl-VB-Nachname, Auswahl-VB-Name, Auswahl-WB-Nachname, Auswahl-WB-Name, Auswahl-Nachname* oder *Auswahl-Name*) oder *Auswahl-Konto-Nummer* anzugeben.
- *Abfrage-Verwaltungsdaten* (pro Verpflichtetem)
 - *Verpflichteten-ID*
 - *Abfragekennung*
 - *Abfrage-Key-ID*

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- *Abfrage-Musterdaten*
 - *Abfrage-Steuerungsdaten*
 - *Abfrage-Version*
 - *Abfragestellen-ID*
 - *Abfrage-maximale-Anzahl-Kontodatensätze*
 - *Abfrage-minimale-Übereinstimmung-Namen*
 - *Abfrage-Anhaltsdaten*
 - *Auswahl-Konto-Nummer*
 - *Auswahl-Einrichtungsdatum*
 - *Auswahl-Auflösungsdatum*
 - *Auswahl-Inhaber-Nachname*
 - *Auswahl-Inhaber-Vorname*
 - *Auswahl-Inhaber-Name*
 - *Auswahl-Inhaber-Geburtsdatum*
 - *Auswahl-VB-Nachname*
 - *Auswahl-VB-Vorname*
 - *Auswahl-VB-Name*
 - *Auswahl-VB-Geburtsdatum*
 - *Auswahl-WB-Nachname*
 - *Auswahl-WB-Vorname*
 - *Auswahl-WB-Anschrift*
 - *Auswahl-WB-Name*
 - *Auswahl-Nachname*
 - *Auswahl-Vorname*
 - *Auswahl-Name*
 - *Auswahl-Geburtsdatum*

Verfahren zum automatisierten Abruf von Kontoinformationen
Schnittstellenspezifikation BAFin - Kreditinstitute

5.2.1.3 Abfrage-Ergebnisse, Abfrage-Bestätigungs-Datei, Abfrage-Trefferzahl-Datei, Abfrage-Ergebnis-Datei

- (1) Die von einem Verpflichteten gesendete *Abfrage-Bestätigungs-Datei* fasst die *Abfrage-Verwaltungsdaten* des Verpflichteten, die *Abfrage-Steuerungsdaten* und die *Abfrage-Empfangsbestätigung* für eine oder mehrere Abfragen als XML-Datei zusammen.
 - (2) Der Dateiname einer *Abfrage-Bestätigungs-Datei* wird wie folgt gebildet: „ACK_<Verpflichteten-ID>_<Abfrage-Zähler>.xml“ (Beispiel: „ACK_0815_4711.xml“). Dabei sind *Verpflichteten-ID* und *Abfrage-Zähler* dem Dateinamen der zugehörigen *Abfrage-Datei* zu entnehmen.
 - (3) Die von einem Verpflichteten gesendete *Abfrage-Trefferzahl-Datei* fasst die *Abfrage-Verwaltungsdaten* des Verpflichteten, die *Abfrage-Steuerungsdaten* und die *Abfrage-Ergebnisstatistik* für eine Abfrage als XML-Datei zusammen.
 - (4) Der Dateiname einer *Abfrage-Trefferzahl-Datei* wird wie folgt gebildet: „CNT_<Verpflichteten-ID>_<Abfrage-Zähler>_<Abfrage-Kennung>.xml“ (Beispiel: „CNT_0815_4711_65536.xml“). Dabei sind *Verpflichteten-ID* und *Abfrage-Zähler* dem Dateinamen der zugehörigen *Abfrage-Datei*, *Abfrage-Kennung* der zugehörigen Abfrage zu entnehmen.
 - (5) Die von einem Verpflichteten gesendete *Abfrage-Ergebnis-Datei* fasst die *Abfrage-Verwaltungsdaten* des Verpflichteten, die *Abfrage-Steuerungsdaten*, die *Abfrage-Ergebnisstatistik* und die *Abfrage-Ergebnisdaten* für genau eine Abfrage als XML-Datei zusammen.
 - (6) Der Dateiname einer *Abfrage-Ergebnis-Datei* wird wie folgt gebildet: „RES_<Verpflichteten-ID>_<Abfrage-Zähler>_<Abfrage-Kennung>.xml“ (Beispiel: „RES_0815_4711_65536.xml“). Dabei sind *Verpflichteten-ID* und *Abfrage-Zähler* dem Dateinamen der zugehörigen *Abfrage-Datei*, *Abfrage-Kennung* der zugehörigen Abfrage zu entnehmen.
- *Abfrage-Empfangsbestätigung*
 - *Abfrage-Fehlercode* („Kein Fehler“, „Syntaxfehler“, „Übermittlungsfehler“, „Inhaltsfehler“, „Parameterfehler“, „Schlüsselfehler“, „Temporärer Systemfehler“, „Permanenter Systemfehler“)
 - *Abfrage-Fehlerbeschreibung*
 - *Abfrage-Ergebnisstatistik*
 - *Abfrage-Trefferzahl*
 - *Abfrage-Anzahl-Kontodatensätze*
 - *Abfragezähler*
 - *Abfrage-Versionsparameter*
 - *Daten-Key-ID*
 - *Gesamt-Anzahl-Kontodatensätze*
 - *Datenaktualisierungszeitpunkt*
 - *Datenaktualisierungsart* („Full“ / „Incremental“)
 - *Abfrage-Ergebnisdaten*
 - Gefundene *Kontodatensätze* gemäß Abschnitt 5.2.1.1 (*Ergebnis-Kontodatensätze*, evtl. mehrere)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

