DPG Deutsche Pfandsystem GmbH

Anlage 7 Anhang 2

Sicherheitstechnische Anforderungen an die IT in DPG-Rücknahmevorrichtungen

Stand: 14. Juni 2016

(Inkrafttreten: 01. Oktober 2016)

zu den Teilnahmebedingungen

Versionsübersicht

Version	Datum	Bearbeiter	Änderungen
0.5	03.03.2006	TÜViT	Vorabversion Instanz Krypto
1.0	07.03.2006	TÜViT	Vervollständigung aller Instanzen und Übergabe an die DPG zur Abnahme (über Roland Berger)
1.1	05.06.2007	DPG	Überarbeitung (1 Jahr Erfahrung)
1.2	18.09.2009	DPG	Überarbeitung
1.3	30.05.2011	DPG	Überarbeitung der Tabellen unter 2.6.1, 2.6.2 und 2.6.3.1
1.4	02.09.2011	DPG	Redaktionelle Anpassungen
1.5	10.09.2013	DPG	Redaktionelle Anpassungen
1.6	14.06.2016	DPG	Redaktionelle Überarbeitung (GTIN-Strichcode durch EAN-Barcode ersetzt)

Inhaltsverzeichnis

1. Einleitung 5

1.1 Ziel dieses Dokumentes 5
1.2 Prozesse innerhalb der DPG-Rücknahmevorrichtungen 5

2. Anforderungen an die Automateninstanzen 9

2.1 Instanz Prüfung (A1a, Z1a) 9
2.1.1 Übersicht aus der Risikobewertung 9
2.1.2 Detaillierung der Schutzanforderungen 9
2.2 Instanz Steuerung (A2a) 9
2.3 Instanz Steuerung (A4a, Z4a) 10
2.3.1 Übersicht aus der Risikobewertung 10
2.3.2 Detaillierung der Schutzanforderungen 10
2.4 Prüfinstanz (A5a) 10
2.4.1 Übersicht aus der Risikobewertung 11
2.4.2 Detaillierung der Schutzanforderungen 11
2.5 Instanz Generator (A6a, Z6a) 11
2.5.1 Übersicht aus der Risikobewertung 12
2.5.2 Detaillierung der Schutzanforderungen 12
2.6 Instanz Krypto (A7a, Z7a) 13
2.6.1 Übersicht aus der Risikobewertung 13
2.6.2 Generische Sicherheitsanforderungen an die Instanz Krypto 14
2.6.3 Detaillierung der Sicherheitsanforderungen 14
2.7 Instanz Kommunikation (A8a, Z8a) 18
2.7.1 Übersicht aus der Risikobewertung 18
2.7.2 Detaillierung der Schutzanforderungen 18

3. Anforderungen an die Kommunikation zwischen den Instanzen 19

3.1 Sensor – Prüfung (A1, Z1) 19
3.1.1 Übersicht aus der Risikobewertung 19
3.1.2 Detaillierung der Schutzanforderungen 19
3.2 Prüfung – Steuerung (A2) 19
3.3 Prüfung – Generator (Z2) 19
3.4 Kompaktor – Steuerung (A4) 20
3.4.1 Übersicht aus der Risikobewertung 20
3.4.2 Detaillierung der Schutzanforderungen 20
3.5 Steuerung – Prüfung (A5) 20
3.6 Prüfung – Generator (A6, Z6) 20
3.6.1 Übersicht aus der Risikobewertung 20
3.6.2 Detaillierung der Schutzanforderungen 21
3.7 Generator – Krypto (A7, Z7) 21
3.7.1 Übersicht aus der Risikobewertung 21

3.7.2 Detaillierung der Schutzanforderungen 21
3.8 Krypto – Kommunikation (A8, Z8) 22
3.8.1 Übersicht aus der Risikobewertung 22
3.8.2 Detaillierung der Schutzanforderungen 22
3.9 Generator – Kommunikation (Z7b) 22
3.9.1 Übersicht aus der Risikobewertung 23
3.9.2 Detaillierung der Schutzanforderungen 23

4. Weitere Anforderungen 23

5. Anhänge 24

5.1 Glossar 24
5.2 Verpflichtung aufgrund von Vorgaben in anderen Dokumenten mit Bezug zu sicherheitstechnischen Anforderungen an die IT in DPG-Rücknahmevorrichtungen 24
5.3 Übersicht Erzeugung signierter Rohdatensatz 25

