
HandHeld-Device (HHD)
zur TAN-Erzeugung
HHD-Erweiterung für unidirektionale Kopplung

Herausgeber:

Bundesverband deutscher Banken e.V., Berlin
Deutscher Sparkassen- und Giroverband e.V., Bonn/Berlin
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Berlin
Bundesverband Öffentlicher Banken Deutschlands e.V., Berlin

Version: V 1.4
Stand: 07.05.2010
Status: Final Version
Bezug: HHD-Version V1.4

Die vorliegende Spezifikation wurde im Auftrag des Zentralen Kreditausschusses entwickelt. Sie wird hiermit zur Implementation in Kunden- und Kreditinstitutssysteme freigegeben.

Die Spezifikation ist urheberrechtlich geschützt. Zur Implementation in Kunden- und Kreditinstitutssysteme wird interessierten Herstellern unentgeltlich ein einfaches Nutzungsrecht eingeräumt. Im Rahmen des genannten Zwecks darf die Spezifikation auch - in unveränderter Form - vervielfältigt und zu den nachstehenden Bedingungen verbreitet werden.

Umgestaltungen, Bearbeitungen, Übersetzungen und jegliche Änderung der Spezifikation sind untersagt. Kennzeichnungen, Copyright-Vermerke und Eigentumsangaben dürfen in keinem Fall geändert werden.

Im Hinblick auf die Unentgeltlichkeit des eingeräumten Nutzungsrechts wird keinerlei Gewährleistung oder Haftung für Fehler der Spezifikation oder die ordnungsgemäße Funktion der auf ihr beruhenden Produkte übernommen. Die Hersteller sind aufgefordert, Fehler oder Auslegungsspielräume der Spezifikation, die die ordnungsgemäße Funktion oder Multibankfähigkeit von Kundenprodukten behindern, dem Zentralen Kreditausschuss zu melden. Es wird weiterhin ausdrücklich darauf hingewiesen, dass Änderungen der Spezifikation durch den Zentralen Kreditausschuss jederzeit und ohne vorherige Ankündigung möglich sind.

Eine Weitergabe der Spezifikation durch den Hersteller an Dritte darf nur unentgeltlich, in unveränderter Form und zu den vorstehenden Bedingungen erfolgen.

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: A
Kapitel: Einleitung Abschnitt: Standardabläufe	Stand: 07.05.2010	Seite: 3

Inhaltsverzeichnis

A. Einleitung	6
B. Generelle Festlegungen zu HHD_{UC}.....	6
B.1 Standardabläufe	7
B.1.1 HHD V1.4 Ablauf zur manuellen Eingabe von Start-Code und Daten	7
B.1.2 HHD V1.4 Ablauf zum gekoppelten Betrieb	8
B.2 Datenübertragungsprotokoll.....	10
B.2.1 Freiheitsgrade und Restriktionen beim Datensatzaufbau ab HHD V1.4.....	11
B.2.2 HHD _{UC} Header und Trailer ab HHD V1.4.....	12
B.2.3 HHD _{UC} Body für HHD V1.4 (Control = 0x01)	14
B.2.4 Prüfsummenbildung bei HHD _{UC}	16
B.3 Sonstige Protokolleigenschaften.....	17
B.3.1 Protokollfestlegungen.....	17
B.3.2 Statusinformationen	17
B.3.3 Energie-Management.....	18
B.3.4 Abbruchszenarien	18
C. Spezielle Festlegungen zur optischen HHD_{UC}-Kopplung.....	19
C.1 Physikalische Rahmenbedingungen	19
C.1.1 Kalibrierung der animierten Grafik	20
C.2 Generelle Definitionen für HHD _{OPT}	21
C.3 Aufbau der Grafik bei HHD _{OPT}	22
C.4 Anhang 25	
C.4.1 Beispiel für die Prüfsummenbildung	25
C.4.2 Eigenschaften der möglichen Grafikformate bei optischer Kopplung.....	28
C.4.2.1 Adobe® Flash®	28
C.4.2.2 JavaScript.....	28
C.4.2.3 Animated GIF	28
C.4.2.4 Sun Java®	28

Kapitel: A	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 4	Stand: 07.05.2010	Kapitel: Einleitung Abschnitt: Standardabläufe

Abbildungsverzeichnis

Abbildung 1: Genereller Aufbau eines HHD _{UC} -Blocks am Beispiel HHD V1.4 (Control=0x01)	10
Abbildung 2: SYNC-Pattern	21
Abbildung 3: Beispielhafte Positionierung des Standard HHD _{OPT} am Bildschirm.....	22
Abbildung 4: Aufbau der animierten Grafik bei HHD _{OPT}	23
Abbildung 5: Beispiel für den zeitlichen Ablauf beim Standard HHD _{OPT}	24
Abbildung 6: Beispiel zur Prüfwertberechnung bei HHD _{UC} V1.4	25

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: A
Kapitel: Einleitung Abschnitt: Standardabläufe	Stand: 07.05.2010	Seite: 5

Literaturhinweise

- [HHD 1.3] Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDevice (HHD) zur TAN-Erzeugung, Version 1.3, 26.10.2007, Final Version, Zentraler Kreditausschuss
- [HHD 1.3.2] Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDevice (HHD) zur TAN-Erzeugung, Version 1.3.2 Final Version, 02.02.2009, Zentraler Kreditausschuss
- [HHD_UC 1.0.1] HHD-Erweiterung für unidirektionale Kopplung, Version 1.0.1 Final Version, 02.02.2009, Zentraler Kreditausschuss
- [HHD 1.4] Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDevice (HHD) zur TAN-Erzeugung, Version 1.4 Final Version, 07.05.2010, Zentraler Kreditausschuss
- [Belegung 1.4] ZKA-TAN-Generator – Belegungsrichtlinien für die Dynamisierung der TAN, Version 1.4 Final Version, 07.05.2010, Zentraler Kreditausschuss
-

Kapitel: A	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 6	Stand: 07.05.2010	Kapitel: Einleitung Abschnitt: Standardabläufe

A. EINLEITUNG

Die vorliegende Spezifikation beschreibt die Übertragung von Daten in Form einer unidirektionalen Kopplung (im Folgenden als HHD_{UC} für HHD – unidirectionally coupled bezeichnet). Die Gerätesteuerung selbst sowie die Art der Visualisierung ist nicht Inhalt dieses Dokumentes, sondern der jeweiligen Spezifikation eines HandHeldDevice (HHD).

Die Verwendung des HandHeld-Device kann mittels einer HHD_{UC} Anwendungsschnittstelle, die in [Belegung 1.4] spezifiziert ist, für FinTS-Kundenprodukte oder die spezifischen Internet-Banking-Anwendungen der Kreditinstitute erfolgen.

Als Hardwarebasis für das HandHeld-Device dienen Geräte mit Display und Tastatur entsprechend den Vorgaben der jeweiligen HHD-Spezifikation. Bei HHD_{UC} werden die Daten unabhängig von der Verbindungsart nur in einer Richtung, nämlich vom Kundenendgerät zum HHD übertragen und dort dann durch den Bediener bestätigt. Ein konkretes Beispiel für eine unidirektionale Kopplung stellt die optische Übertragung mittels einer animierten Grafik dar.

Die Spezifikation ist in zwei Abschnitte unterteilt:

- generelle Festlegungen, die unabhängig vom Übertragungsprotokoll gelten
- spezielle Festlegungen bei Verwendung eines Verfahrens mit optischer Kopplung als der derzeit einzigen Implementierungsvariante

Ziel dieser Standardisierungsbestrebung ist es, auf Basis von möglichst wenigen Varianten eine Möglichkeit zu schaffen, dass jede Internet-Banking-Applikation und jedes FinTS Kundensystem mit jedem am Markt verfügbaren HHD_{UC} verwendet werden kann und herstellerspezifische Ausprägungen vermieden werden können.

Bei den Festlegungen handelt es sich um Ergänzungen zur HHD-Spezifikation. Alle sonstigen, nicht explizit erwähnten Mechanismen und Eigenschaften bleiben erhalten, wie in den entsprechenden Spezifikationen beschrieben.

B. GENERELLE FESTLEGUNGEN ZU HHD_{UC}

Die Verwendung von Geräten mit unidirektionaler Kopplung und die damit verbundenen Eigenschaften sind im jeweiligen HHD-Standard beschrieben. Inhalt dieser Spezifikation ist die Beschreibung der Übertragungsstrecke. Die vorliegende Version der HHD_{UC} Spezifikation beschreibt die Übertragung am konkreten Beispiel von HHD V1.4. Die Festlegungen zu HHD V1.3 sind der HHD_{UC} Spezifikation HHD_{UC} V1.0.1 zu entnehmen und nicht mehr Gegenstand dieser Betrachtung. Die Beschreibung von HHD_{UC} V1.4 ist jedoch bzgl. der HHD-Geräte streng abwärtskompatibel zu HHD_{UC} V1.01., d. h. es werden keine Festlegungen getroffen, die HHD_{UC} V1.0.1 oder HHD V1.3 widersprechen. Desweiteren werden die Protokollmechanismen von HHD_{UC} V1.0.1 weitestmöglich unverändert eingesetzt.

