Herstellererklärung:

Einhaltung der DK-Vorgaben für die Realisierung eines Secoder 3 – Typ G

(Version der Vorlage: 2.0 vom 31.01.2022)

Hersteller[1]: _____

Straße: _____

PLZ / Ort: _____

Tel. / Fax: _____

E-Mail: _____

Registrierungsnummer: _____[2]

Hiermit wird verbindlich zugesichert, dass bei der Herstellung eines Secoder 3 – Typ G mit der unter 1 angegebenen Typ-Bezeichnung und Software-Version die unter 2 – 11 aufgeführten Vorgaben eingehalten werden. Unter „Herstellung eines Secoder 3 – Typ G“ wird dabei sowohl die Produktion und Ausgabe eines neuen Kundenterminals mit bereits installierter Secoder-Software[3] verstanden als auch das nachträgliche Laden der Secoder-Software in ein bereits existierendes Kundenterminal.

[1] Herstellername ebenfalls auch in Kopfzeile eintragen.

[2] Die Registrierungsnummer muss beim Zulassungsbüro der DK beantragt werden.

[3] Mit Secoder-Software wird dabei eine Software für ein Kundenterminal bezeichnet, die durch das Zulassungsverfahren der deutschen Kreditwirtschaft als solche zugelassen wurde.

1 Typ-Bezeichnung und Software-Version des Secoder 3 – Typ G

Typ-Bezeichnung: _____[4]

Software-Version: _____[5]

Nur falls der Secoder 3 – Typ G die Secoderanwendung chipTAN ("ctn") unterstützt:

Lesertyp: _____[6]

2 Umsetzung der Schnittstellenspezifikation

Folgende Versionen/Stände der Spezifikationen und Errata wurden bei der Realisierung des Geräts berücksichtigt:

Umgesetzt[7]	**Optional[8]**	**Spezifikation**	**Version/Stand der Spezifikation[9]**	**Stand der Errata[9]**
X	Nein	Specifications of the Secoder 3G, Platform Requirements		
X	Nein	Specifications of the Secoder 3G, Base Functionality		
	Ja	Specifications of the Secoder 3G, Secoder Application chipTAN		

[4] Die Angaben zum Typ müssen mit den Feldern “Vendor ID“ und “Product ID“ übereinstimmen, die der Secoder als Antwort auf das Kommando SECODER INFO liefert.

[5] Die Angabe zur Version der Software muss mit dem Feldes “implementation version“ übereinstimmen, das der Secoder als Antwort auf das Kommando SECODER INFO liefert.

[6] Angabe des Lesertyps, der u.a. bei Start-Code 09 auf dem Display angezeigt wird.

[7] Spezifikationen der enthaltenen Secoderanwendungen bitte ankreuzen.

[8] Angeben, ob diese Secoderanwendung in allen Geräten vorhanden sein muss (Optional = Nein), oder ob sie in Geräten fehlen kann (Optional = Ja).

[9] Für Spezifikationen bitte Version und Datum der berücksichtigten Dokumente angeben, für Errata deren Stand.

Umgesetzt[7]	Optional[8]	Spezifikation	Version/Stand der Spezifikation[9]	Stand der Errata[9]
	Ja	Specifications of the Secoder 3G, Secoder Application Digital Signature based on the AUT Key		
	Ja	Specifications of the Secoder 3G, Secoder Application EMV SIG		

Wir bestätigen, dass die für die Realisierung eines Secoder 3 – Typ G relevanten Teile der Spezifikationen und Errata vollständig und korrekt implementiert wurden.

Die folgenden Punkte sind uns bekannt:

a. Die aktuellen Errata sind verpflichtender Bestandteil der Schnittstellenspezifikation.

b. Es liegt in der Verantwortung des Herstellers, dass ihm die aktuellen Versionen für Schnittstellenspezifikation und Errata zur Verfügung stehen.

c. Bei Unklarheiten in der Schnittstellenspezifikation müssen diese mit der Deutschen Kreditwirtschaft geklärt werden.

d. Bei aufgedeckten Fehlern in der Schnittstellenspezifikation müssen diese der Deutschen Kreditwirtschaft mitgeteilt werden.