1. Einleitung

1.1 Ziel dieses Dokumentes

Das Ergebnis einer Risikoanalyse auf Basis der ISO/IEC CD 13335-2 für die IT der DPG-Rücknahmevorrichtungen im Januar/Februar 2006 mit dem Fokus auf Vertraulichkeit, Verfügbarkeit und Integrität der IT der DPG-Rücknahmevorrichtungen ist die Notwendigkeit, den Herstellern von DPG-Rücknahmevorrichtungen eine Liste mit den erforderlichen sicherheitstechnischen Anforderungen an die IT der DPG-Rücknahmevorrichtungen zur Verfügung zu stellen. DPG-Rücknahmevorrichtungen sind DPG-Automaten, Großzählautomaten und Zähltische.

Dieses Dokument enthält eine Liste mit sicherheitstechnischen Anforderungen an die IT in DPG-Rücknahmevorrichtungen ("**Anforderungen**"). Dies sind Anforderungen an die Instanzen Prüfung, Steuerung, Generator, Krypto und Kommunikation und deren Kommunikationsverbindungen untereinander. Eine wesentliche Voraussetzung ist, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen. Die Mechanik der Rücknahmevorrichtungen ist nicht Bestandteil der in diesem Dokument enthaltenen Anforderungsliste.

Hersteller von DPG-Rückahmevorrichtungen / Zählzentrumbetreiber müssen diese Anforderungsliste durch geeignete Maßnahmen umsetzen. Die geeignete Umsetzung der Maßnahmen ist durch qualifizierte IT-Auditoren zu verifizieren.

Die in diesem Dokument aufgeführten Anforderungen enthalten keine Vorschläge für konkrete Umsetzungsmaßnahmen, sondern prozessspezifische Vorgaben, die durch technische, personelle, bauliche und/oder organisatorische Maßnahmen erfüllt werden können. Dadurch haben die Hersteller von DPG-Rücknahmevorrichtungen zum einen die gebotene Flexibilität bei der Umsetzung der Anforderungen, zum anderen ist es den Herstellern von DPG-Rücknahmevorrichtungen dadurch möglich, die in ihre Unternehmenskultur passenden Maßnahmen auszuwählen.

Teile der sicherheitstechnischen Anforderungen bei Zählzentren können im Rahmen eines Grundzertifikats nachgewiesen werden. Innerhalb dieser sogenannten Grundzertifizierung wird ein qualifizierter IT-Auditor Teile des Prüfschema beim Hersteller DPG-Rücknahmevorrichtungen verifizieren. Bei Erteilung einer Grundzertifizierung kann dieser das Zertifikat seinen Kunden vorlegen. Der qualifizierte IT-Auditor vor Ort muss dadurch nur die noch nicht geprüften Aspekte verifizieren und kann die Grundzertifizierung im Rahmen seiner Prüfung heranziehen.

1.2 Prozesse innerhalb der DPG-Rücknahmevorrichtungen

Ein Großteil der Sicherheit vor Betrug im DPG-System wird durch die Funktionen der DPG-Rücknahmevorrichtungen gewährleistet. Im Zuge der Risikoanalyse wurden die IT-Abläufe innerhalb einer DPG-Rücknahmevorrichtung in logische Prozessschritte unterteilt.

Abbildung 1 stellt die Prozessschritte innerhalb eines DPG-Automaten grafisch dar.

Abbildung 2 stellt die Prozessschritte innerhalb eines Zählzentrums grafisch dar:

A0a Z0a	Eine DPG-Verpackung wird in die DPG-Rücknahmevorrichtung eingeworfen. Dabei werden der EAN-Barcode und die DPG-Markierung ausgelesen.
A1 Z1	Der gelesene EAN-Barcode und die DPG-Markierung werden vom Sensor an die Prüfinstanz (kann Automatensteuerung oder auch Kamera sein) übergeben.
A1a Z1a	In der Prüfinstanz wird der gelesene EAN-Barcode mit den hinterlegten Artikelstammdaten abgeglichen und die DPG-Markierung geprüft.
A2	Ein Prüfsignal (ok; nicht ok) wird von der Prüfinstanz an die Steuerung übergeben.
Z2	Ein Prüfsignal (ok; nicht ok) wird von der Prüfinstanz an den Generator übergeben.
A2a	Das Prüfsignal wird von der Steuerung entgegengenommen.
Z2a	Das Prüfsignal wird vom Generator entgegen genommen.
A3	Falls das Prüfsignal ‚ok' erfolgt, wird ein ok-Signal an den Kompaktor geleitet.
A3a	Falls das Prüfsignal ‚nicht ok' erfolgt, wird ein nicht-ok-Signal an den Auswerfer geleitet.
A4	Der Kompaktor leitet ein Signal vom Kompaktor an die Steuerung.
A4a Z4a	Falls das Kompaktor-Signal negativ ist, wechselt die DPG-Rücknahmevorrichtung in den Störmodus. Falls das Kompaktor-Signal positiv ist, wird ein ok-Kompaktorsignal von der Steuerung an die Prüfinstanz übergeben.
A5	Es wird ein ok-Kompaktorsignal von der Steuerung an Prüfinstanz übergeben.
A5a	Bei positivem ok-Kompaktorsignal wird die GTIN von der Prüfinstanz an den Generator geleitet.
A6 Z6	Die GTIN wird von der Prüfinstanz an den Generator übertragen.
A6a Z6a	Im Generator werden mit den Automatenstammdaten die Prozessdaten aufbereitet. Es wird der Zeitstempel hinzugefügt.
A7	Die Prozessdaten werden vom Generator an die Kryptoinstanz übergeben.
Z7	Falls das Prüfsignal ‚ok' erfolgt werden die Prozessdaten vom Generator an die Kryptoinstanz übergeben.
Z7b	Falls das Prüfsignal ‚nicht ok' erfolgt werden die Prozessdaten vom Generator an die Kommunikation übergeben.
A7a Z7a	In der Kryptoinstanz werden die Prozessdaten durch die Signatur zu Rohdatensätzen (mit signiertem und unsigniertem Teil).
A8 Z8	Der Rohdatensatz (mit signiertem und unsigniertem Teil) wird von der Kryptoinstanz an die Kommunikation übergeben.
A8a Z8a	In der Kommunikation wird der Header-Datensatz generiert.
A9 Z10	Der Rohdatensatz (mit signiertem und unsigniertem Teil) und der Header-Datensatz werden an Forderungssteller übertragen.
A10	Ein NoRead-Datensatz kann separat an den Forderungssteller übertragen werden.