Die Abläufe für manuellen und gekoppelten Betrieb unterscheiden sich durch einige grundsätzliche Eigenschaften.

Dies bedeutet im Speziellen, dass am Kunden-Endgerät nur Informationen zur Benutzerführung angezeigt werden, die eigentlichen Transaktionsdaten jedoch über eine Kommunikationsstrecke zum HHD_{UC} übertragen und dort dem Kunden am Leserdisplay präsentiert werden.

Der Einsatz eines HHD_{UC} erfordert daher einige Erweiterungen gegenüber dem manuellen Betrieb:

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Standardabläufe	Stand: 07.05.2010	Seite: 7

- Das HHD_{UC} muss in der Lage sein, die gesamten Challenge-Daten in einem einzigen Kommunikationsschritt vom Kunden-Endgerät zu übertragen und dann einzeln über Display und Tastatur dem Kunden zu präsentieren.
- Der Kunde muss über den Betriebszustand und den Status der Übertragung informiert werden.
- Da einerseits Übertragungskomponenten betrieben werden müssen, andererseits keine direkte Verbindung zum Kunden-Endgerät zum Aufladen eines Akku zur Verfügung steht, müssen Möglichkeiten geschaffen werden, den Energiebedarf für die Übertragungskomponenten zu minimieren.
- Es bestehen Abbruchszenarien, die speziell im gekoppelten Betrieb auftreten können.

B.1 Standardabläufe

Die folgenden Standardabläufe ergeben sich aus den Vorgaben durch die HHD-Spezifikation und sollen die Unterschiede zwischen manuellem und gekoppeltem Betrieb am Beispiel von HHD V1.4 verdeutlichen.

Die verwendeten Kodierungen und Tastenbelegungen beziehen sich auf diese HHD-Spezifikation und sind nur als exemplarisch anzusehen (vgl. Abschnitt „B.2.1“).

B.1.1 HHD V1.4 Ablauf zur manuellen Eingabe von Start-Code und Daten

Der folgende Ablauf zeigt den Prozess einer Eingabe von Start-Code und Transaktionsdaten am Beispiel HHD V1.4. Im konkreten Fall wird über den Start-Code „104xxxx“ die Schablone „104“ zur Bestätigung einer Einzelüberweisung Inland ausgewählt:

Vorgang	Display-Anzeige
Einstecken der Chipkarte	keine bzw. Text
Drücken der Taste „TAN“	Start-Code
Drücken von Zifferntasten (max. 12), Abschluss mit „Bestätigen“-Taste	Start-Code 104xxxx
Akzeptieren mit „Bestätigen“-Taste	Überweisung Inland
Eingabe von weiteren Werten in Abhängigkeit der gewählten Schablone	Konto Empf.: BLZ Empf.: Betrag
Abschluss der jeweiligen Eingabe mit der „Bestätigen“-Taste, anschließend erfolgt die Anzeige der TAN	Überweisung TAN: 361620

Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 8	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Standardabläufe


Kennzeichen des Standard HHD-Verfahrens ist, dass der Start-Code und die Transaktionsdaten in getrennten Schritten eingegeben werden, bei denen der Kunde jedes Mal aktiv Daten eintippen und bestätigen muss. Die Ausgabe in der ersten Zeile der Dateneingabemaske ist abhängig von den ersten zwei bis neun Stellen des zuvor eingegebenen Start-Codes.

Während der Kunde den Start-Code vom Bildschirm seines Endgerätes übernehmen kann, muss er den/die Transaktionswert(e) seinem Zahlungsbeleg entnehmen.

Als Ergebnis wird eine TAN generiert, die im Display des HHD angezeigt wird und die der Kunde in das entsprechende Feld an seinem Endgerät eintippen muss.

B.1.2 HHD V1.4 Ablauf zum gekoppelten Betrieb

Der im Folgenden gezeigte Kommunikationsablauf zeigt den um die Übertragungsfunktion erweiterten Ablauf des HHD_{UC}.

Vorgang	Display-Anzeige
Einstecken der Chipkarte	keine bzw. Text
Starten der Übertragungsfunktion	Übertragung aktiviert
während der Datenübertragung	Übertragung 
Alle Datenbytes übertragen, Prüfziffer OK: Der übertragene Start-Code wird nicht angezeigt, sondern fließt später transparent in die TAN-Berechnung mit ein.	Übertragung erfolgreich
Akzeptieren mit „Bestätigen“-Taste	Überweisung Inland
Bestätigen von weiteren Werten in Abhängigkeit der gewählten Schablone	Konto Empf. : 12345678 BLZ Empf. : 70020245 Betrag 22,45
Zustimmung durch Drücken der „Bestätigen“-Taste, anschließend erfolgt die Anzeige der TAN	Überweisung TAN: 472733

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Standardabläufe	Stand: 07.05.2010	Seite: 9

Wie aus der Abbildung ersichtlich, unterteilt sich der Ablauf in die Übertragungsphase und die Bestätigungsphase.

Übertragungsphase

Zu Beginn der Übertragungsphase wird die Übertragungseinheit durch einmaliges Drücken der Starttaste für die Übertragungsfunktion („F“- oder „TAN“-Taste, vgl. [HHD V1.4]) aktiviert. Während der Übertragung wird eine Statusinformation im HHD_{UC}-Display angezeigt. Die Übertragungsphase wird durch einen eindeutigen Anzeigetext „Übertragung erfolgreich“ beendet.

Bestätigungsphase

In der anschließenden Bestätigungsphase werden die Transaktionsdaten elementweise angezeigt. Dabei werden die „Eingabedaten“ des Kunden aus den übertragenen Daten entnommen und der Kunde muss diese – nach entsprechender Überprüfung mit dem Originalbeleg – nur noch bestätigen.

Der Start-Code, der die Freshness herstellt und den Dialogablauf steuert, hat ansonsten aber keine fachliche Relevanz und wird daher dem Kunden im Standardfall nicht angezeigt (Ausnahmen vgl. [HHD 1.4]); er wird jedoch in der anschließenden TAN-Berechnung berücksichtigt.

Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 10	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll

B.2 Datenübertragungsprotokoll

Das Datenübertragungsprotokoll ist sehr schlank gehalten, damit auch bei schmalbandigen Übertragungsmedien keine zu langen Übertragungszeiten auftreten.

Für HHD V1.3.2 besitzt das Datenprotokoll einen festen Aufbau, bestehend aus Start-Code und zwei Datenelementen inkl. der jeweiligen Längfelder (vgl. [HHD_{UC} 1.0.1]). Das Datenübertragungsprotokoll nach HHD_{UC} V1.0.1 ist nicht mehr Inhalt dieser Spezifikation, wird aber aus Gründen der Abwärtskompatibilität in vollem Umfang unterstützt.

Der Aufbau des Protokolls hat sich mit HHD_{UC} Version 1.4 geändert, um auch Datenstrukturen mit unterschiedlicher Struktur transportieren zu können. Dem Feld für die Länge des Start-Code folgt nun ein ControlByte, das auf Datenmuster unterschiedlichen Aufbaus verzweigen kann. Die Existenz des ControlByte wird durch eine definierte Bit-Kombination im Längfeld des Start-Code festgelegt. Hierüber wird auch die Kompatibilität zu HHD_{UC} V1.0.1 sichergestellt.

Die Datenstrukturen selbst können ab HHD V1.4 in gewissem Umfang frei definiert werden:

Start-Kriterium	Länge Challenge	Länge Start-Code	Control Byte	Datensatzaufbau analog Control	Prüfziffer
-----------------	-----------------	------------------	--------------	--------------------------------	------------

Die HHD_{UC}-Blöcke für HHD_{UC} V1.4 sind somit folgendermaßen aufgebaut:

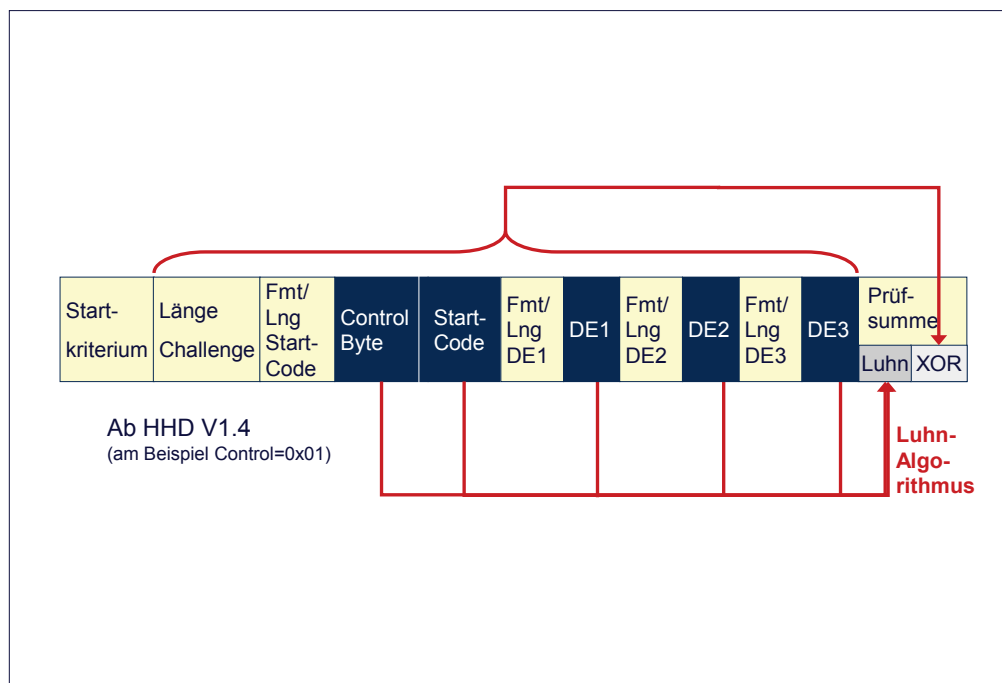


Abbildung 1: Genereller Aufbau eines HHD_{UC}-Blocks am Beispiel HHD V1.4 (Control=0x01)

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll	Stand: 07.05.2010	Seite: 11

B.2.1 Freiheitsgrade und Restriktionen beim Datensatzaufbau ab HHD V1.4

Durch die Steuerung verschiedener Datenstrukturen über das ControlByte ergeben sich folgende Eigenschaften:

- **Sicherheitsmedium**
Bei HHD-Verwendung kommt eine Banken-Chipkarte mit dem Betriebssystem SECCOS zum Einsatz. Es wird dort der ZKA EMV TAN-Generator (ZKA EMV AC Applikation) für die Erzeugung der TANs benutzt.
- **Visualisierung**
Bei HHD-Verwendung mit ControlByte 0x01 kommt das allgemeine Visualisierungskonzept für HHD zum Einsatz (vgl. [HHD 1.4]), ansonsten eine dem ControlByte entsprechende Visualisierungsstruktur.
- **Enthaltene Felder und deren Belegung**
Die Datenstruktur kann beliebige Felder enthalten, die in der Beschreibung entsprechend dokumentiert sein müssen. Es muss auch definiert sein, wie die Belegung der Felder abhängig vom Einsatzzweck zu erfolgen hat.
- **Datenlänge**
Die maximale physische Datenlänge beträgt 255 Byte. Der jeweilige logische Maximalwert ist bei der Beschreibung einer durch das ControlByte definierten HHD-Variante festzulegen.
- **Es muss ein im HHD unterstützter ASCII-Zeichensatz [vgl. HHD 1.4] verwendet werden; der Zeichenvorrat kann an den jeweiligen Verwendungszweck angepasst sein.**
- **Die HHD_{UC} Anwendungsschnittstelle (vgl. [Belegung 1.4]) kann optional verwendet werden. Wird die Verwendung vorgeschrieben, so muss auch eine entsprechende Spezifikation der Elemente „Challenge“ und „Challenge HHD_{UC}“ erfolgen.**

Welche Bedeutung die einzelnen Bestandteile des HHD_{UC}-Blocks haben, ist in den folgenden Abschnitten beschrieben.

Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 12	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll

B.2.2 HHD_{UC} Header und Trailer ab HHD V1.4

Ab der HHD_{UC}-Version 1.4 wird die Struktur für die zu übertragenden Daten in Header, Body und Trailer unterteilt. Damit lassen sich auch für zukünftige HHD-Versionen unterschiedlich aufgebaute Datenstrukturen übertragen.

HHD_{UC} Header und -Trailer haben folgenden Aufbau

Bezeichnung	Länge in Byte	Format	Kommentar
Startkriterium	---	---	abhängig vom Übertragungsmedium
LC	1	binär	Datenlänge (max. 255 ohne LC)
LS	1	binär	Länge Start-Code (max. 62 ohne LS) Aufbau s. u.
Control	1	binär	ControlByte, abhängig von LS, Aufbau s. u.
Datenstruktur, abhängig vom Wert in <code>Control</code>			
CB	1	binär	CheckByte (Prüfsummen-Byte) Linkes Halbbyte: Luhn-Prüfziffer Rechtes Halbbyte: XOR-Summe

◆ Beschreibung:

Startkriterium


Das Startkriterium ist abhängig vom verwendeten Übertragungsmedium festzulegen und in den entsprechenden Kapiteln dieses Dokumentes beschrieben (für die optische HHD_{UC}-Kopplung siehe Abschnitt C).

LC – Länge Challenge

In LC ist die gesamte Datenlänge in einem Byte kodiert. Damit ist eine theoretische Maximallänge von 255 darstellbar.

Bei der Beschreibung der einzelnen Datenstrukturen ist – abhängig vom Wert für `Control` bzw. auch der Anzahl der `ControlBytes` – ein konkreter Maximalwert für eine Struktur festgelegt.

Die Challengelänge bezeichnet die Länge über den gesamten Datenblock, startend mit dem ersten Byte nach LC und endend mit dem rechten Halbbyte von CB (CheckByte).

	<h4>Versionserkennung</h4> <p>Nach Erkennen des Startkriteriums und des Längenfeldes LC muss über die Analyse des Elementes „LS – Länge des Start-Code“ ermittelt werden, um welche Struktur des Datenstroms es sich handelt:</p> <ul style="list-style-type: none"> • HHD V1.3.2
---	---

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll	Stand: 07.05.2010	Seite: 13

	<p>Bei dieser Version ist kein ControlByte enthalten, es gelten die Festlegungen in [HHD_UC 1.0.1].</p> <ul style="list-style-type: none"> HHD V1.4 oder andere Versionen oder Strukturen Über das ControlByte wird gesteuert, welchen Aufbau die nachfolgende Struktur hat.
--	---

LS – Länge des Start-Code

Über das Element `LS` wird die Existenz des ersten ControlByte festgelegt und die Länge / das Format des Start-Code im Body angegeben. Die theoretische Maximallänge eines Start-Code für ein HHD-Verfahren beträgt 63 Byte; der logische Maximalwert ist im jeweiligen Verfahren zu beschreiben.

Die Länge des Start-Code kann bei HHD V1.4 maximal 6 Byte (BCD) bzw. 12 Byte (ASCII) betragen.

Das Element `LS` lässt folgende Kodierungen zu:

Bezeichnung	Information
LS 0 bis 5	Länge des Start-Code
LS 6	0=BCD / 1=ASC
LS 7	0=ohne ControlByte (HHD _{UC} 1.0.1) 1=mit ControlByte (ab HHD _{UC} 1.4)

Control

Über das Element `Control` wird der Aufbau des HHD_{UC}-Body festgelegt. Dabei sind für das erste ControlByte aktuell folgende Werte möglich:

Bezeichnung	Information
Control 0	1: Datenstruktur für HHD 1.4 0: für internationale Verwendung
Control 1 – 6	0 (r. f. u.)
Control 7	0: dies ist das einzige ControlByte 1: weiteres ControlByte folgt

Folge-ControlBytes für internationale Verwendung

Über Folge-ControlBytes können weitere Datenstrukturen strukturiert dargestellt werden. Diese haben folgenden Aufbau:

Bezeichnung	Information
Control 0 - 2	Länderkennung
Control 3 - 6	Versionskennung
Control 7	0: letztes ControlByte 1: weiteres ControlByte folgt

Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 14	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll

Folgende Länderkennungen (Control bit0 - bit2) sind derzeit vorgesehen:

0b000: Deutschland
0b001: Österreich
0b010 – 0b111: (r. f. u)

Länderkennungen werden durch den Zentralen Kreditausschuss vergeben. Die Versionskennungen im Folge-ControlByte werden durch das jeweilige Land festgelegt.

Abhängig von der Anzahl an ControlBytes ändert sich auch die maximale Gesamtlänge LC.

Enthält Control einen Wert, den das HHD nicht unterstützt, so ist die Übertragung mit der Meldung

„Fehler 25“

abzubrechen.

CB = CheckByte / Prüfsummenbyte

Für die Prüfsummenberechnung wird der Luhn-Algorithmus verwendet. Da eine Luhn-Prüfziffer nur aus 4 bit besteht und somit jeder 16. Fehler nicht erkannt werden könnte, wird das rechte Halbbyte zusätzlich durch eine XOR-Operation über die gesamte Struktur gefüllt.

Den exakten Aufbau des Prüfsummenbyte enthält Kapitel C.4.1.