5.2.2 Klassifikation gleichartiger Datenfelder

Dieser Abschnitt fasst Datenfelder zu Datenfeldklassen zusammen, deren Mitglieder bzgl. der Formatierung und Verarbeitung gleich zu behandeln sind.

(1) Folgende Datenfelder gehören zur Klasse *Datumsfelder*:

- *Auswahl-Einrichtungsdatum*
- *Auswahl-Auflösungsdatum*
- *Auswahl-Inhaber-Geburtsdatum*
- *Auswahl-VB-Geburtsdatum*
- *Auswahl-Geburtsdatum*
- *Datensatz-Gültigkeitsbeginn*
- *Datensatz-Gültigkeitsende*
- *Datensatz-Gültigkeitsende_plain*

(2) Folgende Datenfelder gehören zur Klasse *Namensfelder*

- *Inhaber-Nachname*
- *Inhaber-Vorname*
- *VB-Nachname*
- *VB-Vorname*
- *WB-Nachname*
- *WB-Vorname*
- *WB-Anschrift*

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

(3) Folgende Datenfelder gehören zur Klasse *Auswahl-Namensfelder*:

- *Auswahl-Inhaber-Nachname*
- *Auswahl-Inhaber-Vorname*
- *Auswahl-Inhaber-Name*
- *Auswahl-VB-Nachname*
- *Auswahl-VB-Vorname*
- *Auswahl-VB-Name*
- *Auswahl-WB-Nachname*
- *Auswahl-WB-Vorname*
- *Auswahl-WB-Anschrift*
- *Auswahl-WB-Name*
- *Auswahl-Nachname*
- *Auswahl-Vorname*
- *Auswahl-Name*

(4) Folgende Datenfelder gehören zur Klasse *Index-Namensfelder*

- *Index-Inhaber-Nachname*
- *Index-Inhaber-Vorname*
- *Index-VB-Nachname*
- *Index-VB-Vorname*
- *Index-WB-Nachname*
- *Index-WB-Vorname*
- *Index-WB-Anschrift*

Verfahren zum automatisierten Abruf von Kontoinformationen

Schnittstellenspezifikation BAFin - Kreditinstitute

5.2.3 Formate der Datenfelder

Datenfelder sind alle Daten gemäß Abschnitt 5.2.1, die selbst keine weiteren Datenelemente enthalten.

- (1) *Datumfelder* müssen in unverschlüsselter Form ein Format gemäß ISO-8601 aufweisen: „JJJ-MM-TT“ (JJJJ: Kalenderjahr inkl. Jahrtausend; MM: Kalendermonat, ggf. mit führender „0“; TT: Kalendertag, ggf. mit führender „0“) (Beispiele: „2002-08-16“; „1999-12-04“).
- (2) Angaben zu Datum und Uhrzeit sind immer bezogen auf GMT zu speichern (MEZ = GMT + 1 Stunde).
- (3) Die Verpflichteten-ID ist die BAKNr., die aus 6 Ziffern besteht.
- (4) Die *Auswahl-Namensfelder* in den *Abfrage-Anhaltsdaten* enthalten die aus den korrespondierenden Feldern der Anfrage-Anhaltsdaten extrahierten **Tokenlisten** mit normalisierte und einzeln verschlüsselten **Token**. Die verschlüsselten **Token** wurden mit Hilfe der Base64-Transformation auf druckbare Zeichen abgebildet.
- (5) Die *Index-Namensfelder* in den *Abruf-Kontodatensätzen* enthalten die aus den korrespondierenden Feldern der *Kontodatensätze* extrahierten **Tokenlisten** mit normalisierten und einzeln verschlüsselten **Token**. Die verschlüsselten **Token** wurden mit Hilfe der Base64-Transformation auf druckbare Zeichen abgebildet.
- (6) Für **Token** sind Zeichenketten variabler Länge mit einer maximalen Länge von 200 Zeichen vorzusehen.
- (7) Für alle sonstigen Felder sind Zeichenketten variabler Länge mit einer maximalen Länge von 200 Zeichen vorzusehen.

5.3 Verwendung der Daten für die Abfrage-Bearbeitung

5.3.1 Input-Daten

- (1) Alle Input-Daten für die **Abfrage-Bearbeitung** werden über folgende Dateien zugeführt:
 - a) *Import-Kontodatensatz-Datei*
 - b) *Abfrage-Datei*
 - a) Schlüsseldateien **DataCrypt**: Die Schlüsseldateien für **DataCrypt** werden den Verpflichteten in elektronischer Form von der BAFin übermittelt.
 - b) **Test-Kontoinformationen**: *Import-Kontodatensatz-Dateien* mit durch die BAFin vorgegebenen Testdaten.

