HandHeld-Device (HHD)

for the generation of an OTP

HHD enhancement for optical interfaces

HandHeld-Device (HHD) for generation of an OTP		Version:		Chapter:
Document: HHD enhancement for optical interfaces		V 1.5.1		A
Chapter: Introduction		Status as of: 5.06.2018		Page: 3

Contents

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
A	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Introduction
4	5.06.2018	

Table of figures

References

[HHD 1.3]   Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDe-
                    vice (HHD) zur TAN-Erzeugung, Version 1.3, 26.10.2007, Final
                    Version, Zentraler Kreditausschuss

[HHD 1.3.2]   Schnittstellenspezifikation für die ZKA-Chipkarte - HandHeldDe-
                    vice (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 - HandHeldDe-
                    vice (HHD) zur TAN-Erzeugung, Version 1.4 Final Version,
                    07.05.2010, Zentraler Kreditausschuss

[Belegung 1.4.1] ZKA-TAN-Generator – Belegungsrichtlinien für die Dynamisierung
                    der TAN, Version 1.4.1 Final Draft, 04.10.2013, Die Deutsche Kre-
                    ditwirtschaft

[Belegung 1.5]   Belegungsrichtlinien für das chipTAN-Verfahren, Version 1.5,
                    1.Draft, Stand 16.02.2018, Die Deutsche Kreditwirtschaft

[S3G-Ctn]   Specifications of the Secoder 3G, Secoder Application chipTAN,
                    Version 1.2, 21.09.2016 (or higher)

[ISO18004]   ISO/IEC 18004:2000: Information Technology – Automatic Identifi-
                    cation and data capture techniques – Bar code symbology –
                    QR code

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
A	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Introduction
6	5.06.2018	

A. INTRODUCTION

This specification describes the transmission of data in the form of a unidirectional optical coupling (hereinafter referred to as HHD_{UC} for HHD – unidirectionally coupled). The device control itself as well as the type of visualisation is not part of this document, but of the respective specification of a HandHeldDevice (HHD)[1] (see [S3G-Ctn]).

The HandHeld-Device can be used via a HHD_{UC} application interface specified in [Belegung 1.4.1] for FinTS customer products or the specific Internet banking applications of credit institutions.

Devices with a display and keyboard that meet the specifications of the respective HHD specification serve as the hardware basis for the HandHeldDevice or Secoder. With HHD_{UC}, regardless of the connection type, the data is only transmitted in one direction, namely from the access device to the HHD/Secoder and is then confirmed by the operator there. A concrete example for a unidirectional coupling is the optical transmission by means of an animated graphic.

The specification is divided into three sections:

- General specifications which are valid independently of the transmission protocol.

- Particular specifications for the use of an optical coupling method using animated graphics.

- Particular specifications when using methods based on "photographing a matrix code".

The aim of this standardisation attempt is to create, on the basis of as few variants as possible, a method which may ensure that every Internet banking application and every FinTS customer system can be used with every HHD_{UC} available on the market and that manufacturer-specific characteristics can be avoided.

The specifications are supplementary to the Secoder or HHD specification. All other mechanisms and features not explicitly mentioned are maintained as described in the corresponding specifications.

---

[1] The term HandHeldDevice (HHD) is still used in this version of the document due to historical reasons, but in this version it is used for a Secoder 3 reader with the Secoder application chipTAN (ctn). The specifications for the Secoder 3 form the basis for the corresponding reader devices.

HandHeld-Device (HHD) for generation of an OTP		Version:	Chapter:
Document: HHD enhancement for optical interfaces		V 1.5.1	B
Chapter: General specifications for HHDUC		Status as of: 5.06.2018	Page: 7

B. GENERAL SPECIFICATIONS FOR HHD$_{UC}$

The use of devices with unidirectional coupling and the associated characteristics are described in the respective HHD standard. This specification, however, describes the (unidirectional) transmission protocol. This version of the HHD$_{UC}$ specification describes the transmission using the concrete example of HHD V1.4, as it was also adopted in the specifications for Secoder 3 (see [S3G-Ctn]). The specifications for HHD V1.3 can be found in the HHD$_{UC}$ specification HHDUC V1.0.1 and are no longer subject of this consideration. However, the description of HHD$_{UC}$ V1.4 is strictly backward compatible with HHD$_{UC}$ V1.01 with regard to the HHDUC devices, i.e. no specifications are made which are inconsistent with HHD$_{UC}$ V1.0.1 or HHD V1.3. Furthermore, the protocol mechanisms of HHD$_{UC}$ V1.0.1 are used as unmodified as possible.

The processes for manual and coupled operation differ in a number of basic properties.

More specifically, this means that only user guidance information is displayed on the customer's device, while the actual transaction data is transmitted via a communication link to the HHD$_{UC}$, where it is shown to the customer on the display.

The use of a HHD$_{UC}$ therefore requires some enhancements compared to manual operation:

- The HHD$_{UC}$ must be able to transmit the entire Challenge data from the customer device in one or more communication steps and then individually show it to the customer via display and keyboard.

- If several communication steps are required for the transmission of the challenge, the entire challenge must be assembled internally from the individual communication steps before the actual processing of the challenge is continued.

- The customer must be informed of the operating status and the status of the transmission.

- Since on the one hand transmission components have to be operated and on the other hand there is no direct connection to the customer's device to charge a rechargeable battery, there must be ways of minimising the energy requirement for the transmission components.

- There are cancellation scenarios that may especially occur in coupled operation.

B.1 Standard procedures

The following standard procedures result from the specifications of the HHD specification and are intended to illustrate the differences between manual and coupled operation using HHD V1.4 as an example.

The codes and key assignments used refer to this HHD specification and may only be considered as examples (see section „B.2.1").

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
B	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: General specifications for HHDUC
8	5.06.2018	

B.1.1 HHD V1.4 Procedure for manually entering start code and data

The following procedure shows the process of entering start code and transaction data using HHD V1.4 as an example. In this specific case, the start code "104xxxx" is used to select the template "104" to confirm an individual domestic transfer:

Procedure	Display indication
Inserting the smart card	none or text
Pressing the "TAN" key	Start-Code
Pressing numeric keys (max. 12), confirming with " confirm " key	Start-Code 104xxxx
Accepting with „confirm" key	Überweisung Inland
Input of further values depending on the selected template	Konto Empf.: BLZ Empf.: Betrag
Press the "confirm" key to confirm the entry and the TAN will be displayed	Überweisung TAN: 361620

Characteristic of the standard HHD procedure is that the start code and the transaction data have to be entered in separate steps, in which the customer must actively enter and confirm data each time. The output in the first line of the data entry screen depends on the first two to nine digits of the previously entered start code.

While the customer can take the start code from the screen of his device, he is required to take the transaction value(s) from his payment receipt.

As a result, a TAN is generated, which is shown on the HHD display and which the customer must enter in the corresponding field of his device.

HandHeld-Device (HHD) for generation of an OTP	Version:	Chapter:
Document: HHD enhancement for optical interfaces	V 1.5.1	B
Chapter: General specifications for HHDUC	Status as of: 5.06.2018	Page: 9

B.1.2 HHD V1.4 Procedure for coupled operation

The communication sequence shown below illustrates the HHD$_{UC}$ sequence extended by the transfer function using the example of an optical coupling using animated graphics.