B.2.3 HHD_{UC} Body für HHD V1.4 (Control = 0x01)

Bei HHD V1.4 hat der HHD_{UC} Body folgenden Aufbau:

◆ Generelle Eigenschaften:

Die Datenstruktur für `Control=0x01` hat folgende Eigenschaften:

Sicherheitsmedium	Es kommt die ZKA Banken-Chipkarte auf Basis SECCOS in Verbindung mit der ZKA EMV AC Applikation Debit zum Einsatz
Visualisierung	Die Visualisierung geschieht auf Basis des in [HHD 1.4] festgelegten Visualisierungskonzeptes. Zusätzlich gelten die in [Belegung 1.4] beschriebenen Richtlinien.
maximale Challengelänge	Die gesamte Datenlänge für LC ergibt sich aus der Summe der maximalen Einzelwerte und beträgt 77 Byte (inkl. ein ControlByte und CheckByte)
Maximale Länge des Start-Code	Als Start-Code Länge sind maximal 6 Byte (BCD) bzw. 12 Byte (ASCII) möglich.
Zeichensatz	Es wird der HHD-Zeichensatz verwendet (vgl.

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll	Stand: 07.05.2010	Seite: 15

[HHD 1.4]).

Zeichenvorrat

Es wird der in [HHD 1.4] beschriebene Zeichenvorrat unterstützt. Die Tastenbelegungen entsprechen HHD V1.4 und sind zu denen von HHD V1.3 abwärtskompatibel.

HHD_{UC} Anwendungs-
schnittstelle

Unterstützung verpflichtend, Spezifikation siehe Abschnitt [Belegung 1.4].

◆ Datenstruktur bei HHD V1.4 (Control=0x01):

Bezeichnung	Länge in Byte	Format	Kommentar
Start-Code	max. (BCD) max. 12 (ASC)	(LS)	Im Format BCD ggf. mit „F“ auf Bytegrenze ergänzt
LDE1	1	binär	bit 0 bis bit 5: Länge Datenelement 1 bit 6: 0=BCD / 1=ASC
Datenelement 1	max. 6 bzw. 18 (BCD) max. 12 bzw. 36 (ASC)	(LDE1)	Im Format BCD ggf. mit „F“ auf Bytegrenze ergänzt
LDE2	1	binär	bit 0 bis bit 5: Länge Datenelement 2 bit 6: 0=BCD / 1=ASC
Datenelement 2	max. 6 bzw. 18 (BCD) max. 12 bzw. 36 (ASC)	(LDE2)	Im Format BCD ggf. mit „F“ auf Bytegrenze ergänzt
LDE3	1	binär	bit 0 bis bit 5: Länge Datenelement 3 bit 6: 0=BCD / 1=ASC
Datenelement 3	max. 6 bzw. 18 (BCD) max. 12 bzw. 36 (ASC)	(LDE3)	Im Format BCD ggf. mit „F“ auf Bytegrenze ergänzt

◆ Beschreibung:

Start-Code

Es gelten die Festlegungen in [HHD 1.4].

LDE1 / LDE2 / LDE3 = Länge des Datenelements 1, 2, 3

Hierdurch wird die Länge des Datenelements 1, 2 oder 3 exklusive dem Längenfeld LDE 1, 2 bzw. 3 selbst bezeichnet. Die Länge eines Datenelements kann maximal 6 / 18 Byte (BCD) bzw. 12 / 36 Byte (ASCII) betragen. Nur eines der drei Datenelemente kann jeweils bis zu 18 / 36 Byte lang sein (vgl. [HHD 1.4]), für die verbleibenden Datenelemente gilt dann die Gesamtlänge von 6 / 12 Byte.

Die Längenfelder LS, LDE1, LDE2 und LDE3 sind folgendermaßen aufgebaut:

LDE_x 0 bis 5 : Länge der Daten

LDE_x 6 : Format der Daten:


Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 16	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Datenübertragungsprotokoll

0 = BCD

1 = ASCII

LDEx 7 : 0 (r. f. u)

Unabhängig von der Verwendung der Schablonen- oder Selektionstechnik und den Informationen im Start-Code (vgl. [HHD 1.4]) können im HHD_{UC}-Protokoll Datenelemente ausgelassen werden, indem als Länge LDE1, LDE2 oder LDE3 = '00' angegeben wird. Dadurch wird gekennzeichnet, dass das jeweilige, durch den Start-Code definierte Datenelement nicht im HHD_{UC}-Datenstrom enthalten ist. Somit sind für leere Datenelemente die Längenfelder zu übertragen, wenn danach noch nicht-leere Datenelemente folgen. Leere Datenelemente am Ende des Datenstromes können komplett inklusive Längensfeld entfallen.

	<p>Die Festlegung des Datenformates BCD oder ASCII bezieht sich ausschließlich auf die Datenübertragung und hat keinerlei Auswirkung auf die weitere Verarbeitung im HHD. Insbesondere bleibt der Aufbau des VisData-Puffers für die TAN-Generierung davon unberührt.</p>
---	---

Datenelement 1, 2, 3

Es gelten die in [HHD 1.4] definierten Datenelemente. Sollte ein Datenelement eine Zahl mit Komma-Trennung oder Vorzeichen beinhalten (z. B. Betrag oder Anzahl), so muss als Format ASCII gewählt werden, da ggf. auch ein Sonderzeichen mit übertragen werden muss.

B.2.4 Prüfsummenbildung bei HHD_{UC}

Das Prüfsummenbyte setzt sich aus zwei Halbbytes zusammen, die wie folgt gefüllt werden:

Linkes Halbbyte: Luhn-Prüfziffer

Als Methode zur Prüfsummenbildung wird der Luhn-Algorithmus verwendet. Hierzu werden die reinen Nettodaten ohne Längenfelder aber inklusive der BCD-Füllzeichen auf volle Byte aneinander gereiht. Welche Daten konkret in die Prüfsummenbildung eingehen, entnehmen Sie bitte dem Beispiel in Abschnitt C.4.1. Im Fall von ASCII-Daten werden die entsprechenden ASCII-Codes des HHD-Zeichensatzes verwendet. Über die so angereihten Daten wird im linken Halbbyte der Wert ergänzt, der zum Erreichen einer modulo-10 Nullsumme nach dem Luhn-Algorithmus benötigt wird. Die Summenbildung erfolgt hierbei von links nach rechts (vgl. Beispiel).

Der Zeichenvorrat für die ASCII-Daten sieht außer den Ziffern 0 bis 9 auch Buchstaben und Sonderzeichen vor, die im ASCII-Code einen nicht numerischen Wert enthalten können. Diese Zeichen werden folgendermaßen behandelt, wie am Beispiel des Kommas gezeigt werden kann:

Ist in den ASCII-Daten ein Komma (0x2C) als nicht numerischer Wert enthalten, so wird der Wert 0xC als '12' interpretiert. Somit fließt ein Komma (0x2C) als $2 * 12 = 24$ bzw. als Ziffer 2 und 4 in die Prüfsummenbildung ein.

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: B
Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Sonstige Protokolleigenschaften	Stand: 07.05.2010	Seite: 17

Für die Berechnung der Luhn-Prüfziffer sind die folgenden Schritte durchzuführen:

- Schritt 1: Mit der rechtesten Ziffer beginnend ist einschließlich dieser Ziffer jede übernächste Ziffer zu verdoppeln (mit 2 multiplizieren).
- Schritt 2: Die einzelnen Ziffern der Produkte aus Schritt 1 und die bei diesen Multiplikationen unberührt gebliebenen Ziffern sind zu addieren.
- Schritt 3: Das Ergebnis der Addition aus Schritt 2 ist von dem auf die nächst höhere Zahl mit der Einerstelle 0 aufgerundeten Ergebnis der Addition aus Schritt 2 abzuziehen. Wenn das Ergebnis der Addition aus Schritt 2 bereits eine Zahl mit der Einerstelle 0 ergibt (z. B. 30, 40, usw.), ist die Prüfziffer 0.

Rechtes Halbbyte: XOR-Operation

Es wird über alle Halbbytes – beginnend mit dem linken Halbbyte von LC und endend mit dem rechten Halbbyte des letzten Datenelements – eine XOR-Operation durchgeführt.

Ein Beispiel zur Prüfsummenbildung befindet sich in Abschnitt C.4.1.

B.3 Sonstige Protokolleigenschaften

B.3.1 Protokollfestlegungen

Das HHD_{UC} wartet nach dem Empfang des Startkriteriums so lange, bis der gesamte HHD_{UC}-Block unterbrechungsfrei und komplett empfangen wurde.

Nach Empfang des HHD_{UC}-Blocks wird dieser anhand des in Abschnitt B.2.4 beschriebenen Verfahrens auf Fehler geprüft.

Ist das Ergebnis der Nachrechnung negativ, so wartet das Terminal erneut auf die Erkennung des Startkriteriums um den Vorgang zu wiederholen. Dabei startet auch die Anzeige des Übertragungsstatus nach Erkennung des Startkriteriums (und der direkt nachfolgenden Challenge-Länge) wiederum bei 0%.

Dieser Vorgang wird bei korrekter Nachrechnung der CheckSum, bzw. nach insgesamt fünf fehlerhaften Durchläufen beendet.

Im Fehlerfall wird folgende Meldung ausgegeben:

Übertragung
abgebrochen

Die Anzeige der jeweiligen Meldung kann durch Drücken der „Bestätigen“-Taste oder der „Abbruch“-Taste unterbrochen und das Gerät abgeschaltet werden; ansonsten schaltet sich das Gerät nach einem Timeout von ca. 30 Sekunden aus.