5.3.2 Systemdaten

- (1) In der **Abfragekomponente** sind folgende Daten permanent vorzuhalten und fortzuschreiben:
 - a) *Abfragezähler*
 - b) *Abfrage-Versionsparameter*
 - c) *Daten-Key-ID*
 - d) *Gesamt-Anzahl-Kontodatensätze*
 - e) *Datenaktualisierungszeitpunkt*
 - f) *Datenaktualisierungsart* („Full“ / „Incremental“)

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (2) Folgende temporären Daten in der **Abfragekomponente** sind nach Verwendung zu löschen:
- a) *Abruf-Kontodatensatz-Datei*
 - b) Alle Dateien die Abfragen betreffen

5.3.3 Output-Daten

- (1) Alle Output-Daten der **Abfrage-Bearbeitung** werden in den folgenden Dateien transferiert:
- a) *Abfrage-Bestätigungs-Datei*
 - b) *Abfrage-Trefferzahl-Datei*
 - c) *Abfrage-Ergebnis-Datei*

6 Prozess-Beschreibung

6.1 Rollen

- (1) Der Verpflichtete übermittelt der BAFin die personellen Belegungen der Rollen sowie alle für eine unverzügliche Kontaktaufnahme erforderlichen Daten. Dies sind im einzelnen:
 - a) Rolle im § 24c-Auskunftsverfahren (Administrator Abfragekomponente, etc.)
 - b) Abteilung (IT, Rechenzentrum, Geldwäsche, etc.)
 - c) Anrede
 - d) Titel
 - e) Namenszusatz
 - f) Nachname
 - g) Vorname
 - h) Position (Organigramm)
 - i) Funktion (fachlich)
 - j) Telefon 1
 - k) Telefon 2
 - l) Fax
 - m) E-Mail

6.1.1 BAFin

Die **BAFin** gibt alle technischen und organisatorischen Anforderungen bzgl. des Auskunftsverfahrens vor, welche die Schnittstelle der BAFin zu den Verpflichteten betreffen. Weiterhin stellt die **BAFin** Verfahrensparameter zur Verfügung, welche die Netzwerkverbindung, die kryptographischen Mechanismen und die Abfragelogik betreffen.

6.1.2 Betreiber

- (1) **Betreiber Abfragekomponente** ist in der Regel der Verpflichtete. Falls dieser die **Abfragekomponente** durch einen Dritten betreiben lässt (Fremdbetrieb, z.B. in einem Rechenzentrum), dann ist dieser Dritte der **Betreiber Abfragekomponente**. Auch in diesem Fall ist letztendlich der Verpflichtete verantwortlich für alle Aspekte des Auskunftsverfahrens.

6.1.3 Administrator Abfragekomponente des Verpflichteten

- (1) Der **Administrator Abfragekomponente** ist zuständig für den regulären Betrieb, die Wartung und die Störungsbehebung der System-Komponenten. Ausgenommen ist ggf. **Firewall / VPN-Gateway Abfrage-Zugang**, das im wesentlichen von der **BAFin** administriert wird.
- (2) Der **Administrator Abfragekomponente** ist im Falle des Fremdbetriebs der **Abfragekomponente** der zuständige Administrator des **Betreibers Abfragekomponente**.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

6.1.4 Technisch Verantwortlicher des Verpflichteten

- (1) Der **technisch Verantwortliche** des Verpflichteten ist verantwortlich für alle technischen Aspekte des Auskunftsverfahrens bzgl. der System-Komponenten. Ausgenommen ist ggf. **Firewall / VPN-Gateway Abfrage-Zugang**, das im wesentlichen von der **BAFin** administriert wird.
- (2) Der **technisch Verantwortliche** kann im Falle des Fremdbetriebs der **Abfragekomponente** der zuständige Verantwortliche des **Betreibers Abfragekomponente** sein (z.B. Leiter des Rechenzentrums).

6.1.5 Verfahrensverantwortlicher des Verpflichteten

- (1) Der **Verfahrensverantwortliche** des Verpflichteten ist verantwortlich für alle Aspekte des Auskunftsverfahrens (technisch, fachlich, etc.).

6.1.6 Datenschutzbeauftragter des Verpflichteten

- (1) Der **Datenschutzbeauftragte** (DSB) des Verpflichteten ist verantwortlich für alle Aspekte des Auskunftsverfahrens, die den Schutz personenbezogener Daten betreffen.

6.2 Organisatorische Abläufe

Mit System-Komponenten sind im folgenden die System-Komponenten beim **Betreiber Abfragekomponente** gemeint.