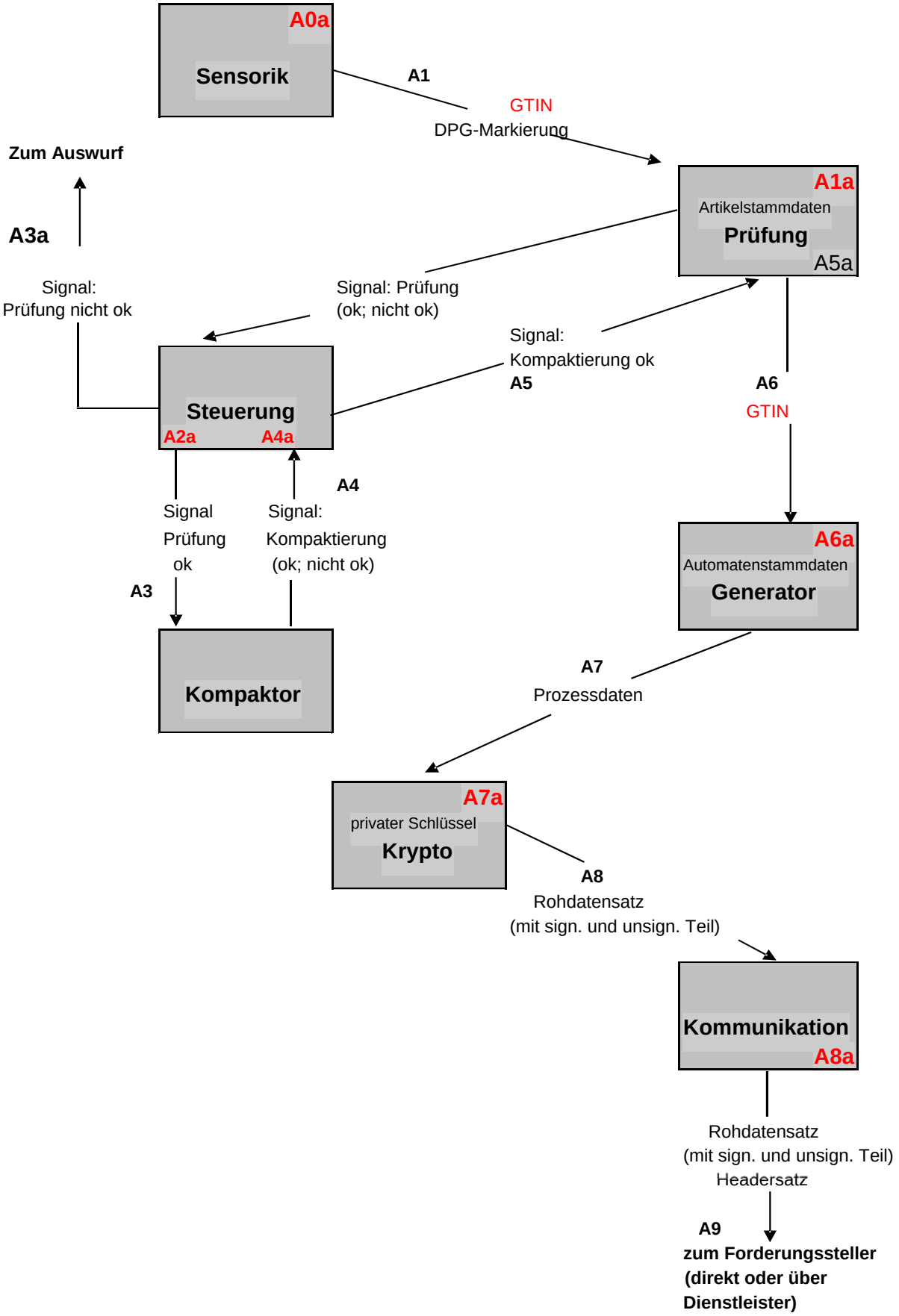

Abbildung 1: Prozesse innerhalb eines DPG-Automaten

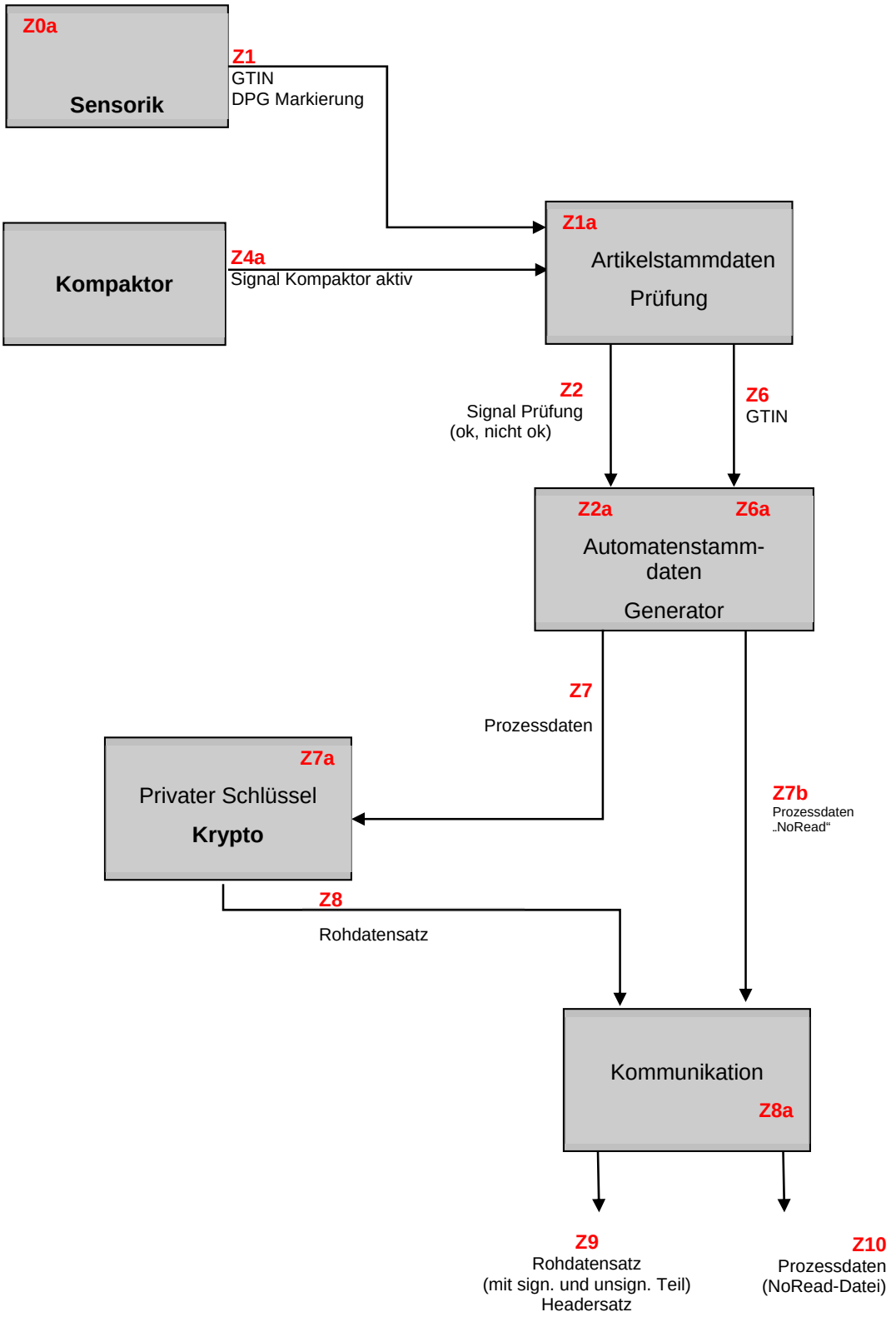

Abbildung 2: Prozesse innerhalb eines Zählzentrums

2. Anforderungen an die Automateninstanzen

2.1 Instanz Prüfung (A1a, Z1a)

In der Prüfinstanz werden der gelesene EAN-Barcode und die DPG-Markierung gegen die hinterlegten Artikelstammdaten geprüft.

2.1.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	**Schwachstelle**	**Risiko**
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
in Prüfinstanz: Prüfung gelesener EAN-Barcode und DPG-Markierung gegen hinterlegten Artikelstammdaten	A1a Z1a	GTIN, DPG-Markierung, Artikelstammdaten	Artikelstammdaten: Änderung in der Form, dass für alle Artikel DPG-Markierung nicht sein muss	Manipulation der hinterlegten Artikelstammdaten durch schreibenden Zugriff	**4**
		GTIN, DPG-Markierung, Artikelstammdaten	Prüfung gegen Artikelstammdaten findet nicht statt (es werden keine Artikelstammdaten zur Generierung der Prozessdaten benötigt)	Zugriff auf Prüfinstanz, z.B. Hersteller	**4**

2.1.2 Detaillierung der Schutzanforderungen

- In der Prüfinstanz muss die Integrität der Artikelstammdaten sichergestellt sein. Es darf kein unbefugter Zugriff auf die Artikelstammdaten möglich sein.
- Ein unbefugter Zugriff auf die Programme der Prüfinstanz muss verhindert werden. Dies gilt während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und ihren Betrieb. Die Programme dürfen keine unerwünschten Funktionen ausführen können, d.h. sie dürfen nur die spezifizierten und durch die DPG freigegebenen Funktionen ausführen können. Dieses ist durch geeignete Mittel zu verifizieren.
- Die Programme der Prüfinstanz müssen sich gegen Manipulation schützen. Veränderungen an den Programmen müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen (z.B. Störmeldung, Unterbrechung der Funktion). Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.

2.2 Instanz Steuerung (A2a)

Es wurden keine Risiken ermittelt.

2.3 Instanz Steuerung (A4a, Z4a)

Falls das Kompaktor-Signal negativ ist, wechselt die DPG-Rücknahmevorrichtung in den Störmodus. Falls das Kompaktor-Signal positiv ist, wird ein ok-Kompaktorsignal von der Steuerung an Prüfinstanz übergeben.