Procedure	Display indication
Inserting the smart card	none or text
Starting the transfer functio	**Übertragung aktiviert**
during data transmission	**Übertragung** ‖‖‖‖‖
All data bytes transferred, check digit OK: The transmitted start code is not displayed, but is transparently included in the TAN calculation later.	**Übertragung erfolgreich**
Accept with "confirm" key	**Überweisung Inland**
Confirmation of further values depending on the selected template	**Konto Empf.: 12345678** **BLZ Empf.: 70020245** **Betrag 22,45**
Approve by pressing the "confirm" key, then the TAN is displayed	**Überweisung TAN: 472733**

As shown in the figure, the process is divided into the transmission phase and the confirmation phase.

Transmission phase

At the beginning of the transmission phase, the transmission unit is activated by pressing the start button of the transmission function ("F" or "TAN" button, see [S3G-Ctn]) once. During transmission, status information is shown on the HHD$_{UC}$ display. The successful transmission phase is completed with the text "Transmission successful" shown on the display.

When using a procedure based on photographing a matrix code, the transfer phase consists of photographing the matrix code. In this case, the successful transmission

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
B	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: General specifications for HHDUC
10	5.06.2018	

phase is also completed with the text "Transmission successful" shown on the display.

The transmission phase includes the verification of the correct transmission according to section B.2.4. If a transmission error is detected, the transmission phase is canceled and the display text "Transmission canceled" is shown. See also section B.3.1.

Confirmation phase

In the subsequent confirmation phase, the transaction data is displayed element by element. The customer's "input data" is taken from the transmitted data and the customer only needs to confirm it after verifying it with the original voucher.

The start code, which creates Freshness and controls the dialog flow, has no other business relevance and is therefore not displayed to the customer in the standard case (exceptions see [S3G-Ctn]); however, it is taken into account in the subsequent TAN calculation.

B.2   Data transfer protocol

The data transfer protocol is kept very compact so that there are no excessive transmission times even when using narrow-band transmission protocols.

As for HHD V1.3.2, the data protocol follows a fixed structure comprising start code and two data elements including the respective length fields (see [HHD$_{UC}$ 1.0.1]). The data transfer protocol according to HHD$_{UC}$ V1.0.1 is no longer part of this specification, but completely supported to ensure backward compatibility.

With HHD$_{UC}$ Version 1.4, the structure of the protocol has changed to allow data structures with different structures to be transferred. Now a ControlByte follows the field for the length of the start code, which can branch to data patterns of different structure. A defined bit combination in the length field of the start code determines the validity of the ControlByte. This also ensures compatibility with HHD$_{UC}$ V1.0.1.

From HHD V1.4, the data structures can be defined individually to a certain extent:

Start criterion	HHD$_{uc}$ data block	AMS data block (optional)

The start criterion depends on the concrete transmission procedure. If an AMS data block exists, it directly follows the HHD$_{UC}$ data block, which means that there must be no start criterion between the two data blocks.
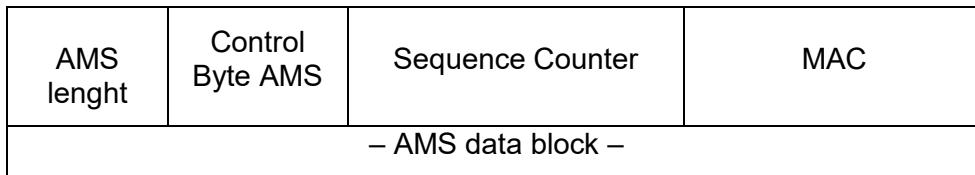
The HHD$_{UC}$ data block has the following structure:

HHDuc lenght	Start code lenght	Control Byte HHDuc	Data record structure analog Control	Check digit
– HHDuc data block –				

Content and structure of the HHD$_{UC}$ data block is described in the document [S3G-Ctn] (section 9.3).

The optional AMS data block has the following structure:

AMS lenght	Control Byte AMS	Sequence Counter	MAC
– AMS data block –			

Content and general structure of the AMS data block is also described in the document [S3G-Ctn] (section 9.3). The exact coding of individual fields may depend on the specific transfer protocol.

B.2.1 Degrees of freedom and restrictions in data record setup from HHD V1.4

The control of different data structures via the ControlByte results in the following:

- Security medium
  When using HHD, a bank smart card with the SECCOS operating system is used. The DK EMV TAN generator (DK EMV AC application) is used to generate the TANs.

- Visualisation
  When using HHD with ControlByte 0x01, the general visualisation concept for HHD is used (see [S3G-Ctn]), alternatively a visualisation structure corresponding to the ControlByte is used.

- Included fields and their content
  The data structure can contain any fields which have to be documented in the description. It must also be defined how the fields shall be filled depending on the purpose.

- Data lenght
  The maximum physical data length of the HHD_{UC} data block is 255 bytes. The respective logical maximum value must be defined in the description of an HHD variant defined by the ControlByte.

- An ASCII character set (cf. [S3G-Ctn]), which the HHD supports, must be used; the character set can be adapted to the respective purpose.

- The HHD_{UC} application interface (see [Belegung 1.4.1]) can be used optionally. In case usage is required, a corresponding specification of the elements "Challenge" and "Challenge HHD_{UC}" is required.

The meaning of the individual components of the HHD_{UC} data block is described in the following sections.

B.2.2 HHD$_{UC}$ header and trailer from HHD V1.4

As of version 1.4.2 of this document, the contents of this section are included in document [S3G-Ctn] (section 9.3).

B.2.3 HHD$_{UC}$ Body for HHD V1.4 (Control = 0x01)

As of version 1.4.2 of this document, the contents of this section are included in document [S3G-Ctn] (section 9.3).

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
B	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: General specifications for HHDUC
12	5.06.2018	

B.2.4 Checksum calculation for HHD$_{UC}$

As of version 1.4.2 of this document, the contents of this section are included in document [S3G-Ctn] (section 9.3).

B.3 Further protocol characteristics

B.3.1 Protocol specifications
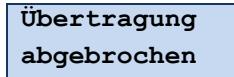
After receiving the start criterion, the HHD$_{UC}$ waits until the entire HHD$_{UC}$ data block has been received completely and without interruption. The length of the HHD$_{UC}$ data block results from its first byte (HHD$_{UC}$ length). If further data follows after the HHD$_{UC}$ data block (i.e. a start criterion does not follow directly), the AMS data block is also read in. The length of the AMS data block results from its first byte (AMS length).

After receiving the HHD$_{UC}$ data block, it is reviewed for errors using the procedure described in Section B.2.4.

If the result of the recalculation is negative, the terminal waits for the detection of the start criterion to repeat the process. The display of the transmission status also starts at 0% again after detecting the start criterion (and the directly following challenge length). If the HHD$_{UC}$ data block has to be read in again, the AMS data block is also read in again.

This process is canceled if the CheckSum is recalculated correctly or after a total of five unsuccessful attempts.

If an error occurs, the following message is displayed:

```
Übertragung
abgebrochen
```

The display of the respective message can be interrupted by pressing the "Confirm" key or the "Cancel" key and the device is switched off; otherwise the device is switched off after a timeout of approx. 30 seconds.

B.3.2 Status informationen

In order to be able to quantitatively show the progress of the transmission on the display, the device must initially be able to determine the total length of the data to be transmitted. The AMS data block (if available) is not taken into account.