3 Verwaltung der Software-Versionen

Bei verschiedenen Versionen der Software eines Secoder 3 werden die folgenden Vorgaben erfüllt:

a. Verschiedene Versionen der Firmware/Software eines Secoder 3 führen zu unterschiedlichen Belegungen für den Wert von "implementation version", der im Rahmen der Antwortdaten zu dem Secoder-Kommando SECODER INFO zurückgegeben wird.

b. Nach einem Update einer Firmware/Software in einem Secoder 3 liefern folgende Aufrufe des Kommandos SECODER INFO in den Antwortdaten für "implementation version" den Wert für die neue Firmware/Software.

c. Nach einem Update einer Firmware/Software in einem Secoder 3 ist gewährleistet, dass eine im Display (im Rahmen der Startup- bzw. Idle-Message) angezeigte Secoder-Spezifikations- (Interface Version) und Firmware-Version (Implementation Version) stets authentisch ist, d.h. dem Stand der in dem Kundenterminal geladenen Firmware/Software entspricht.

Nur falls der Secoder 3 – Typ G die Secoderanwendung chipTAN ("ctn") unterstützt:

d. Verschiedene Versionen der Firmware/Software eines Secoder 3 führen zu unterschiedlichen Belegungen für den Wert von "Lesertyp", der u.a. bei einem Start-Code 09 auf dem Display des Lesers angezeigt wird.

e. Nach einem Update einer Firmware/Software in einem Secoder 3 liefert ein folgender Start-Code 09 die zu der neuen Firmware/Software gehörende Belegung für den Wert von "Lesertyp".

4 Allgemeine Anforderung an die Verteilung von Kundenterminals bzw. Firmware

a. Wir sichern zu, dass wir keine Kundenterminals bzw. Firmware-Versionen in den Umlauf bringen, die nicht von der Deutschen Kreditwirtschaft zugelassen sind, sich aber dennoch am Display des Kundenterminals (im Rahmen der Startup- bzw. Idle-Message) als Secoder ausweisen.

b. Es ist gewährleistet, dass eine im Display (im Rahmen der Startup- bzw. Idle-Message) angezeigte Secoder-Spezifikations- (Interface Version) und Firmware-Version (Implementation Version) stets authentisch ist, d.h. dem Stand der in dem Kundenterminal enthaltenen Firmware entspricht.

c. Alle in Umlauf gebrachten Kundenterminals, die für eine Nutzung als Secoder geeignet sind, sind mit einer Versiegelung versehen, anhand derer ein Benutzer einen etwaigen Manipulationsversuch erkennen kann.

d. Im Internet (unter der URL _____[10]) werden Darstellungen unbeschädigter Siegel zur Verfügung gestellt. Die Deutsche Kreditwirtschaft kann auf die Darstellungen des Herstellers im Internet verlinken.

5 Schnittstellen für die Dateneingabe bzw. Datenübergabe

Das Kundenterminal Secoder 3 – Typ G, auf das sich diese Herstellererklärung bezieht, unterstützt die folgenden Schnittstellen für die Dateneingabe bzw. Datenübergabe[11]:

- □ Bluetooth
- □ Optische unidirektionale Kopplung
- □ Manuelle Dateneingabe

[10] Bitte URL der Internetseite einfügen.

[11] Bitte verfügbare Schnittstellen ankreuzen.

Wir bestätigen:

a. Falls das Kundenterminal eine bidirektionale Verbindung basierend auf Bluetooth unterstützt, wird bestätigt, dass die Anforderungen des „Bluetooth Qualification Program“ erfüllt wurden und dass das Kundenterminal das Bluetooth-Logo tragen darf. Ein entsprechender Nachweis über das "End Product Listing" des Geräts bei der Bluetooth Special Interest Group liegt uns vor.

b. Falls das Kundenterminal eine bidirektionale Verbindung basierend auf Bluetooth unterstützt, wird bestätigt, dass die Realisierung dieser Schnittstelle die folgenden Vorgaben erfüllt.