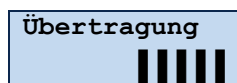
B.3.2 Statusinformationen

Um den Fortschritt der Übertragung quantifiziert im Display anzeigen zu können muss das Gerät zu Beginn die Gesamtlänge der zu übertragenden Daten ermitteln können.

Hierzu ist in den zu übertragenden Daten sowohl die Gesamtlänge des Datenstroms als auch die Länge der einzelnen Elemente enthalten. Diese erlauben dem HHD_{UC}, den Fortschritt der Übertragung relativ zur Gesamtlänge des HHD_{UC}-Blocks berechnen zu können.

Kapitel: B	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 18	Stand: 07.05.2010	Kapitel: Generelle Festlegungen zu HHDUC Abschnitt: Sonstige Protokolleigenschaften

Der Kunde wird durch die Anzeige



über den Übertragungsfortschritt informiert.

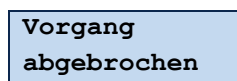
B.3.3 Energie-Management

Bei Betrieb des Kommunikationsbausteins muss dieser sich im dauerhaften Betriebsmodus befinden, was einen entsprechend hohen Strombedarf zur Folge hat. Somit sollte der Kommunikationsbaustein nur bei Bedarf und bewusst aktiviert und zum frühestmöglichen Zeitpunkt (z. B. der erfolgreichen Prüfung des CheckByte) wieder deaktiviert werden. Der Bediener kann somit zu Beginn entscheiden, ob er die TAN-Erzeugung mittels Eingabe der kontextsensitiven Daten per Tastatur des Geräts durchführen möchte (Start des Vorgangs durch Betätigung der TAN-Taste bei HHD V1.4 im Standardlayout) oder ob er hierzu den Kommunikationsbaustein verwenden möchte (Start durch die Betätigung der „F“-Taste bei HHD V1.4 im Standardlayout). Welche Tasten bzw. Funktionen konkret verwendet werden, beschreibt die jeweilige HHD-Spezifikation.

B.3.4 Abbruchszenarien

Durch Betätigung der „Abbruch“-Taste wird der Vorgang abgebrochen. Hierbei ist es unerheblich, ob die Übertragung gerade aktiviert wurde, noch aktiv ist (Anzeige des Prozentwertes des Übertragungsstatus) oder bereits eine Anzeige der übertragenen Daten im Display des Lesers erfolgt.

Bei Betätigung der „Abbruch“-Taste erfolgt grundsätzlich die Anzeige:

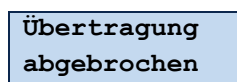


Die Anzeige dieser Meldung kann durch Drücken der „Bestätigen“-Taste oder der „Abbruch“-Taste unterbrochen und das Gerät abgeschaltet werden; ansonsten schaltet sich das Gerät nach einem Timeout von ca. 30 Sekunden aus.

Somit wird eine Einzelkorrektur der über die Kommunikationsschnittstelle übertragenen Daten nicht ermöglicht.

Wird das HHD_{UC} während der Datenübertragung aus dem Empfangsbereich entfernt, so wird ein Timeout von ca. 5 Sekunden gestartet. Innerhalb dieser Zeit kann das HHD_{UC} wieder im Empfangsbereich positioniert werden, um den Vorgang der Datenübertragung wieder aufzunehmen. Das HHD_{UC} wartet in diesem Fall erneut auf die Erkennung des Startkriteriums. Dabei startet auch die Anzeige des Übertragungsstatus nach Erkennen des Startkriteriums (und der direkt nachfolgenden Challengelänge) wiederum bei 0%.

Sollte der Timeout ablaufen, ohne dass es zu einer Wiederaufnahme der Übertragung kommt, so wird folgende Meldung angezeigt:



Die gleiche Fehlermeldung wird bei jedem physischen Übertragungsfehler angezeigt, also auch, wenn z. B. ein Längenfeld falsch ist. Bei fehlerhafter Prüfziffer erfolgt der Abbruch nach fünf fehlerhaften Durchläufen (vgl. Abschnitt B.3.1)

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: C
Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Physikalische Rahmenbedingungen	Stand: 07.05.2010	Seite: 19

C. SPEZIELLE FESTLEGUNGEN ZUR OPTISCHEN HHD_{UC}-KOPPLUNG

Im Folgenden werden zusätzliche Festlegungen getroffen, die sich auf die Verwendung einer optischen Kopplung auf Basis von animierten Grafiken zwischen Kunden-Endgerät und HHD_{UC} ergeben – im Folgenden als HHD_{OPT} bezeichnet. Die Kommunikationsstrecke besteht in diesem Fall aus einer optischen Verbindung zwischen den beiden Partnern. Am Bildschirm des Kunden-Endgerätes wird eine dynamische Grafik angezeigt, in der die zu übertragenden Daten kodiert sind, so dass diese von den optischen Empfangselementen im HHD_{OPT} gelesen werden können. HHD_{OPT} ist eine Ausprägung eines optischen Kopplungsverfahrens; weitere Verfahren können bei Verfügbarkeit entsprechender Technologien zu einem späteren Zeitpunkt ergänzt und in vergleichbarer Weise beschrieben werden.

Bezüglich des Protokolls sind keine Erweiterungen zu den in Abschnitt B beschriebenen Festlegungen zum HHD_{UC} nötig.

Die optische Kopplung der beiden Geräte wird von einigen Rahmenbedingungen bestimmt, die den herstellerunabhängigen Betrieb eines HHD_{OPT} mit optischer Kopplung ermöglichen sollen.

C.1 Physikalische Rahmenbedingungen

Um die ermittelten Transaktionsdaten optisch zum HHD_{OPT} übertragen zu können, muss eine für das Kunden-Endgerät geeignete Grafik dynamisch aufgebaut werden. Hierfür gelten folgende Kriterien als entscheidend:

- Die dynamische Aufbereitung muss schnell und Ressourcen schonend erfolgen können; die resultierende Grafik muss vom Datenvolumen her möglichst klein sein.
 - Das verwendete Medium muss eine möglichst rasche Übertragung der Grafik über die optische Koppelstrecke erlauben, d. h. die Blink-Frequenz muss möglichst hoch sein, was zur Folge hat, dass die Abstimmung zwischen Prozessor, Grafikkarte, Bildschirm und Präsentationsprogramm optimal gewählt sein muss. Die minimale bzw. maximale zu unterstützende Blinkfrequenz beträgt 2 Hz bzw. 20 Hz.
 - Die erzeugte Grafik muss auf jedem beliebigen Display darstellbar sein, unabhängig von . . .
 - der Art des Bildschirms (Röhrenmonitor, TFT, Plasma, ...)
 - der Größe des Bildschirms und
 - der gewählten Auflösung.
 - Das Standard HHD_{OPT} muss zwei Markierungen besitzen, welche die Position der äußeren optischen Elemente kennzeichnen. Diese entsprechen den Marken in der standardisierten Grafik (vgl. Abschnitt C.3) und erleichtern die Positionierung durch den Kunden.
 - Je nach Implementierung muss die am besten geeignete Umsetzungsvariante gewählt werden. Für das Senden der Transaktionsdaten analog dem HHD_{UC}-Protokoll existieren folgende Möglichkeiten der Umsetzung:
-

Kapitel: C	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 20	Stand: 07.05.2010	Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Physikalische Rahmenbedingungen

Darstellung	Systemvoraussetzungen auf Kundenseite
Adobe® Flash®	Adobe® Flash® -Player muss installiert sein
JavaScript	JavaScript muss im Browser aktiviert sein
Animated GIF	keine
Sun Java®	Java® Virtual Machine muss installiert sein

Nähere Informationen zu den Eigenschaften der einzelnen Umsetzungsmöglichkeiten befinden sich im Anhang des Abschnitts C.4.2.

Die optischen Eigenschaften des HHD_{OPT} werden durch folgende Parameter bestimmt:

- Die physikalischen Eigenschaften der gewählten optischen Empfangselemente (z. B. Fototransistoren) bzgl. Energiebedarf, Kennlinien und Schutz gegen Übersprechen bzw. Umgebungslicht. Hier ist vom Hersteller eine geeignete Auswahl zu treffen.
- Ob es sich bei den optischen Empfangselementen um diskrete oder integrierte Bauelemente handelt, ist für die Betrachtung nicht relevant und muss aus Kosten- und Zuverlässigkeitsaspekten vom Hersteller selbst entschieden werden.
- Abgeleitet hiervon ergeben sich Mindestabstände der optischen Empfangselemente bzw. die Gerätegröße sowie deren Anzahl. Die Gerätegröße kann vom Hersteller in gewissem Umfang selbst festgelegt werden (vgl. Abschnitt C.1.1 „Kalibrierung der animierten Grafik“). Für die Anzahl der optischen Elemente hat sich im Dialog mit unterschiedlichen Herstellern die Anzahl 5 als Optimum herausgestellt und wird in der Spezifikation als fester Wert zugrundegelegt.