The data to be transferred contains both the total length of the HHD$_{UC}$ data block and the length of the individual elements. These allow the HHD$_{UC}$ to calculate the progress of the transmission in relation to the total length of the HHD$_{UC}$ data block.

With displaying the message

```
Übertragung
 ▌▌▌▌▌
```

the customer is informed about the transfer progress.

HandHeld-Device (HHD) for generation of an OTP	Version:	Chapter:
Document: HHD enhancement for optical interfaces	V 1.5.1	B
Chapter: General specifications for HHDUC	Status as of: 5.06.2018	Page: 13

B.3.3 Energy management

The communication module must be in permanent operating mode during operation, which results in a correspondingly high power requirement. Thus, the communication block should only be activated consciously when required, and deactivated at the earliest possible time (e.g. after successful check of the CheckByte). The operator can therefore decide at the beginning whether he wants to carry out the TAN generation by entering the context-sensitive data via the device keyboard (initiate the process by pressing the TAN key of HHD V1.4 in the standard layout) or to use the communication module for this purpose (initiate the process by pressing the "F" key of HHD V1.4 in the standard layout). The respective HHD specification describes which keys or functions are specifically used.

B.3.4 Cancelation scenarios

By pressing the "Cancel" key, the process is cancelled. It is irrelevant if the transmission has just been activated, is still active (display of the percentage value of the transmission status) or if the transmitted data is already shown on the reader's display.

When the "Cancel" button is pressed, the following is always shown:

```
Vorgang
abgebrochen
```

The display of this message can be interrupted by pressing the "Confirm" key or the "Cancel" key and the device is switched off; otherwise the device is switched off after a timeout of approx. 30 seconds.

This means that an individual correction of the data transmitted via the communication interface is not possible.

If the HHD_{UC} is removed from the reception range during data transmission, a timeout of approx. 5 seconds is started. Within this time, the HHD_{UC} can be repositioned in the reception area to resume the data transmission process. In this case the HHD_{UC} waits for the detection of the start criterion again. After detecting the start criterion (and the directly following length of the HHD_{UC} data block) the display of the transmission status starts at 0% again.

If the timeout expires without resuming the transmission, the following message will be displayed:

```
Übertragung
abgebrochen
```

The same error message is displayed for each physical transmission error, even if, for example, a length field is incorrect. If the check digit is incorrect, cancelation follows after five unsuccessful attempts (cf. Section B.3.1)

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
C	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Particular specifications for optical HHDUC-coupling with
14	5.06.2018	animated graphics (HHDopt)

C. PARTICULAR SPECIFICATIONS FOR OPTICAL HHD$_{UC}$-COUPLING WITH ANIMATED GRAPHICS (HHD$_{OPT}$)

In the following, additional specifications regarding the use of an optical coupling based on animated graphics between the customer device and HHD$_{UC}$ - hereinafter referred to as HHD$_{OPT}$ - are defined. In this case, the communication link consists of an optical connection between the two parties. A dynamic graphic is displayed on the screen of the customer's device in which the data to be transmitted is coded so that it can be read by the optical receiver elements in the HHD$_{OPT}$. HHD$_{OPT}$ is a form of an optical coupling process. See section D for an alternative based on matrix codes. Further procedures can be added and described in a comparable way at a later date if the corresponding technologies are available.

With regard to the protocol, no additional specifications to the HHD$_{UC}$ specifications described in section B are required. When coding the data in the AMS data block (if available), however, the specifications in section C.5 must be met.

The optical coupling of the two devices is determined by a number of framework conditions that are intended to enable the manufacturer-independent operation of a HHD$_{OPT}$ with optical coupling.

C.1 Physical frameworks

To optically transfer the determined transaction data to HHD$_{OPT}$, a graphic compatible with the customer device must be generated dynamically. The following criteria are considered to be decisive:

- Dynamic processing must be fast and resource-saving; the resulting graphic must be as small as possible in terms of data volume.

- The medium used must allow the graphics to be transmitted as quickly as possible via the optical coupling path, i.e. the blink frequency must be as high as possible, with the result that the coordination between processor, graphics card, screen and presentation programme must be selected properly. The minimum and maximum blinking frequency to be supported is 2 Hz and 20 Hz.

- The generated graphic must be able to be displayed on any display, independently of . . .

    - the type of screen/display (CRT monitor, TFT, plasma, ...)

    - the size of the screen and

    - the chosen screen resolution.

- The standard HHD$_{OPT}$ must have two markings which indicate the position of the outer optical elements. These correspond to the marks in the standardised graphic (see section C.3) and facilitate the positioning by the customer.

- Depending on the implementation, the most suitable implementation method must be chosen. For sending transaction data using an animated graphic, the following options are available:

Depiction	System requirements on customer side
Adobe® Flash®	Adobe® Flash® player must be installed
JavaScript	JavaScript must be enabled in your browser
Animated GIF	none
Sun Java®	Java® Virtual Machine must be installed

More detailed information on the characteristics of the individual implementation options can be found in section C.6.2.

The optical characteristics of the HHD_{OPT} are determined by the following parameters:

- The physical characteristics of the selected optical receiving elements (e.g. photo transistors) with regard to energy consumption, characteristic curves and protection against crosstalk and ambient light. The manufacturer shall choose a proper solution.

- It is irrelevant whether the optical receiver elements are discrete or integrated components and the decision therefore depends on the manufacturer's cost and reliability considerations.

- Derived from the above, there are minimum distances between the optical receiving elements or the device size and their quantity. The device size can be determined by the manufacturer to a certain extent (see section C.1.1 "Calibration of the animated graphic"). For the number of optical elements, a quantity of 5 has proven to be the optimum in dialogue with different manufacturers and is used as fixed value in the specification.

Since a manufacturer-independent design of the optical coupling is to be obtained, the following chapters describe the operation of an HHD_{OPT}:

Before a product can be used as HHD_{OPT}, it must be ensured that the dynamic graphics shown below can be reliably interpreted in the supported formats of the design type.

C.1.1 Calibration of the animated graphics

The objective of the presentation of the animated graphic is the proper presentation on any screen for any product without manual customer intervention. However, since the size of the devices is not fixed and not every graphic format (e.g. Animated GIF) is scaleable, the customer may have to adjust the animated graphic to the size of the HHD_{OPT} or the screen resolution.

Depending on the display format used, this calibration can be performed locally in the browser (e.g. JavaScript) or on the web server (e.g. Animated GIF) (see appendix).

Depending on the implementation, the calibration can be carried out by "dragging" the graphic on specially marked fields or by using icons such as a large and a small magnifying glass.

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
C	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Particular specifications for optical HHDUC-coupling with
16	5.06.2018	animated graphics (HHDopt)

C.1.2 Required limitation of display duration and size

In order to avoid that the customer may suffer from epileptic symptoms, the following general conditions must be adhered to when displaying the animated graphic:

Display duration:

The display duration must not exceed 60 seconds. After this time has elapsed, the animation must be stopped automatically and the customer must be offered a suitable control element for a restart.

Size limitation:

The size of the animated graphic must be adjustable within specific limits in order to support products of different designs. If the size is increased by more than 50% of the initial size of the animated graphic, a corresponding warning is to be issued and only after the customer has confirmed this warning he can continue with further enlargement.

C.2 General HHD$_{OPT}$ definitions

The following specifications apply to the signals used and their meaning.