6.2.1 Einrichtung der System-Komponenten

- (1) Die Einrichtung der System-Komponenten liegt in der Verantwortung des **Administrators Abfragekomponente**.
- (2) Der **Administrator Abfragekomponente** stimmt alle technischen Parameter mit der **BAFin** ab und ist für die Konfiguration der System-Komponenten gemäß den Anforderungen und Vorgaben der **BAFin** verantwortlich.
- (3) Der **Administrator Abfragekomponente** ist verantwortlich für die korrekte Einrichtung des regelmäßigen Imports der Kontoinformationen.
- (4) Der **Administrator Abfragekomponente** ist verantwortlich für die Einrichtung einer regelmäßige Sicherung der für eine Wiederherstellung des Betriebs erforderlichen Daten.
- (5) Der **Administrator Abfragekomponente** ist verantwortlich für die Initiierung der Integrations- und Abnahmetests mit der **BAFin**. Die **BAFin** unterstützt ihn hierbei.

6.2.2 Betrieb

- (1) Der technische Betrieb der System-Komponenten liegt in der Verantwortung des **Administrators Abfragekomponente**.
- (2) Der **Administrator Abfragekomponente** ist verantwortlich für die Überwachung und Aufrechterhaltung des Betriebs der System-Komponenten.
- (3) Der **Administrator Abfragekomponente** ist verantwortlich für die Überwachung des regelmäßigen Imports der Kontoinformationen.
- (4) Der **Administrator Abfragekomponente** ist verantwortlich für die Überwachung der regelmäßige Sicherung der für eine Wiederherstellung des Betriebs erforderlichen Daten.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

6.2.3 Störungsbehebung

6.2.3.1 Meldung und Eskalation einer Störung durch die BAFin

- (1) Falls die **BAFin** Störungen in den Systemkomponenten feststellt, dann meldet sie diese dem **Administrator Abfragekomponente** unverzüglich nach bekannt werden.
- (2) Ziel einer Eskalation der Störungsbearbeitung ist es, dass der Verpflichtete weitere Schritte zur Behebung der Störung einleitet. Eine Eskalation erfolgt, wenn der Ansprechpartner des Verpflichteten nicht erreicht werden kann oder abzusehen ist, dass zur Behebung der Störung weiterführende Maßnahmen erforderlich sind. Die **BAFin** eskaliert an folgende weiteren Ansprechpartner des Verpflichteten:
 - a) **technisch Verantwortlicher**
 - b) **Verfahrensverantwortlicher** des Verpflichteten
 - c) **Geschäftsleitung** des Verpflichteten
- (3) Nach Abschluss der Störungsbehebung meldet der **Administrator Abfragekomponente** der BAFin die Wiederaufnahme des regulären Betriebs.

6.2.3.2 Maßnahmen zur Störungsbehebung

- (1) Der **Administrator Abfragekomponente** ist verantwortlich für die unverzügliche Wiederherstellung des regulären Betriebs im Falle eine Störung der System-Komponenten beim Verpflichteten. Die **BAFin** unterstützt ihn soweit möglich bei der Störungsanalyse und durch Senden von Testabfragen.
- (2) Während der Störungsbehebung ist jederzeit sicherzustellen, dass die Vertraulichkeit der Abfragen und der Kontoinformationen gewahrt bleibt. Bei einem Austausch von System-Komponenten sind ggf. darauf gespeicherte vertrauliche Daten zuverlässig zu löschen.

6.2.4 Wartung

- (1) Der **Administrator Abfragekomponente** stimmt alle technischen Parameter mit der **BAFin** ab und ist für die Konfiguration der System-Komponenten gemäß den Anforderungen und Vorgaben der **BAFin** verantwortlich.
- (2) In der Regel sind Wartungsarbeiten so durchzuführen, dass der reguläre Betrieb nicht beeinträchtigt wird. Insbesondere müssen die geforderten Antwortzeiten eingehalten werden.
- (3) Nach einer Änderung der Konfiguration der System-Komponenten (z.B. Schlüsselwechsel, Software-Updates) muss der **Administrator Abfragekomponente** die korrekte Funktion der System-Komponenten testen. Die **BAFin** unterstützt ihn soweit möglich und erforderlich durch Senden von Testabfragen.
- (4) Der **Administrator Abfragekomponente** hat die Konsistenz der in der **Abfragekomponente** vorgehaltenen Kontoinformationen ggf. durch regelmäßiges Neuladen sicherzustellen. Auch während des Neuladens müssen die Kontoinformationen für Abfragen verfügbar sein.
- (5) Der **Administrator Abfragekomponente** ist verantwortlich für die Durchführung von Schlüsselwechseln für das Modul **DataCrypt**, Secure-Copy und das VPN-Gateway. Die neuen Schlüssel werden von der **BAFin** in elektronischer Form zur Verfügung gestellt.
- (6) Nach einem Schlüsselwechsel für das Modul **DataCrypt** sind die Kontoinformationen ab dem von der **BAFin** vorgegebenen Zeitpunkt mit dem neuen Schlüssel verschlüsselt in der **Abfragekomponente** vorzuhalten. Ab diesem Zeitpunkt ist die *Daten-Key-ID* zu aktualisieren.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (7) Nach einer Aktualisierung der Software der **Abfragekomponente** muss die vorgehaltene Versionsnummer des technischen Abfrageverfahrens (*Abfrage-Versionsparameter*) für die *Abfrage-Ergebnisstatistiken* ggf. aktualisiert werden:

7 Nicht funktionale Anforderungen (normativ)

7.1 Mengengerüst

- (1) Die Systemkomponenten des Verpflichteten, welche das Auskunftsverfahren betreffen, sind so auszulegen, dass die geforderten Performanz ausreichend ist für eine Bearbeitung von durchschnittlich 10.000 Abfragen pro Woche. Die Systemkomponenten müssen hochskaliert werden können, da durch die Spezifikation einer „datenbanklogischen Black Box“ nur Abfragen mit exaktem, vollständigem Suchmuster möglich sind. Evtl. notwendige Abfragen mit Unschärfen (z.B. auf Grund von Transkriptionsvarianten in kyrillisch geschriebenen Namen) sind daher nur durch Einzelabfrage aller möglichen Varianten möglich. Dies kann dazu führen, dass aus einer einzelnen Suche eine Vielzahl von Einzelabfragen an die Abfragekomponente resultieren. Eine ausreichende Auslegung der Abfragekomponente stellt sicher, dass auch in Einzelfällen hoher Spitzenlast, die maximal erlaubte durchschnittliche und die maximale Antwortzeit eingehalten werden können. Eine ausreichende Auslegung der Abfragekomponente sichert auch unter Berücksichtigung der erstgenannten Punkte einen ausreichenden Abstand zu den tatsächlichen Anforderungen. Eine grundsätzliche Auslegung auf höhere Skalierbarkeit sichert die Verpflichteten zusätzlich ab. Für Auslegung der Komponenten zur Datenübertragung kann mit einer zu übertragenen Datenmenge von ca. 2 KB pro Abfrage (ohne Treffer) gerechnet werden. Hierfür sollte in der ersten Betriebsphase des Auskunftsverfahrens ein ISDN-Basisanschluss mit 2 B-Kanälen ausreichend sein.
- (2) Alle Anforderungen, die das Mengengerüst betreffen, sind je Verpflichtetem zu interpretieren. Abfragekomponenten, die das Auskunftsverfahren für mehrere Verpflichtete implementieren (mandantenfähige Abfragekomponenten), müssen gemäß der Anzahl der Mandanten ausgelegt werden.

7.2 Performanz

- (1) **Bestätigungszeit** ist die Zeitdauer vom Empfang der *Abfrage-Datei* bis zum erfolgreichen Versenden der *Abfrage-Bestätigungs-Datei* durch den Verpflichteten. Die **Bestätigungszeit** darf im jährlichen Durchschnitt höchstens 30 Minuten betragen.
- (2) **Antwortzeit** ist die Zeitdauer vom Empfang der Abfrage-Datei bis zum erfolgreichen Versenden der Abfrage-Trefferzahl-Datei durch den Verpflichteten. Die **Antwortzeit** darf im jährlichen Durchschnitt höchstens 30 Minuten betragen. Die **Antwortzeit** darf höchstens 12 Stunden betragen (**maximale Antwortzeit**).

7.3 Datenaktualität

- (1) Geänderte Kontoinformationen muss der Verpflichtete spätestens im Anschluß an die „End-of-Day“ Datenverarbeitung der Banksysteme, in zu begründenden Ausnahmen bis spätestens um 24:00 am Tag nach der Änderung in der Abfragekomponente bereitstellen.
- (2) Seitens der Verpflichteten sind nicht nur die jeweils aktuellen Kontoinformationen, sondern auch historische Kontoinformationen drei Jahre vorzuhalten. Historische Kontoinformationen sind tagesgenau drei Jahre nach *Datensatz-Gültigkeitsende* für geänderte Kontodaten bzw. drei Jahre nach *Auflösungsdatum* für den gesamten Kontodatensatz zu löschen.

7.4 Verfügbarkeit

- (1) Das Empfangen und Bearbeiten von Abfragen muss seitens des Verpflichteten jederzeit (24 Stunden täglich) möglich sein. Dies gilt insbesondere auch während der Aktualisierung der Kontoinformationen durch den Verpflichteten. Die Verfügbarkeit muss im jährlichen Durchschnitt fortlaufend mindestens 99% betragen. Dies entspricht einer maximalen Ausfallzeit

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

von 3,65 Tagen pro Jahr. Bei der Berechnung der Verfügbarkeit werden Ausfallzeiten der Systeme der BAFin nicht mit einbezogen.

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

- (2) Die Systeme des Verpflichteten, welche das Auskunftsverfahren betreffen, sind durch den Verpflichteten fortlaufend zu überwachen. Dies betrifft insbesondere folgende Komponenten:
 - a) Netzwerkzugang
 - b) Systemplattform (Hardware und Betriebssystem) der Abfragekomponente
 - c) Zustand der Applikation zur Abfragebearbeitung
 - d) Datenaktualisierung
- (3) Störungen in den Systemen des Verpflichteten, welche das Auskunftsverfahren betreffen sind so schnell zu beheben, dass die maximale Antwortzeit nicht überschritten wird.
- (4) Wartungsarbeiten an den Systemen des Verpflichteten, welche das Auskunftsverfahren betreffen, sind der BAFin mindestens einen Geschäftstag im Voraus zu melden. Ein diesbezüglicher Ansprechpartner bei der BAFin wird den Verpflichteten rechtzeitig benannt.