Da eine herstellerunabhängige Gestaltung der optischen Kopplung erzielt werden soll, gilt die Darstellung in den folgenden Kapiteln als Vorgabe für den Betrieb eines HHD_{OPT}:

Voraussetzung für den Einsatz eines Produktes als HHD_{OPT} ist, dass die im Folgenden dargestellte dynamische Grafik in den zu unterstützenden Formaten der Bauart entsprechend zuverlässig interpretiert werden kann.

C.1.1 Kalibrierung der animierten Grafik

Ziel der Darstellung der animierten Grafik ist die korrekte Darstellung auf einem beliebigen Bildschirm für ein beliebiges Produkt ohne manuelle Eingriffe des Kunden. Da jedoch zum einen die Baugröße der Geräte nicht festgeschrieben ist und zum anderen nicht jedes Grafikformat (z. B. Animated GIF) frei skalierbar ist, muss der Kunde ggf. die animierte Grafik an die Größe des HHD_{OPT} bzw. die Bildschirmauflösung anpassen.

Abhängig vom verwendeten Darstellungsformat kann diese Kalibrierung lokal im Browser (z. B. JavaScript) oder am Webserver (z. B. Animated GIF) vorgenommen werden (vgl. Anhang).

Die Kalibrierung kann je nach Implementierung durch „Ziehen“ der Grafik an speziell dafür markierten Flächen oder über Schaltsymbole wie eine große und kleine Lupe erfolgen.

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: C
Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Generelle Definitionen für HHDOPT	Stand: 07.05.2010	Seite: 21

C.2 Generelle Definitionen für HHD_{OPT}

Die folgenden Festlegungen gelten für die verwendeten Signale und deren Bedeutung.

Bezeichnung	Information
CLK	Datenkanal mit der Taktung für die Datenübertragung; es werden bei jedem Übergang „1“ → „0“ Daten übernommen.
SYNC	SYNC-Pattern, das als Start-Erkennung dient
Data 0 ... 3	Bit-Werte eines zu übertragenden Halbbytes in einem Datenkanal

Weiterhin gilt folgende Festlegung:

weiß (high) = '1'
schwarz (low) = '0'

Es wird bei jedem Datenbyte jeweils zuerst das niederwertige Halbbyte übertragen.

Die Wertigkeiten der Data-Flächen bezogen auf das jeweilige Halbbyte sind wie folgt:

Data 0: Wertigkeit = 2^0

Data 1: Wertigkeit = 2^1

Data 2: Wertigkeit = 2^2

Data 3: Wertigkeit = 2^3

Synchronisation

Es kommt ein definiertes SYNC-Pattern zum Einsatz, das zur Erkennung des Anfangs einer Message im Idle-Mode dient.

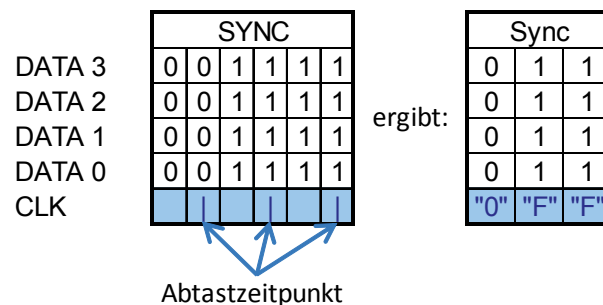



Abbildung 2: SYNC-Pattern

Da die Daten nur zum Abtastzeitpunkt  bei abfallender Flanke übernommen werden, ergibt sich die Zeichenfolge "OFF".

Dieses Muster "OFF" darf im Bereich der Längenfelder, Daten und Prüfziffer nicht auftreten. Für die Daten selbst kann dies ausgeschlossen werden, da diese nur aus den definierten Zeichen bestehen dürfen. Da die Aneinanderreihung von Längen- bzw. Prüffeldern schon von der Länge her keinen Bestandteil des SYNC-Pattern er-

Kapitel: C	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 22	Stand: 07.05.2010	Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Aufbau der Grafik bei HHD _{OPT}

geben kann, können hierbei ebenfalls keine Kollisionen entstehen. Somit ist der Regelbetrieb kollisionsfrei. Da sich auch in keinen anderen Situationen ein plausibler Datenstrom ergibt und die Übertragung nach Timeout abgebrochen wird, kann das gewählte SYNC-Pattern im Rahmen des definierten Datenvorrats als kollisionsfrei angesehen werden.

Während der Synchronisation läuft das CLK-Signal weiter, um eine kontinuierliche Taktung der internen Prozesse zu ermöglichen. Das in der obigen Abbildung gezeigte SYNC-Pattern stellt sicher, dass der Synchronisationspunkt zuverlässig gefunden werden kann, da innerhalb der Byte-Sequenz ein definierter Wechsel von „1“ → „0“ in allen Datenkanälen erfolgt.

C.3 Aufbau der Grafik bei HHD_{OPT}

Bei HHD_{OPT} sind die optischen Empfangselemente an einer der vier Seitenflächen angereicht, wie die folgende Darstellung am Beispiel einer Integration auf einer Querseite zeigt:

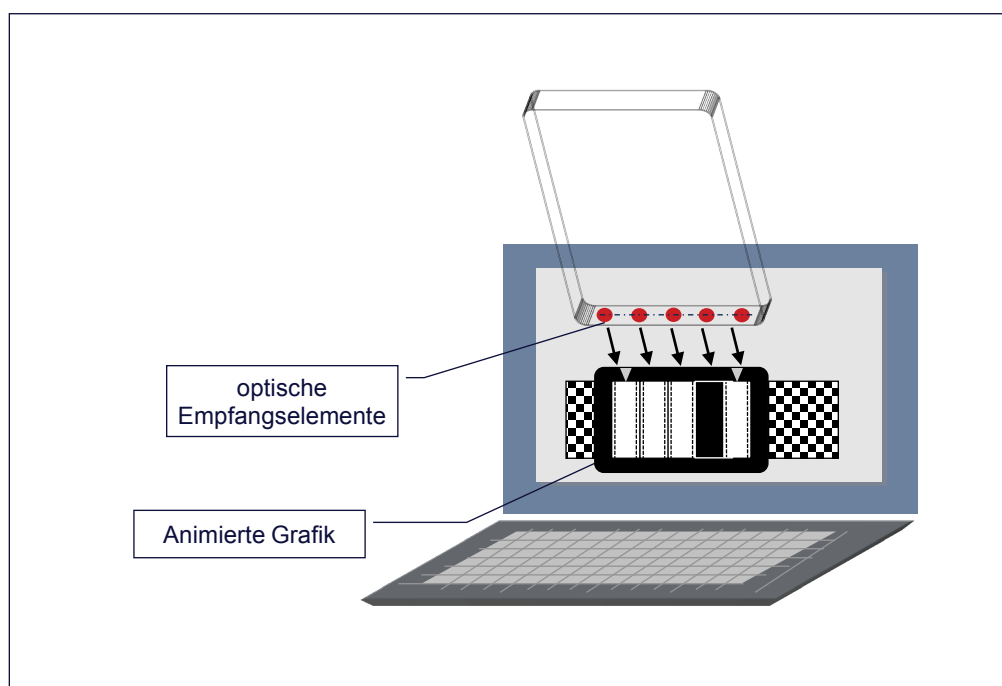


Abbildung 3: Beispielhafte Positionierung des Standard HHD_{OPT} am Bildschirm

Grafikaufbau bei HHD_{OPT}

Die folgende Abbildung zeigt den Aufbau der animierten Grafik mit beispielhaften Abmessungen in Millimetern. Die realen Abmessungen werden anhand der zu unterstützenden Bildschirmauflösungen und Geräte optimiert und können von diesem Beispiel abweichen. Die Größe der Grafik kann mittels der Kalibrierungsfunktion (vgl. Abschnitt C.1.1) an die physikalischen Maße des konkreten Gerätes bei der gewählten Bildschirmauflösung angepasst werden.

Die eigentliche animierte Grafik wird durch einen schwarzen Rahmen eingefasst, um zum einen ein ruhigeres Erscheinungsbild zu erreichen und zum anderen einen definierten Abschluss des Messbereiches zu erhalten. In den Rahmen sind zwei weiße Markierungen integriert, die zur einfachen Positionierung des HHD_{OPT} dienen sollen (vgl. hierzu auch Abschnitt C.1).

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: C
Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Aufbau der Grafik bei HHD _{OPT}	Stand: 07.05.2010	Seite: 23

Die fünf animierten Grafikbestandteile werden durch schwarze Balken getrennt, um Übersprecheffekte zu minimieren.