Designation	Information
CLK	Data channel with clocking for data transmission; at each transition "1" $\rightarrow$ "0" data is accepted.
SYNC	SYNC pattern that serves as start-detection.
Data 0 … 3	Bit values of a half-byte to be transmitted in a data channel

Also, the following applies:

white (high) = '1'
black (low)   = '0'

For each data byte, the least significant half-byte is transmitted first.

The values of the data fields related to the respective half-byte are as follows:

Data 0: Value = 2^0

Data 1: Value = 2^1

Data 2: Value = 2^2

Data 3: Value = 2^3

Synchronisation

A defined SYNC pattern is used to detect the beginning of a message in idle mode.
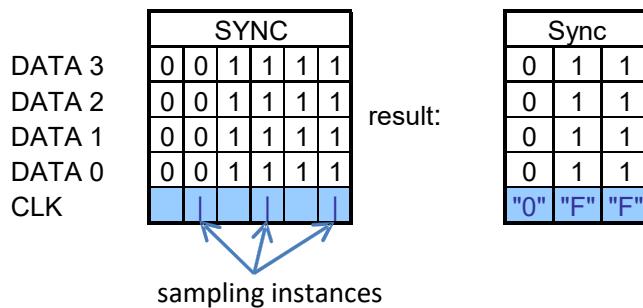
Figure 1: SYNC pattern

Since the data is only accepted at the sampling time ⊓ with a falling edge, the character sequence "0FF" results.

This pattern "0FF" must not occur in the area of the length fields, data and check digit. For the data of the HHDuc data block this is guaranteed by its construction and coding of the data elements contained. If the data to be transmitted contains an AMS data block this has to be ensured by the implementation. See section C.5 for details how this has to be handled.

During synchronisation, the CLK signal continues to operate to allow continuous clocking of the internal processes. The SYNC pattern shown in the figure above en-sures that the synchronisation point can be located reliably, since within the byte sequence a defined change from "1" to "0" occurs in all data channels.

C.3   Composition of the Animated Graphic for HHD$_{OPT}$

For HHD$_{OPT}$, the optical elements used for receiving the data are arranged on one of the four sides, as the following illustration shows using the example of an integration at one of the sides:
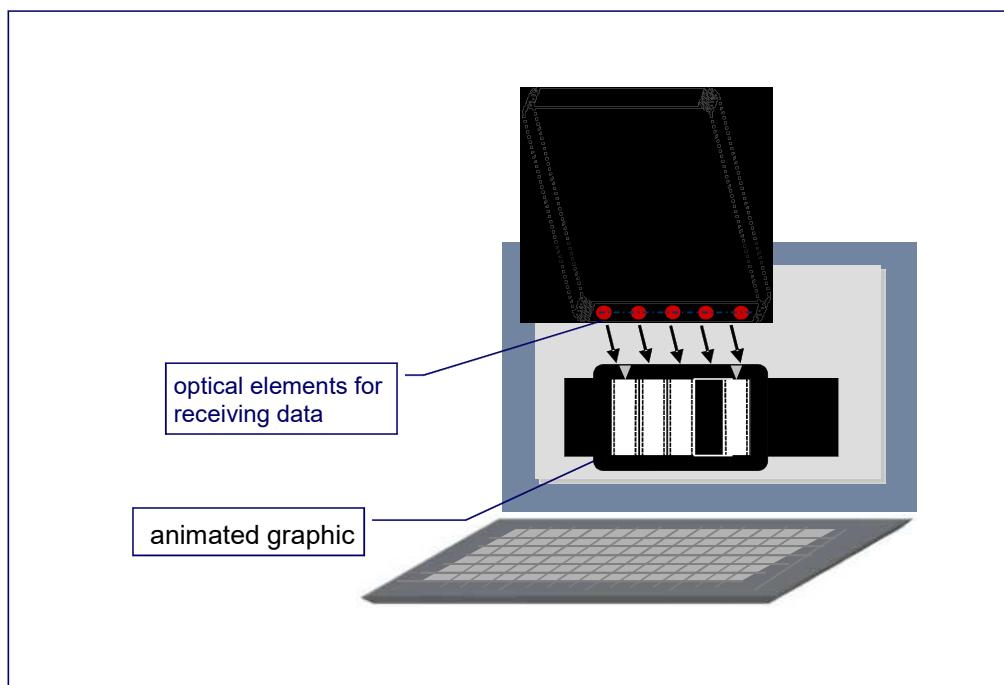

Figure 2: Example positioning of the standard HHD$_{OPT}$ on the screen

HHD$_{OPT}$ graphic structure

The following figure shows the structure of the animated graphic with exemplary dimensions in millimetres. The real dimensions are optimised on the basis of the screen resolutions and devices to be supported and may deviate from this example. The size of the graphic can be adapted to the physical dimensions of the specific device at the selected screen resolution using the calibration function (see section C.1.1).

The actual animated graphic is framed by a black frame in order to achieve a smoother appearance on the one hand and to achieve a defined end of the measuring range on the other hand. Two white markings are integrated in the frame to facilitate the positioning of the HHD$_{OPT}$ (see also section C.1).

The five animated graphic components are separated by black bars to reduce crosstalk effects.
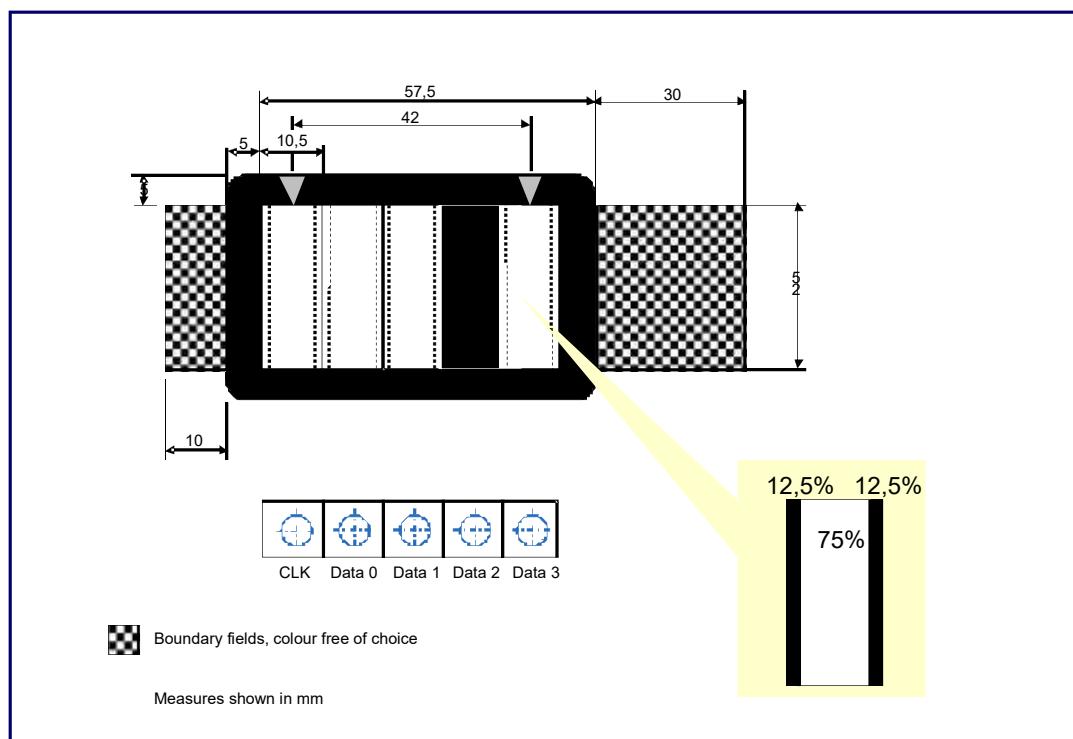
Figure 3: Structure of the animated HHD$_{OPT}$ graphics

Procedure

The clock pulse (change between black and white) is constantly controlled by the frequency of the system (Flash®, JavaScript, Animated GIF, monitor repetition frequency, graphics card, etc.).