7.5 Sicherheitsanforderungen

7.5.1 Zugriffsschutz

- (1) Als Sicherheitsniveau für den Zugriffsschutz der für das Auskunftsverfahren relevanten System-Komponenten ist mindestens eine Umsetzung des IT-Grundschutzhandbuches [02.GHB] erforderlich.

7.5.2 Datensicherheit

- (1) Als Sicherheitsniveau für die allgemeine Datensicherheit, insbesondere in Bezug auf personenbezogene Daten, ist mindestens eine Umsetzung des IT-Grundschutzhandbuches [02.GHB] erforderlich.

7.5.3 Datenkonsistenz

- (1) Die Konsistenz der Kontoinformationen ist durch den Verpflichteten jederzeit sicherzustellen.

7.6 Rechtliche Restriktionen

- (1) Die Verpflichteten haben jederzeit die Anforderungen des Bundesdatenschutzgesetzes zu beachten.
- (2) Bei den Verpflichteten dürfen auf Grund der Vorgaben des § 24c KWG folgende Daten in keinem Fall protokolliert oder auf sonstige Weise zugänglich gemacht werden:
 - a) bei der Abfrage angegebene Daten (d.h. während der Durchführung einer Abfrage von der BAFin zum Verpflichteten transferierte Daten)
 - b) Abfrageergebnisse (d.h. während der Durchführung einer Abfrage von dem Verpflichteten zur BAFin zu transferierende Daten oder transferierte Daten sowie Zwischenergebnisse)

7.7 Systemarchitektur

Bzgl. der Systemarchitektur werden keine speziellen Vorgaben gemacht. Die Verschlüsselungs-Software **DataCrypt** für die datenbanklogische Blackbox wird durch die BAFin für folgende Systemezur Verfügung gestellt: MS Windows, Solaris, AIX, Linux, HP-UX.

7.8 Netzwerkarchitektur

Bzgl. der Netzwerkarchitektur werden über die Anforderungen aus Kapitel 3 hinaus keine weiteren Vorgaben gemacht. Insbesondere liegt die Anbindung der internen Systeme des Verpflichteten an die Abfragekomponente für die Datenaktualisierung allein in der Verantwortung des Verpflichteten.

7.9 Systemtests

7.9.1 Integrationstest durch die BAFin

- (1) Für die Inbetriebnahme der Abfragesysteme können seitens der BAFin folgende Tests durchgeführt werden, die der Verpflichtete angemessen unterstützen muss:
- a) Penetrationstest: Prüfung der System-Komponenten auf allgemeine Schwachstellen
 - b) Test der Datei-Übertragung über das Transfernetz-1
 - c) Test der Datei-Übertragung über das Transfernetz-2 (Fallback)
 - d) Test Abfrage mit unverschlüsselten Daten
 - e) Test-Abfrage mit verschlüsselten Daten
 - f) Schlüsselwechsel und Test-Abfrage mit verschlüsselten Daten
 - g) Test der Abfragelogik durch Testreihe mit Test-Abfragen auf einer Testdatenbank. Die Testdatensätze werden durch die BAFin in elektronischer Form vorgegeben.

7.9.2 Tests im laufenden Betrieb durch die BAFin

- (1) Im laufenden Betrieb werden seitens der BAFin folgende Tests durchgeführt, die der Verpflichtete angemessen unterstützen muss:
- a) Verfügbarkeits-Test durch Test-Abfrage auf Test-Datensatz. Die Testdatensätze werden durch die BAFin in elektronischer Form vorgegeben. Hierfür muss der Verpflichtete 10 beliebige Kontonummern reservieren und der BAFin mitteilen. Die 10 Kontonummern dürfen nicht für reale Konten verwendet werden. Test-Daten zu diesen Kontonummern sind ausdrücklich *nicht* durch die Verpflichteten bereitzustellen.
 - b) Teile des Integrationstests bei Änderungen der Systemkonfiguration.

7.9.3 Weitere Tests

Tests des Imports und Penetrationstests seiner internen System liegen in der Verantwortung des Verpflichteten.