Spezifikation	**Version/Stand der Spezifikation[9]**	**Stand der Errata[9]**
Bluetooth Low Energy – GATT Service and Profile for chipTAN-Reader		

c. Das Kundenterminal unterstützt eine bidirektionale Verbindung basierend auf USB, die – unter Berücksichtigung der spezifischen Anforderungen der oben genannten Spezifikationen – USB 2.0- (oder höher) und CCID-spezifikationskonform ausgeführt ist.

d. Falls das Kundenterminal eine optische unidirektionale Kopplung unterstützt, wird bestätigt, dass die Realisierung dieser Schnittstelle die folgenden Vorgaben erfüllt.

Spezifikation	**Version/Stand der Spezifikation[9]**	**Stand der Errata[9]**
HHD-Erweiterung für unidirektionale Kopplung		

e. Falls das Kundenterminal eine optische unidirektionale Kopplung unterstützt und die Tastatur des Kundenterminals über Tasten zur Eingabe von Ziffern verfügt, wird bestätigt, dass das Kundenterminal auch die manuelle Dateneingabe unterstützt.

6 Schnittstellen für die Kommunikation mit der Chipkarte

Es wird bestätigt, dass das Gerät die elektromechanische Verträglichkeit der kontaktbehafteten Schnittstelle zur Chipkarte erfüllt.

7 Filterregeln

Der Unterzeichner bestätigt, dass alle relevanten Filterregeln aus den in Abschnitt 2 genannten Spezifikationen vollständig und korrekt implementiert wurden.

Bei dem Kundenterminal, auf das sich diese Herstellererklärung bezieht,

□ ist die Defaultanwendung vollständig blockiert[12].

□ ist die Defaultanwendung aktiviert.

Für den ersten Fall gilt:

> Für das Kundenterminal ist die Defaultanwendung deaktiviert. Chipkartenkommandos können daher weder direkt noch indirekt durch das Zugangsgerät über das Kundenterminal an die Chipkarte gegeben werden.

Für den zweiten Fall gilt:

> Für das Kundenterminal ist die Defaultanwendung aktiviert. Chipkartenkommandos können daher direkt oder indirekt durch das Zugangsgerät über das Kundenterminal an die Chipkarte gegeben werden. Es gilt aber, dass kein Chipkartenkommando direkt oder indirekt durch das Zugangsgerät über das Kundenterminal an die Chipkarte gegeben werden kann, sofern dies einer der relevanten Filterregeln widerspricht.

8 Laden einer Secoder-Software in ein bereits existierendes Kundenterminal

Eine Secoder-Software wird nur dann in ein bereits existierendes Kundenterminal ohne Secoder-Software geladen, falls das Kundenterminal die folgenden Anforderungen erfüllt:

a. Der Mechanismus für eine Änderung der Firmware/Software des Kundenterminals erfüllt alle in Abschnitt 9 beschriebenen Anforderungen. Dies gilt für alle Firmware/Software-Versionen, die seit Ausgabe des Kundenterminals in dem Kundenterminal vorhanden waren.

b. Das Kundenterminal erfüllt zusammen mit der geladenen Secoder-Software alle relevanten Anforderungen aus dieser Herstellererklärung.

c. Es ist gewährleistet, dass eine im Display (im Rahmen der Startup- bzw. Idle-Message) angezeigte Secoder-Spezifikations- (Interface Version) und Firmware-Version (Implementation Version) stets authentisch ist, d.h. dem aktuellen Stand der geladenen Firmware entspricht.