The sequence begins with a SYNC pattern, as described in Section C.2.

With the following rising edge of the CLK signal, the individual data bit areas are set to the desired value ("1" or "0") and scanned by the device with a certain delay (suppression of the transient response), e.g. with the falling edge of the CLK signal.

While the quantity and significance of the optical elements as well as the time sequence are the subject of this specification and must be guaranteed by the implemented animated graphic, the procedures for measurement for reading the animat-

ed graphic (e.g. measurement with rising and/or falling edge) will be specific for each manufacturer of the HHD$_{OPT}$ device.
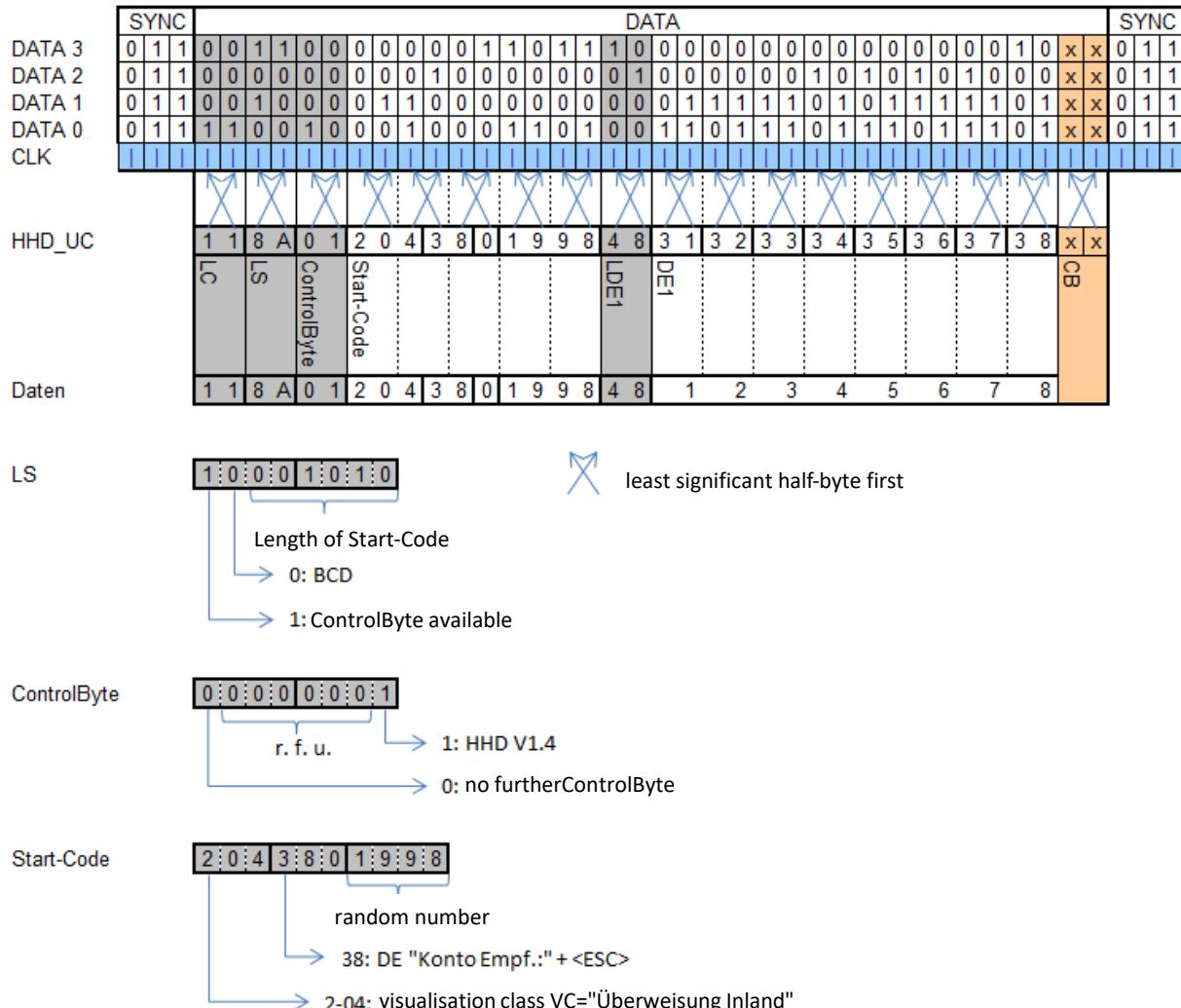
Figure 4: Time sequence example for the standard HHD$_{OPT}$ (i.e. without AMS data)

C.4 HHDuc data block restrictions

If the control byte of the HHDuc data block (field control at position 3) has the value 0x01, then this is data for the HHD procedure according to version 1.4.

When using HHD_{OPT}, the following restrictions apply in this case:

Not more than one of the data elements contained in the data block has a maximum length of 36 characters. The maximum length of this data element in bytes is 18 bytes for BCD coding and 36 bytes for ASCII coding. The other data elements have a maximum length of 12 characters. The maximum length of these other data elements in bytes is 6 bytes for BCD coding and 12 bytes for ASCII coding.

C.5 Coding of the AMS data block

Since the pattern "0FF" is used as a SYNC pattern (start recognition), this pattern must not be part of the AMS data block. However, this pattern can theoretically occur in the sequence counter and the MAC. To avoid this while using HHD_{OPT} in the extended HHDuc data block, the fields in position 8 (sequence counter) and position 9 (MAC) must not be encoded in 8-bit binary but in 7-bit binary.

To convert the fields in position 8 and 9 to a 7-bit encoding, both must be converted together (18 bytes) as described in section 9.3.1 of [S3G-Ctn]. The result then is 21 bytes long and replaces the fields at positions 8 and 9 in the extended HHDuc data block. Accordingly, AMS_Control.b5=1 and AMS_LC=22 must be set in the extended HHDuc data block (see the description of the extended HHDuc data block in section 9.3.1 of [S3G-Ctn]).

The described conversion of the extended HHDuc data block must be carried out before creating the animated graphic.

Note: If a Secoder receives an extended HHDuc data block with AMS_Control.b5=1, it internally resets the described conversion before further processing.

C.6 Annex

C.6.1 Example for the checksum calculation

As of version 1.4.2 of this document, this example is included in the document [S3G-Ctn] (Section 9.3).

C.6.2 Characteristics of the possible graphic formats for optical coupling

The following describes the characteristics of the possible graphic formats that can be used for optical coupling.

The method used in the respective customer situation depends on the specific implementation and is decided by the respective processing software on behalf of the bank or with regard to the customer product. If necessary, a decision tree can also be used, which, for example, selects the appropriate procedure on the basis of the identified browser settings. In any case, the choice of graphic format should always be transparent to the customer and not linked to administrative activities. The same applies to customer products that either support the standards / products natively or integrate corresponding browser libraries.