8 Anhang

8.1 Document-Type-Definition (DTD)

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- DTD fuer Auskunftersuchen gemaess § 24c KWG (Bundesanstalt fuer
Finanzdienstleistungsaufsicht, BAFIN) -->

<!ELEMENT abfrage-anhaltsdaten (indexfeld+)>
<!ELEMENT abfrage-anzahl-kontodatensaetze (#PCDATA)>
<!ELEMENT abfrage-bestaetigungs-datei (abfrage-bestaetigung+)>
<!ELEMENT abfrage-bestaetigung (abfrage-verwaltungsdaten, abfrage-
steuerungsdaten, abfrage-empfangsbestaetigung)>
<!ELEMENT abfrage-datei (abfrage+)>
<!ELEMENT abfrage (abfrage-verwaltungsdaten, abfrage-musterdaten)>
<!ELEMENT abfrage-empfangsbestaetigung (abfrage-fehler)>
<!ELEMENT abfrage-ergebnis-datei (abfrage-verwaltungsdaten, abfrage-
steuerungsdaten, abfrage-ergebnisstatistik, abfrage-ergebnisdaten)>
<!ELEMENT abfrage-ergebnisdaten (ergebnis-kontodatensatz)>
<!ELEMENT abfrage-ergebnisstatistik (abfrage-trefferzahl, abfrage-anzahl-
kontodatensaetze, abfragezaehler, abfrage-versionsparameter, daten-key-id,
gesamt-anzahl-kontodatensaetze, datenaktualisierungszeitpunkt,
datenaktualisierungsart)>
<!ELEMENT abfrage-fehler (#PCDATA)>
<!ATTLIST abfrage-fehler
    code (Kein-Fehler | Syntaxfehler | Uebermittlungsfehler |
Inhaltsfehler | Parameterfehler | Schluesselfehler | Temporaerer-
Systemfehler | Permanenter-Systemfehler) #REQUIRED
>
<!ELEMENT abfrage-key-id (#PCDATA)>
<!ELEMENT abfrage-maximale-anzahl-kontodatensaetze (#PCDATA)>
<!ELEMENT abfrage-minimale-uebereinstimmung-namen (#PCDATA)>
<!ELEMENT abfrage-muster-datei (anfragekennung, abfrage-musterdaten)>
<!ELEMENT abfrage-musterdaten (abfrage-steuerungsdaten, abfrage-
anhaltsdaten)>
<!ELEMENT abfrage-protokoll-datei (anfragekennung, abfrage-
verwaltungsdaten+, abfrage-musterdaten)>
<!ELEMENT abfrage-steuerungsdaten (abfrage-version, abfragestellen-id,
abfrage-maximale-anzahl-kontodatensaetze, abfrage-minimale-
uebereinstimmung-namen)>
<!ELEMENT abfrage-trefferzahl (#PCDATA)>
<!ELEMENT abfrage-trefferzahl-datei (abfrage-verwaltungsdaten, abfrage-
steuerungsdaten, abfrage-ergebnisstatistik)>
<!ELEMENT abfrage-version (#PCDATA)>
<!ELEMENT abfrage-versionsparameter (#PCDATA)>
<!ELEMENT abfrage-verwaltungsdaten (verpflichteten-id, abfragekennung,
abfrage-key-id)>
<!ELEMENT abfrageergebnis-protokoll-datei (abfrage-verwaltungsdaten,
abfrage-trefferzahl, abfrage-anzahl-kontodatensaetze, abfrage-
ergebnisdaten)>
<!ELEMENT abfragekennung (#PCDATA)>
<!ELEMENT abfragestellen-id (#PCDATA)>
<!ELEMENT abfragezaehler (#PCDATA)>
<!ELEMENT abruf-kontodatensatz (indexfeld | kryptextfeld | verpflichteten-
id | datensatz-hash | kontostammdatensatz+)+>
<!-- <!ELEMENT abruf-kontodatensatz (indexfeld | kryptextfeld |
klartextfeld | verpflichteten-id | konto-id | datensatz-hash |
```

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