9 Autorisierte Updates der Firmware/Software

Bei jeder Durchführung eines Updates der Firmware/Software werden (mindestens) die folgenden Anforderungen erfüllt:

[12] Diese Option ist nur möglich, falls die Secoderanwendung "aut" (Signatur basierte Authentifizierung mittels AUT-Schlüssel) durch den Secoder 3 – Typ G **nicht** unterstützt wird.

a. Der zur Absicherung des Updates genutzte Herstellerschlüssel wird durch uns maximal bis Ende _____[13] eingesetzt (intendierte Gültigkeit).

b. Die unter a genannte intendierte Gültigkeit des Herstellerschlüssels wird dem Sicherheitsgutachter mitgeteilt und durch den Gutachter in seinem Gutachten bewertet. Wir werden die Gültigkeit des Herstellerschlüssels entsprechend verkürzen, falls dies durch den Gutachter in seinem Gutachten gefordert wird.

c. Nach Ablauf der Gültigkeit eines Herstellerschlüssels werden durch uns keine Updates mehr mit diesem Herstellerschlüssel abgesichert.

d. Die Authentizität und Vertraulichkeit des privaten Herstellerschlüssels und die Authentizität des öffentlichen Herstellerschlüssels wird durch uns sichergestellt und garantiert. Eine nicht von uns autorisierte Verwendung des privaten Herstellerschlüssels zur Signierung der Firmware/Software ist nicht möglich.

e. Eine von uns nicht autorisierte Veränderung des zugehörigen öffentlichen Schlüssels ist über keine der Schnittstellen des Kundenterminals möglich.

f. Die Sicherheit des Mechanismus zum Update der Firmware/Software basiert nicht auf einem Geheimnis, das innerhalb des Kundenterminals gespeichert ist.

g. Das Kundenterminal akzeptiert bei einem Update von Firmware/Software keine alten Versionen der Firmware bzw. Software.

h. Bei einem Update darf eine Drittanwendung nur eingebracht werden, falls hierfür eine Zustimmung der DK vorliegt. Für eine Drittanwendung darf nur solche Software eingebracht werden, durch die alle Sicherheitseigenschaften aus Abschnitt 2.8 des Dokuments "Sicherheitseigenschaften des Kundenterminals Secoder 3" (in der aktuell verabschiedeten Version) erfüllt werden.

i. Bei einem Update darf für eine Secoderanwendung nur Software eingebracht werden, für die die notwendige Zulassung der DK vorliegt.

j. Bei einem Update darf die Software für eine Secoderanwendung nur in ein Gerät geladen werden, für das die notwendige Zulassung der DK vorliegt.

k. Kann ein begonnener Firmware/Software-Update nicht erfolgreich beendet werden, ist danach die bisherige Firmware/Software des Geräts wie vor dem Start des Updates wieder unverändert aktiv.

Die relevanten Mechanismen (z.B. Rollenkonzept, Keymanagement-Policy) wurden durch uns in einem Sicherheitskonzept vollständig beschrieben. Dieses Sicherheitskonzept wurde dem Sicherheitsgutachter vorgelegt. Es wird bestätigt, dass die in dem Sicherheitskonzept beschriebenen Sicherheitsmechanismen umgesetzt sind.

[13] Das Jahr eintragen, bis zu dessen Ende der Herstellerschlüssel maximal genutzt werden soll.

10 Drittanwendungen

In dem Kundenterminal, auf das sich diese Herstellererklärung bezieht,

- □ sind Drittanwendungen[14] enthalten, bzw. können Drittanwendungen zukünftig nachgeladen werden.
- □ sind keine Drittanwendungen enthalten und werden zukünftig auch keine Drittanwendungen nachgeladen.

Für den ersten Fall wird explizit bestätigt:

> Für die einzubringenden Drittanwendungen liegen die notwendigen Zustimmung der DK vor.
>
> Durch die enthaltenen bzw. später nachzuladenden Drittanwendungen wird die Sicherheit der in dem Kundenterminal enthaltenen Secoderanwendungen nicht negativ beeinflusst. Die enthaltenen Drittanwendungen erfüllen die Sicherheitseigenschaften aus Abschnitt 2.8 des Dokuments "Sicherheitseigenschaften des Kundenterminals Secoder 3" (in der aktuell verabschiedeten Version).