C.6.2.1 Adobe® Flash®

This method allows the generation of the smallest and fastest graphics. However, the Adobe® Flash® player must be installed first. Due to the mentioned characteristics and the good performance behaviour during the dynamic generation of a one-time created class by parameterisation, this method allows an optimal implementation of the optical coupling.

However, the use of the Adobe® Flash® method requires the activation of dynamic components in the browser. If this is not desired or if the use of Flash components is not recommended by an institute, either of the two other methods must be used.

C.6.2.2 JavaScript

The use of JavaScript requires the activation of this option in the browser of the access device. In this case, JavaScript also offers sufficiently good characteristics with regard to the specified requirements.

C.6.2.3 Animated GIF

Since this method does not require any system requirements or browser settings, this graphic format can be used independently from the browser settings.

However, the downside of Animated GIF is the fact that a GIF graphic must be built completely from the web server and no dynamic functions in the browser can be used, e.g. for changing the graphic size depending on the screen resolution. In addition, the operating speed of this method is comparatively low.

C.6.2.4 Sun Java®

Sun Java® meets the required performance and speed requirements, but requires the installation of a Sun Java® virtual machine and its loading at runtime, which makes the use of this method as HHD_{OPT} only useful in Java applications.

D. PARTICULAR SPECIFICATIONS FOR THE USE OF MATRIX CODES

If a chipTAN reader has a camera, the HHDuc data block and, if available, the AMS data block can also be transferred to the chipTAN reader by photographing a corresponding matrix code instead of using an animated graphic. This procedure is called HHD_{QR}, HHD_{FM} or HHD_{MC} (depending on the specific method used to generate the matrix code). When using a matrix code as part of the chipTAN procedure, the following aspects must be considered.

D.1 Reader requirements

The chipTAN reader for the HHD_{QR}, HHD_{FM} or HHD_{MC} procedure must be implemented as a stand-alone device in accordance with the specifications for Secoder 3 and contain the Secoder application chipTAN [S3G-Ctn]. The manufacturer must confirm this by means of an appropriate manufacturer's declaration.

The chipTAN reader must never be implemented as a simulation on a smartphone or any other device.

After extracting the HHD_{UC} data block and, if applicable, the AMS data block from the matrix code, further processing of the data must take place as described in [S3G-Ctn] or Chapter B of this specification.

HandHeld-Device (HHD) for generation of an OTP	Version:	Chapter:
Document: HHD enhancement for optical interfaces	V 1.5.1	D
Chapter: Particular specifications for the use of matrix codes	Status as of: 5.06.2018	Page: 23

D.2 QR Codes[1] (HHD$_{QR}$)

If the matrix code is generated according to the specification of a QR code (see www.qrcode.com), the procedure is referred to as HHD$_{QR}$. In this case, the following requirements must be met when generating the QR code.

D.2.1 General features

D.2.1.1 HHDuc data volume and QR Code size

The maximum size of a HHD$_{UC}$ data block including AMS is 150 bytes for HHD V1.4. Four BQR bytes and one byte AMS indicator are added, see section D.2.1.3. This is the scale for the required capacity and the associated version 8 of the QR code at ECC level L. If HHD V1.3.2 without AMS is used for a minimum consideration, the maximum size is 47 bytes (+ 4 BQR bytes + 1 AMS indicator byte).

Based on these sizes, a chipTAN reader must support the following versions (source: www.qrcode.com).

Version	Module	ECC Level	Binary data	Usage data (DE = data element)
4	33 x 33	L	78	HHD V1.3.2 + AMS
		M	62	HHD V1.3.2 / max. 1 DE + AMS, max. 2 DE
5	37 x 37	L	106	HHD V1.3.2 + AMS
		M	84	HHD V1.3.2 + AMS
6	41 x 41	L	134	HHD V1.4
		M	106	HHD V1.3.2 + AMS
7	45 x 45	L	154	HHD V1.4
		M	122	HHD V1.3.2 + AMS
8	49 x 49	L	192	HHD V1.4 + AMS
		M	152	HHD V1.4

Figure 5: Data capacity and versions of QR Codes

Note: For the calculation shown in the table, the parameters ECI mode according to [ISO18004] with value 1 for ISO-8859-1 character set and 8-bit byte mode for the user data were taken into account for generating the QR code.

Based on the required capacity, a smaller version with ECC level L(ow) (7%) should be preferred to a larger version with ECC level M(edium) (15%). In incorporation of logos (see section D.2.1.5) may require a larger version.

The QR code versions 4 to 8 and the ECC level L / M can be combined as desired.

When displaying the QR code, it is essential to ensure that each module of the QR code ALWAYS uses the same amount of pixels when it is displayed, i.e. there must be no mix of modules with e.g. 3 pixels and 4 pixels within a QR code.

---

[1] QR-Code is a registered trademark of DENSO WAVE Inc., it is free to use, but it must be referenced. See also:

https://register.dpma.de/DPMAregister/marke/registerHABM?AKZ=013123104&CURSOR=4

This may vary for different QR codes. However, at least 3 pixels per module should be used.

D.2.1.2 Positioning aid

For the most convenient user experience, a QR code reader may include a frame in the camera window to assist the user with positioning the camera. This may help the user to center the camera on the QR code. The necessity as well as the concrete design of the positioning aid is the responsibility of the chip-TAN reader manufacturer.

D.2.1.3 Identifier for Banking QR-Code (BQR)

Before starting the interpretation of the QR code, e.g. by verifying the optional AMS MAC - for this purpose an inserted smart card would have been accessed already - an identification mark for a banking QR code (abbreviation "BQR") is introduced. This identifier consists of a constant "DK" (2 bytes) at the beginning of the data stream and a 2 byte long CRC16 test value at the end. The resulting message is structured as follows:
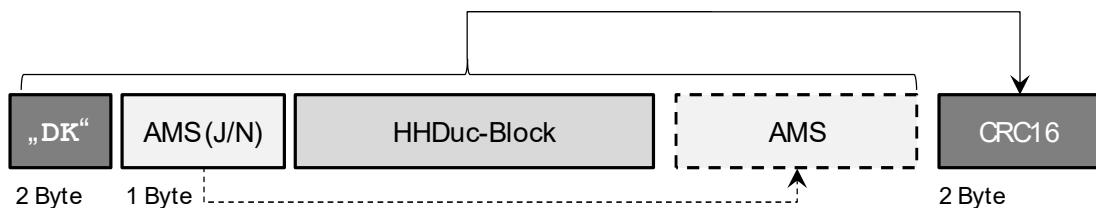
Figure 6: Structure of a banking QR-Code

The constant "DK" always marks a Banking QR code. If this constant occurs, the CRC16 test value must then be calculated and compared using the block described above. This concludes the BQR identification.

To determine the CRC check value, the following CRC-16 polynomial, starting with the least significant bit (LSB), is to be used:

$$x^{16} + x^{15} + x^2 + 1 = (x + 1)(x^{15} + x + 1)$$

The following specifications shall apply:

Initial value	0
Final XOR value	0
Data bytes inversion	N
CRC result inversion before final XOR	N

The smart card may only be accessed if the verification of BQR is successful. This avoids unnecessary access to the smart card.