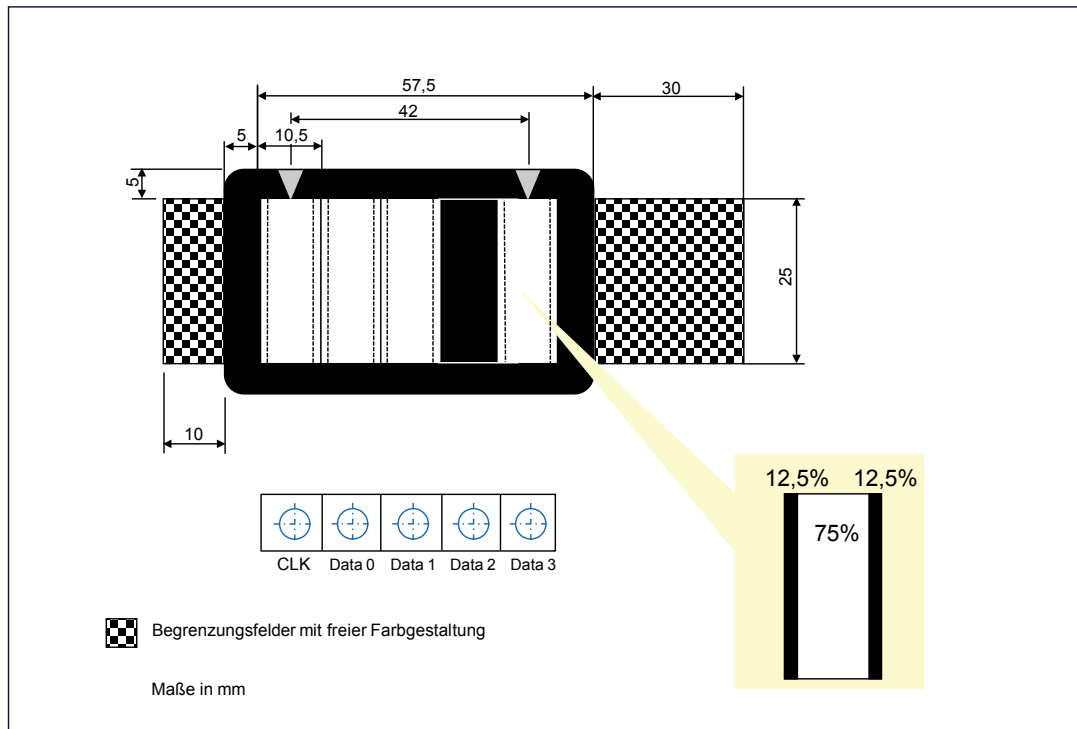


Abbildung 4: Aufbau der animierten Grafik bei HHD_{OPT}

Ablauf

Der Takt wird ständig in der vom System (Flash[®], JavaScript, Animated GIF, Monitorwiederholfrequenz, Grafikkarte etc.) möglichen Frequenz angesteuert (Wechsel schwarz/weiß).

Die Abfolge beginnt mit einem SYNC-Pattern, wie es in Abschnitt C.2 dargestellt wurde.

Mit der nun nachfolgenden ansteigenden Flanke des CLK-Signals werden die einzelnen Flächen der Datenbits auf den gewünschten Wert („1“ oder „0“) gesetzt und vom Leser mit einer gewissen Verzögerung (Ausblendung des Einschwingverhaltens), z. B. mit der abfallenden Flanke des CLK-Signals abgetastet.

Während die Anzahl und Bedeutung der optischen Elemente sowie der zeitliche Ablauf Inhalt der vorliegenden Spezifikation sind und Instituts-seitig garantiert werden müssen, sind die Verfahren der Messung im HHD_{OPT} (z. B. Messung bei aufsteigender und/oder abfallender Flanke) herstellerspezifisch zu lösen.

Kapitel:	C	Version:	V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung
Seite:	24	Stand:	07.05.2010	Dokument: HHD-Erweiterung für unidirektionale Kopplung
		Kapitel:	Spezielle Festlegungen zur optischen HHDUC-Kopplung	
		Abschnitt:	Aufbau der Grafik bei HHD _{OPT}	

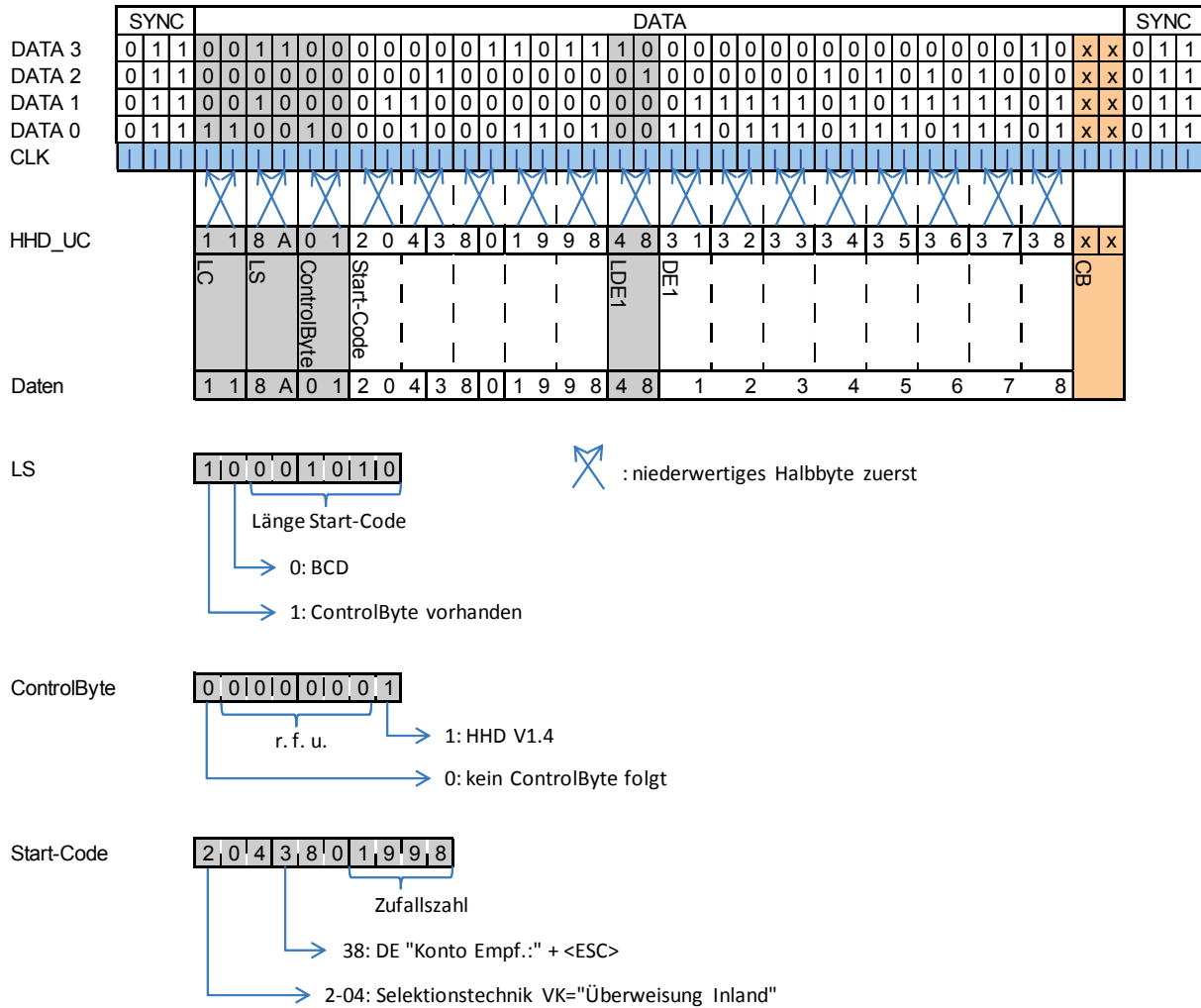


Abbildung 5: Beispiel für den zeitlichen Ablauf beim Standard HHD_{OPT}

C.4 Anhang

C.4.1 Beispiel für die Prüfsummenbildung

- ◆ Beispiel für die Prüfsummenbildung auf Basis von HHD V1.4:

Für das Beispiel werden folgende Werte zugrunde gelegt:

LC = 16	Wert	0b00010000
L(Start-Code) = 5	Wert	0b10000101
ControlByte	Wert	0x01
Start-Code	Wert	2082901998
	Format	BCD
L(Datenelement 1) = 8	Wert	0b01001000
Datenelement 1	Wert	IE99BOFI
	Format	ASC

Der Übertragungsblock hat dann – ohne Berücksichtigung des Startkriteriums – folgenden Aufbau:

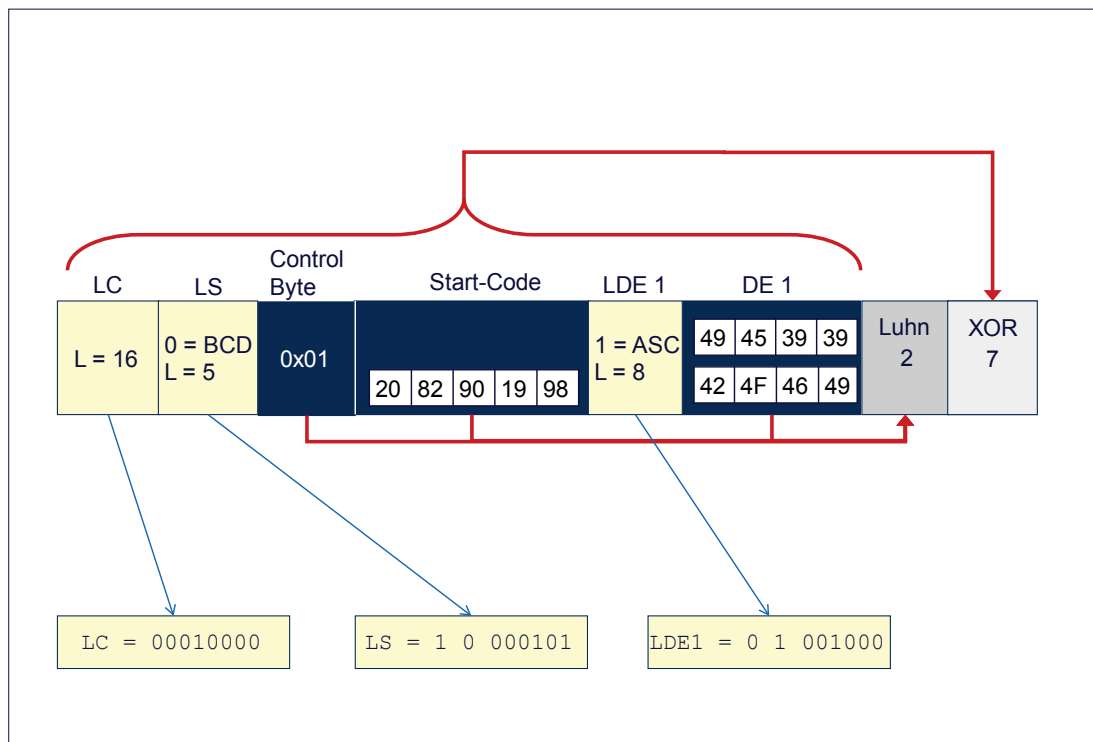


Abbildung 6: Beispiel zur Prüfziffernberechnung bei HHD_{UC} V1.4

Kapitel: C	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 26	Stand: 07.05.2010	Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Anhang

Für die Bildung der Prüfziffer sind zwei Arbeitsgänge notwendig.

Prüfsummenbildung Schritt 1 (linkes Halbbyte): Bildung der Luhn-Prüfziffer

In einem ersten Schritt wird zur Bildung des linken Halbbytes die Luhn-Prüfziffer über folgende Datenstruktur berechnet:

Element	Format	Daten
ControlByte		01
Start-Code	BCD	20 82 90 19 98
Datenelement 1	ASC	49 45 39 39 42 4F 46 49

Die Luhn-Prüfziffer wird wie folgt aufgebaut (die Aufteilung in 2 Teiloperationen wurde nur aus redaktionellen Gründen vorgenommen):

ControlByte und Start-Code (BCD)													Σ
	0	1	2	0	8	2	9	0	1	9	9	8	
		x2		x2		x2		x2		x2		x2	
	2		0		4		0		(1+8)		(1+6)		
	0	2	2	0	8	4	9	0	1	9	9	7	

Datenelement 1 (ASC)														Σ		
4	9	4	5	3	9	3	9	4	2	4	F	4	6	4	9	
	x2		x2		x2		x2		x2		x2		x2		x2	
(1+8)		(1+0)		(1+8)		(1+8)		4		(3+0)		(1+2)		(1+8)		
4	9	4	1	3	9	3	9	4	4	4	3	4	3	4	9	
Luhn-Prüfziffer = 130 - 128 = 2													Σ	128		

Prüfsummenbildung Schritt 2 (rechtes Halbbyte): XOR-Operation

In einem zweiten Schritt wird das rechte Halbbyte mit einer XOR-Operation berechnet (Die Aufteilung in 2 XOR-Operationen geschieht hier nur aus redaktionellen Gründen):

XOR-Operation Teil 1: XOR-Teilsumme über den Start-Code

Element	Daten	binär			
LC	16	0	0	0	1
		0	0	0	0
LS	5	1	0	0	0
		0	1	0	1
ControlByte	0x01	0	0	0	0
		0	0	0	1
Start-Code	2	0	0	1	0

HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung	Version: V 1.4	Kapitel: C
Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Anhang	Stand: 07.05.2010	Seite: 27

Element	Daten	binär			
	0	0	0	0	0
	8	1	0	0	0
	2	0	0	1	0
	9	1	0	0	1
	0	0	0	0	0
	1	0	0	0	1
	9	1	0	0	1
	9	1	0	0	1
	8	1	0	0	0
XOR-Teilsumme		0	1	0	1

XOR-Operation Teil 2: XOR-Teilsumme über das Datenelement 1:

Element	Daten	ASC	binär			
XOR-Übertrag			0	1	0	1
LDE1	8		0	1	0	0
			1	0	0	0
BDE1	I	4	0	1	0	0
		9	1	0	0	1
	E	4	0	1	0	0
		5	0	1	0	1
	9	3	0	0	1	1
		9	1	0	0	1
	9	3	0	0	1	1
		9	1	0	0	1
	B	4	0	1	0	0
		2	0	0	1	0
	O	4	0	1	0	0
		F	1	1	1	1
	F	4	0	1	0	0
		6	0	1	1	0
I	4	0	1	0	0	
	9	1	0	0	1	
XOR-Summe			0	1	1	1

Somit ist das Ergebnis der XOR-Operation: **7**

Damit ergibt sich für die Prüfziffer der Wert **27**.

Kapitel: C	Version: V 1.4	HandHeld-Device (HHD) zur TAN-Erzeugung Dokument: HHD-Erweiterung für unidirektionale Kopplung
Seite: 28	Stand: 07.05.2010	Kapitel: Spezielle Festlegungen zur optischen HHDUC-Kopplung Abschnitt: Anhang

C.4.2 Eigenschaften der möglichen Grafikformate bei optischer Kopplung

Im Folgenden werden die Eigenschaften der möglichen Grafikformate für die Verwendung im Rahmen der optischen Kopplung beschrieben.

Welches Verfahren konkret in der jeweiligen Kundensituation zum Einsatz kommt, ist implementierungsabhängig und wird von der jeweiligen Aufbereitungssoftware auf Kreditinstitutsseite bzw. im Kundenprodukt entschieden. Ggf. kann auch ein Entscheidungsbaum verwendet werden, der z. B. anhand der ermittelten Browsereinstellungen das geeignete Verfahren auswählt. In jedem Fall sollte die Auswahl des Grafikformates für den Kunden transparent und nicht mit administrativen Tätigkeiten verbunden sein. Die Ausführungen gelten auch für Kundenprodukte, wenn diese entweder die Standards / Produkte native unterstützen oder entsprechende Browserbibliotheken einbinden.

C.4.2.1 Adobe® Flash®

Mit diesem Verfahren lassen sich die kleinsten und schnellsten Grafiken erzeugen. Allerdings ist für die Wiedergabe die einmalige Installation des Adobe® Flash®-Players Voraussetzung. Durch die genannten Eigenschaften und das gute Performanceverhalten bei der dynamischen Erzeugung durch Parametrisierung einer einmal erstellten Klasse gelingt mit diesem Verfahren eine optimale Umsetzung der optischen Kopplung.

Allerdings ist für den Einsatz des Adobe® Flash®-Verfahrens die Freischaltung dynamischer Komponenten im Browser Voraussetzung. Ist dies nicht gewünscht oder wird der Einsatz von Flash-Komponenten von einem Institut nicht empfohlen, so muss auf eine der beiden anderen Varianten ausgewichen werden.

C.4.2.2 JavaScript

Der Einsatz von JavaScript setzt voraus, dass diese Darstellungsmöglichkeit im Browser am Kundenendgerät aktiviert ist. Ist dies der Fall, besitzt JavaScript ebenfalls hinreichend gute Eigenschaften in Bezug auf die dargestellten Anforderungen.

C.4.2.3 Animated GIF

Da für dieses Verfahren keine Systemvoraussetzungen bestehen und auch keine Einstellungen im Browser vorgenommen werden müssen, kann dieses Grafikformat unabhängig von den Browsereinstellungen zum Einsatz gelangen.

Nachteil von Animated GIF ist die Tatsache, dass eine GIF-Grafik komplett am Webserver aufgebaut werden muss und keine dynamischen Funktionen im Browser z. B. für die Änderung der Grafikgröße abhängig von der Bildschirmauflösung herangezogen werden können. Außerdem ist die Geschwindigkeit bei diesem Verfahren vergleichsweise niedrig.

C.4.2.4 Sun Java®

Sun Java® erfüllt zwar die geforderten Eigenschaften hinsichtlich Performance und Schnelligkeit, setzt aber die Installation einer Sun Java® Virtual Machine und deren Laden zur Laufzeit voraus, was dieses Verfahren für einen Einsatz als HHD_{OPT} nur in Java-Applikationen als sinnvoll erscheinen lässt.