```
kontostammdatensatz+)+> -->
<!ELEMENT abruf-kontodatensatz-datei (abruf-kontodatensatz+)>
<!ELEMENT aktenzeichen-bafin (#PCDATA)>
<!ELEMENT aktenzeichen-bedarfstraeger (#PCDATA)>
<!ELEMENT anfrage-abschluss (#PCDATA)>
<!ELEMENT anfrage-anhaltsdaten (klartextfeld+)>
<!ELEMENT anfrage-datei (anfrage-verwaltungsdaten, anfrage-steuerungsdaten,
anfrage-anhaltsdaten)>
<!ELEMENT anfrage-erfasser (#PCDATA)>
<!ELEMENT anfrage-ergebnis-bearbeiter (#PCDATA)>
<!ELEMENT anfrage-ergebnis-datei (anfrageergebnis-verwaltungsdaten,
anfrage-ergebnisdaten-verpflichteter*)>
<!ELEMENT anfrage-ergebnisdaten-verpflichteter (verpflichteten-id,
kontodatensatz+)>
<!ELEMENT anfrage-initiierung (#PCDATA)>
<!ELEMENT anfrage-maximale-anzahl-kontodatensaetze (#PCDATA)>
<!ELEMENT anfrage-minimale-uebereinstimmung-namen (#PCDATA)>
<!ELEMENT anfrage-revisor (#PCDATA)>
<!ELEMENT anfrage-steuerungsdaten (anfrage-maximale-anzahl-
kontodatensaetze, anfrage-minimale-uebereinstimmung-namen)>
<!ELEMENT anfrage-verwaltungsdaten (anfrage-initiierung, bedarfstraeger,
aktenzeichen-bedarfstraeger, anfrage-erfasser, anfrage-revisor,
aktenzeichen-bafin)>
<!ELEMENT anfrageergebnis-verwaltungsdaten (anfrage-ergebnis-bearbeiter,
anfrage-abschluss)>
<!ELEMENT anfragekennung (#PCDATA)>
<!ELEMENT bedarfstraeger (#PCDATA)>
<!ELEMENT daten-key-id (#PCDATA)>
<!ELEMENT datenaktualisierungsart EMPTY>
<!ATTLIST datenaktualisierungsart
    type (Full | Incremental) #REQUIRED
>
<!ELEMENT datenaktualisierungszeitpunkt (#PCDATA)>
<!ELEMENT datensatz-hash (#PCDATA)>
<!ELEMENT ergebnis-kontodatensatz ((kryptextfeld | klartextfeld)+,
kontostammdatensatz+, datensatz-hash)>
<!ELEMENT gesamt-anzahl-kontodatensaetze (#PCDATA)>
<!-- <!ELEMENT import-kontodatensatz (verpflichteten-id, konto-id,
klartextfeld+, kontostammdatensatz+)> -->
<!ELEMENT import-kontodatensatz (verpflichteten-id, klartextfeld+,
kontostammdatensatz+)>
<!ELEMENT import-kontodatensatz-datei (import-kontodatensatz+)>
<!ELEMENT indexfeld (token+)>
<!ATTLIST indexfeld
    name (Inhaber-Nachname | Inhaber-Name | Inhaber-Vorname | Inhaber-
Geburtsdatum | Konto-Nummer | Nachname | Name | VB-Nachname | VB-Name | VB-
Vorname | VB-Geburtsdatum | Vorname | WB-Anschrift | WB-Nachname | WB-Name
| WB-Vorname) #REQUIRED
>
<!ELEMENT inhaber (klartextfeld | indexfeld | kryptextfeld)+>
<!ELEMENT klartextfeld (#PCDATA)>
<!ATTLIST klartextfeld
    name (Aufloesungsdatum | Einrichtungsdatum | Geburtsdatum | Inhaber-
Geburtsdatum | Inhaber-Nachname | Inhaber-Name | Inhaber-Vorname | Konto-
Nummer | Nachname | Name | VB-Geburtsdatum | VB-Nachname | VB-Name | VB-
Vorname | Vorname | WB-Anschrift | WB-Nachname | WB-Name | WB-Vorname)
#REQUIRED
>
<!ELEMENT konan (import-kontodatensatz-datei | abruf-kontodatensatz-datei |
```

Verfahren zum automatisierten Abruf von Kontoinformationen Schnittstellenspezifikation BAFin - Kreditinstitute

```
anfrage-datei | anfrage-ergebnis-datei | abfrage-muster-datei | abfrage-
protokoll-datei | abfrage-datei | abfrage-bestaetigungs-datei | abfrage-
trefferzahl-datei | abfrage-ergebnis-datei | abfrageergebnis-protokoll-
datei)>
<!ATTLIST konan
    version CDATA #REQUIRED
>
<!ELEMENT kontodatensatz (klartextfeld+, kontostammdatensatz+)>
<!ELEMENT konto-id (#PCDATA)>
<!ELEMENT kontostammdatensatz (inhaber+, vb*, wb*)>
<!ATTLIST kontostammdatensatz
    datensatz-gueltingkeitsbeginn CDATA #REQUIRED
    datensatz-gueltingkeitsende CDATA #IMPLIED
    datensatz-gueltingkeitsende-plain CDATA #IMPLIED
>
<!ELEMENT kryptextfeld (#PCDATA)>
<!ATTLIST kryptextfeld
    name (Aufloesungsdatum | Einrichtungsdatum | Inhaber-Geburtsdatum |
Inhaber-Nachname | Inhaber-Vorname | Konto-Nummer | VB-Geburtsdatum | VB-
Nachname | VB-Vorname | WB-Anschrift | WB-Nachname | WB-Vorname) #REQUIRED
>
<!ELEMENT token (#PCDATA)>
<!ELEMENT vb (klartextfeld | indexfeld | kryptextfeld)+>
<!ELEMENT verpflichteten-id (#PCDATA)>
<!ELEMENT wb (klartextfeld | indexfeld | kryptextfeld)+>
```

Tabelle 2: XML-Document-Type-Definition (DTD)

8.2 Aufrufschnittstelle des Moduls DataCrypt

Das Modul **DataCrypt** wird als binäre ausführbare Datei zur Verfügung gestellt.

Die Angabe allgemeiner Parameter und der zu verwendenden Schlüssel erfolgt durch eine Konfigurationsdatei.

Die Schlüssel müssen als Dateien zur Verfügung gestellt werden. Die Schlüsseldateien werden durch die BAFin bereitgestellt.

Beim Aufruf können entweder die zu verwendenden Dateien angegeben werden, oder es werden die allgemeinen Ein-/Ausgabe-Ströme (stdin / stdout) verwendet.