HandHeld-Device (HHD) for generation of an OTP		Version:	Chapter:
Document: HHD enhancement for optical interfaces		V 1.5.1	D
Chapter: Particular specifications for the use of matrix codes		Status as of: 5.06.2018	Page: 25

The new CRC-protected AMS indicator introduced in the Banking QR code with the values "J" or "N" clearly indicates whether the data stream contains an AMS data structure or not.

Notes:

- The use of the Banking QR code does not serve to increase security, but protects a possibly inserted smart card from unnecessary accesses and increases the battery life of the reader device.

- A chipTAN reader can optionally be used to read standard QR codes (i.e. those without a BQR identifier) and show the result on the display. It is up to the manufacturer of the chipTAN reader if and in which form this function is made available.
  If the chipTAN reader cannot display a standard QR code, the following message must be shown and processing must be canceled if the verification of the BQR fails:

```
Kein Banking
QR-Code
```

D.2.1.4 Banking QR-Code scrambling

If the QR code is valid according to section D.2.1.3, which is the result of the BQR verification, the HHD_{UC} data must be made illegible before generating the QR code and transmitting it to the access device. Otherwise a user could discover financial data in the data stream when using a standard smartphone app, which could lead to irritation and uncertainty.

For making the data illegible, the data has to be XORed (two bytes by two bytes) with the fixed bytes "DK" (i.e. '44 4B').

This scrambling starts after the constant "DK" at the 3rd byte of the banking QR code and ends after the CRC test value.

Notes:

- This function does not increase security either.

D.2.1.5 Integrated image and logo support

In order to mark specific chipTAN QR codes as such, an operator can optionally integrate small images or logos.
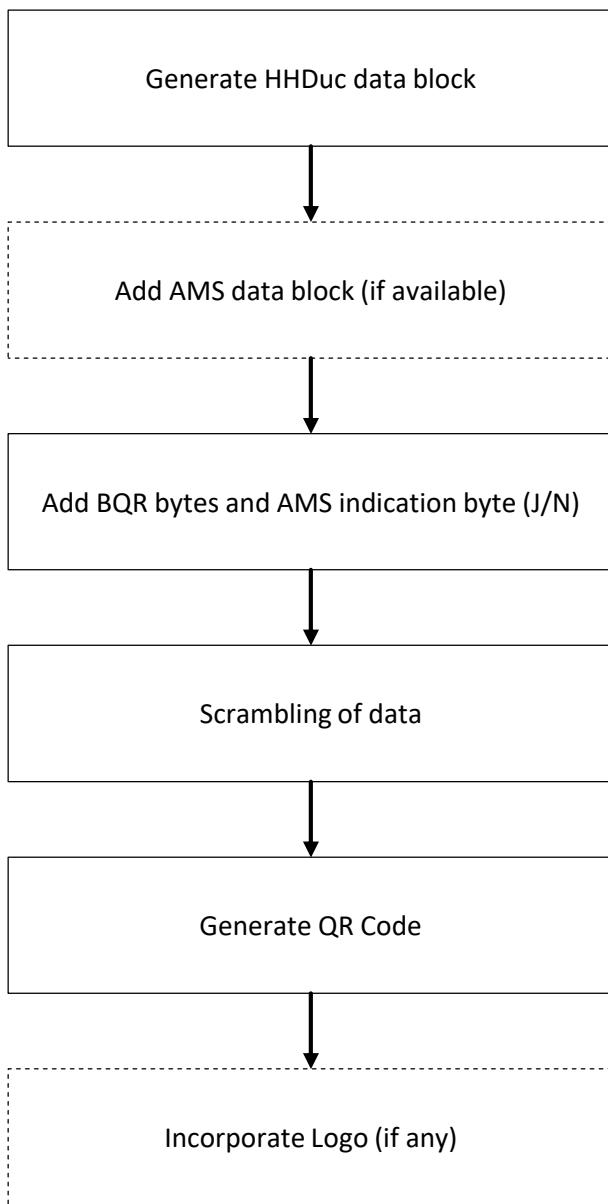
In any case, the type and size of such images can negatively affect the reading behaviour of the QR code and the battery life. The respective institute is responsible for ensuring that the highest possible reading process quality is achieved regarding all reader products used.

D.2.2 Procedure for generating a banking QR-Code

The following graphic shows the procedure for generating a banking QR code with all mandatory and optional substeps:

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
D	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Particular specifications for the use of matrix codes
26	5.06.2018	

```
┌─────────────────────────────────────┐
│                                     │
│      Generate HHDuc data block      │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
                                     
│     Add AMS data block (if available)│
                                     
└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│ Add BQR bytes and AMS indication    │
│            byte (J/N)               │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│         Scrambling of data          │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌─────────────────────────────────────┐
│                                     │
│          Generate QR Code           │
│                                     │
└─────────────────────────────────────┘
                  │
                  ▼
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
                                     
│        Incorporate Logo (if any)    │
                                     
└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

Figure 7: Procedure for generating a chipTAN QR code

The QR code generated on the server-side is transferred as a graphic (e.g. with MIME-Type=PNG) to the client and displayed there.

D.2.3 Definition of QR-Code parameters

In addition to the specifications in the previous section, the following parameters have been taken into account in the HHD$_{QR}$ procedure:
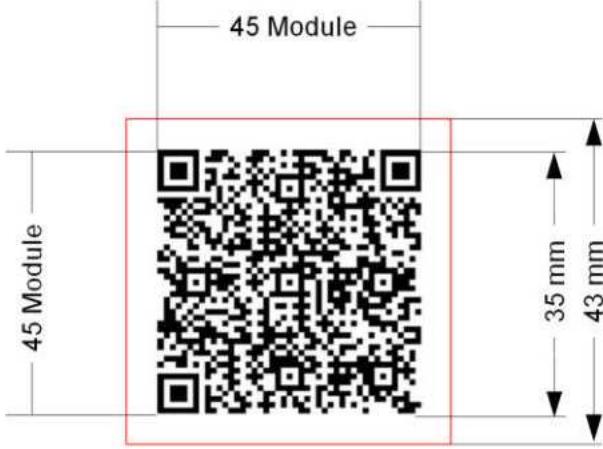
Parameter	to be supported by a QR-Code chipTAN reader (optional functions are shown in italics)
QR Code specification	ISO/IEC 18004:2006
QR Code Model	Model 2
Type	static
Data type	binary data (8-bit byte mode)
ECI-Header	011100000001' 12 bit consisting of 4 bit identifier for ECI mode and 8 bit identifier for character set (1 = ISO-8859-1)
Error correction	ECC Level L *ECC Level M*
QR Code Version	Minimum: Version 4 - 33 x 33 Module Maximum: Version 8 - 49 x 49 Module
Colours	black / white
Quiet Zone	- 4 Module - white
Additional optional functions	*- Support of integrated images / logos* *- Scanning of non-banking QR codes*
MIME-Types[2]	PNG, GIF, JPG
Displayed image size	Minimum: 35 x 35 mm Maximum: not defined
Recording time of a QR code, beginning with the QR code being shown on the screen of the access device and ending when the calculated data is shown on the chipTAN reader display.	max. 300 ms
Camera for display delay in focusing process before QR code is read*.*	max. 200 ms

---

[2] For the use of server-based QR code generation

Parameter	to be supported by a QR-Code chipTAN reader (optional functions are shown in italics)
QR code example for version 7 with ECC level L for transmitting a maximum of 154 bytes of binary data (e.g. HHD V1.4 without AMS)	

D.2.4 Example for generating a chipTAN-QR Code

The following steps show the structure of the individual data structures up to the generation of chipTAN-QR codes as described in section D.2.2.

D.2.4.1 HHDuc data block for QR-Code calculation

In this example, the following HHD_{UC} structure is used for an individual bank transfer containing the data elements "account/IBAN" (the last 10 digits) and "amount":

	Element	Content	Hexadecimal representation
HHDuc-Block	LC		1D
	LS		C8
	Control		01
	Start-Code	„821 12345"	38 32 31 31 32 33 34 35
	L(DE1)		
	DE1	„0123456789"	30 31 32 33 34 35 36 37 38 39
	L(DE2)		
	DE2	„100,00"	31 30 30 2C 30 30
	Checkbyte		02

This leads to the following data stream for the BQR determination:

1D C8 01 3832313132333435 4A 30313233343536373839 46 3130302C3030 02

D.2.4.2 BQR determination

The following data are added for the BQR determination:

	Element	Content	Hexadecimal representation
BQR-1	DK	„DK"	44 4B
	AMS-Flag	„N"	4E
HHDuc-Block			
BQR-2	CRC-16		42 35

This leads to the following result, which is then used for the scrambling:

444B 4E 1D C8 01 3832313132333435 4A 30313233343536373839 46 3130302C3030 02 4235

Note: It should be considered that the data for the formation of the CRC-16 are processed exactly as shown. Many of the routines available online first convert the data stream to ASCII and then calculate CRC-16 from this data, which leads to an incorrect result.

D.2.4.3 Banking QR-Code scrambling

For the banking QR code scrambling, the transferred data structure is manipulated via XOR using the constants "DK" (0x'44 4B'). In this case, it is started at the 3rd byte, so that the constant value "DK" is retained in plain text. The operation results in the following data structure:

444B 0A 56 8C 4A 7C79757A7678707E 0E 7B7579777F717D73737D 0D 757B7467747B 46 0971

D.2.4.4 QR-Code generation

With the resulting data string for a scrambled banking QR code, a suitable QR code can now be generated.

The following QR codes were generated using parameter version = 7 and ECC Level = L.

Part of the generation process is the application of a mask according to section 8.8 of [ISO18004]. There are 8 different masks available. The mask is selected automatically using the procedure described in [ISO18004]. Tests have shown, however, that different masks are used for specific implementations. The resulting QR code can therefore be quite different. There are no issues with the contained data and readability though, since the mask used is part of the QR code. However, the visual comparison reveals differences.

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
D	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Particular specifications for the use of matrix codes
30	5.06.2018	

The following table shows the different QR codes for the example shown above:

Mask	QR-Code
0 (000)	
1 (001)	
2 (010)	
3 (011)	

Mask	QR-Code
4 (100)	
5 (101)	
6 (110)	
7 (111)	

Chapter:	Version:	HandHeld-Device (HHD) for generation of an OTP
D	V 1.5.1	Document: HHD enhancement for optical interfaces
Page:	Status as of:	Chapter: Particular specifications for the use of matrix codes
32	5.06.2018	

D.3   Colour matrix code (HHD_{FM})

Since the beginning of 2017, the color matrix code method, based on CrontoSign Copyright © 2016 VASCO Data Security, together with the SECODER 3G chip-TAN 1.1, has been used in the Cooperative Financial Group. The Deutsche Genossenschafts-Verlag eG has taken over the further development, testing and coordination. Companies wishing to integrate and use the colour matrix code method based on SECODER 3G must consult the Deutsche Genossenschafts-Verlag or VASCO Data Security in order to establish the necessary framework conditions for its implementation.

In the following, the basic characteristics of the colour matrix code method are described.

D.3.1   Colour matrix code format and structure

This chapter describes the basic characteristics of the coloured matrix code.

The colour matrix code consists of a square image in the colours red, green, blue or white. The image is framed by a black frame with a width of two units containing the actual user data. Inside the frame there is a white zone (padding) with a width of one unit. Within this zone the actual coloured data content is visualised with 25 to 25 units. Each individual unit (colour dot) must have a minimum size of 3 pixels. The total image size is about 4 x 4 cm.
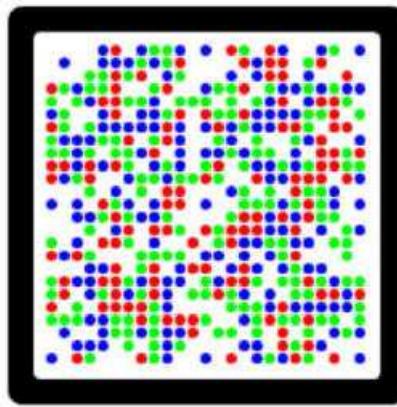

Figure 8: Colour matrix code

D.3.2   Colour matrix code dynamic content

The colour matrix code data content consists of three elements.

Payload	Error cor-rection	Error de-tection

HandHeld-Device (HHD) for generation of an OTP		Version:	Chapter:
Document: HHD enhancement for optical interfaces		V 1.5.1	D
Chapter: Particular specifications for the use of matrix codes		Status as of: 5.06.2018	Page: 33

The elements are defined as follows.

Property	Length	Purpose
Payload	101 bytes	Payload with padding and obfuscation
Error correction	38 bytes	Reed-Solomon error correction.
Error detection	3 bytes	CRC-24

D.3.2.1 Payload

The payload starts with a version byte. If the HHD_{UC} block is <= 100 bytes, a single colour matrix code is generated. In case the HHD_{UC} data block is > 100 bytes, two colour matrix codes are generated. When interpreting the colour matrix code visually, sequential reading and merging of the string must be supported.

Content:

Single colour matrix code (If HHD_{UC} data block <= 100 bytes)

0x05	HHD_{UC} Data Block

Double colour matrix code (If HHD_{UC} data block > 100 bytes)

0x15	0x00	HHDuc Data Block (bytes 0 -99)
0x15	0x21	HHDuc Data Block (bytes 100 -LC)

Padding

A colour matrix code has a fixed number of bits. The bits not used are padded.

Obfuscation

To reduce the visibility of static or repeated data patterns in the colour matrix code, data scrambling is used after padding the content.

D.3.2.2 Error correction

Reed-Solomon codes are used for error correction.

D.3.2.3 Error detection

For error detection, a checksum of the payload is created and added at the end of the byte string.

Further technical details should be clarified with the above-mentioned contact persons.

D.4 Generation of further matrix codes (HHD$_{MC}$)

If none of the methods described above is used to generate the matrix code, the method is referred to as the HHD$_{MC}$ method.

As part of the HHD$_{MC}$ procedure, the customer product must generate the matrix code on the access device. The output data is available as HHD$_{UC}$ data block and in some cases as AMS data block as described in chapter B.

The matrix code generated shall be displayable on any display of an access device, independently of

- the type of screen (CRT monitor, TFT, plasma, ...)
- the size of the screen and
- the selected screen resolution.

In addition, the DK makes no further specifications for the HHD$_{MC}$ method as to how the matrix code is to be generated. It is the responsibility of the manufacturer of the chipTAN reader and the provider of the HHD$_{MC}$ method to ensure that all patent requirements for the use of the selected matrix code are met.