11 Weitere Sicherheitseigenschaften

Der Unterzeichner bestätigt, dass die folgenden weiteren Sicherheitseigenschaften durch das Gerät eingehalten werden:

a. Ein Tastendruck auf die Tastatur des Secoders hat keinerlei Rückmeldung des Secoders an den PC zur Folge. Daten, die durch den Kunden am Secoder eingegeben werden, werden nicht an den PC übergeben.

b. Ein transparenter Zugriff auf das Display des Secoders vom PC aus ist nicht möglich. Das Display des Secoders wird nur mit den definierten, leserintern implementierten Funktionen angesprochen.

c. Speicherbereiche, die Daten beinhalten, die über die Tastatur des Secoders eingegeben wurden, werden aktiv durch Überschreiben mit Default-Werten gelöscht, nachdem die Verarbeitung dieser Daten abgeschlossen wurde.

d. Der Speicherbereich, in dem ein PIN-Wert abgelegt wurde, wird aktiv durch Überschreiben mit Default-Werten gelöscht, nachdem der PIN-Wert durch die Anwendung nicht mehr benötigt wird.

[14] Als Drittanwendung wird eine Leseranwendung in dem Kundenterminal bezeichnet, die nicht durch die DK spezifiziert wurde.

e. Nach einem Reset ist im Secoder die Defaultanwendung aktiv. Sofern vor dem Reset eine andere als die Defaultanwendung aktiv war, wird diese abgebrochen. Dem Kunden wird der Abbruch einer Transaktion angezeigt und er muss von ihm bestätigt werden.

f. Falls der Secoder die Secoderanwendung ctn enthält und diese in dem Secoder aktiv ist, werden alle durch das Zugangsgerät übergebenen Kartenkommandos und PIN-Kommandos durch den Secoder blockiert.

g. Die Firmware/Software des Kundenterminals kann mit der Ausnahme von autorisierten Updates gemäß den Vorgaben aus Abschnitt 9 über keine der Schnittstellen des Kundenterminals geändert werden. Dies gilt sowohl für externe Schnittstellen (z.B. USB, Bluetooth) als auch für interne Programmierschnittstellen. Eine Beschreibung und plausible Darstellung der zur Sicherstellung dieser Anforderungen umgesetzten Mechanismen ist in dem Sicherheitskonzept gemäß Abschnitt 9 enthalten.

Die Deutsche Kreditwirtschaft behält sich vor, die Einhaltung dieser Erklärung zu prüfen. Falls durch die DK gefordert müssen die in dieser Erklärung genannten Nachweise vorgelegt werden.

Diese Erklärung tritt zum Unterzeichnungsdatum in Kraft.

Ort	Datum[15]	Unterschrift
_____	_____	_____

Die Bereitstellung dieser vollständig ausgefüllten und unterschriebenen Herstellererklärung ist Vorbedingung für die Teilnahme am DK-Zulassungsverfahren. Die unterschriebene Herstellererklärung ist an folgende Adressen zu senden:

DK-Zulassungsbüro
c/o Bundesverband Öffentlicher Banken Deutschlands e.V.
Postfach 11 02 72
10832 Berlin

Die Angaben unterliegen dem Datenschutz und werden nicht einzeln weitergegeben oder veröffentlicht.

Nach Abschluss der Zulassung stellt das Zulassungsbüro im positiven Fall ein Zertifikat über die Zulassung des Secoder 3 – Typ G aus. Nach Ausstellung des Zertifikats darf der Hersteller für das Gerät gemäß Abschnitt 1 folgendes Secoder-Siegel der Deutschen Kreditwirtschaft verwenden:

[15] Datum der Erklärung auch in Fußzeile eintragen.


empfohlen von den
Secoder
zertifiziert
Banken und Sparkassen