2.3.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	**Schwachstelle**	**Risiko**
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
in Steuerung: falls negativ: Störungsmodus	A4a Z4a	Signal	Manipulation des Signals in ein positives Signal	Manipulation durch schreibenden Zugriff auf Kommunikationsweg Kompaktierer-Steuerung	**5**

2.3.2 Detaillierung der Schutzanforderungen

- Das Signal des Kompaktors muss in der Steuerung gegen Integritätsveränderung geschützt werden.
- Die Programme zur Verarbeitung des Signals vom Kompaktor müssen derart arbeiten, dass der Automat bei einem negativen Signal in den Störmodus wechselt.
- Ein unbefugter Zugriff auf die Programme der Steuerung muss verhindert werden. Dies gilt während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtungen und des Betriebs der DPG-Rücknahmevorrichtungen. Die Programme dürfen keine unerwünschten Funktionen ausführen können, d.h. sie dürfen nur die spezifizierten und durch die DPG freigegebenen Funktionen ausführen können. Dieses ist durch geeignete Mittel zu verifizieren.
- Die Programme der Steuerung müssen sich gegen Manipulation schützen. Veränderungen an den Programmen müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen. Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.

2.4 Prüfinstanz (A5a)

Bei einem positivem Kompaktorsignal ‚ok' wird die GTIN von der Prüfinstanz an den Generator geleitet.

2.4.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
in Prüfinstanz	A5a	GTIN	Manipulation der Prüfinstanz in der Form, dass willkürlich GTIN erzeugt werden	Zugriff auf Prüfinstanz-Programm; Austausch des Prüfinstanz-Programms (z.B. durch organisierte Kriminalität)	**7**

2.4.2 Detaillierung der Schutzanforderungen

- Die GTIN darf nur bei positivem Signal des Kompaktors (= erfolgreiche Kompaktierung der DPG-Verpackung) an den Generator übergeben werden.
- Die Daten in der Prüfinstanz (GTIN, DPG-Markierung, Artikelstammdaten) müssen gegen unberechtigte Veränderung und unberechtigten Zugriff geschützt sein.
- Ein unbefugter Zugriff auf die Programme der Prüfinstanz muss verhindert werden. Dies gilt während der Entwicklung, der Einspielung in den DPG-Automaten und des Betriebs des DPG-Automaten. Die Programme dürfen keine unerwünschten Funktionen ausführen können, d.h. sie dürfen nur die spezifizierten und durch die DPG freigegebenen Funktionen ausführen können. Dieses ist durch geeignete Mittel zu verifizieren.
- Die Programme der Prüfinstanz müssen sich gegen Manipulation schützen. Veränderungen an den Programmen müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen (z.B. Einstellung des Betriebs). Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Es darf nicht möglich sein, willkürlich gültige GTIN von der Prüfinstanz an den Generator zu versenden.

2.5 Instanz Generator (A6a, Z6a)

Im Generator werden mit den Automatenstammdaten die Prozessdaten aufbereitet. Es wird der Zeitstempel hinzugefügt.

2.5.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
in Generator: Aufbereitung zu Prozessdaten	A6a Z6a	Prozessdaten, Automatenstammdaten	willkürliche Erzeugung von Prozessdaten (s. A6)	Zugriff auf Generator-Programm; Austausch des Generator-Programms (z.B. durch organisierte Kriminalität	**7**
in Generator: Erzeugen NoRead für Daten mit Signal ‚nicht ok`	Z6a	Prozessdaten, Automatenstammdaten	willkürliche Erzeugung von Prozessdaten (s. Z6)	Zugriff auf Generator-Programm; Austausch des Generator-Programms	**7**

2.5.2 Detaillierung der Schutzanforderungen

- Die Daten des Generators (Automatenstammdaten, Prozessdaten) müssen gegen unberechtigte Veränderung und unberechtigten Zugriff geschützt sein.
- Ein unbefugter Zugriff auf die Programme des Generators muss verhindert werden. Dies gilt während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und ihres Betriebs. Die Programme dürfen keine unerwünschten Funktionen ausführen können, d.h. sie dürfen nur die spezifizierten und durch die DPG freigegebenen Funktionen ausführen können. Dieses ist durch geeignete Mittel zu verifizieren.
- Die Programme des Generators müssen sich gegen Manipulation schützen. Veränderungen an den Programmen müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen, z.B. Einstellung des Betriebs, müssen erfolgen. Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Es darf nicht möglich sein, willkürlich gültige Prozessdaten oder Daten bei Prüfsignal ‚nicht ok' vom Generator an die Kryptoinstanz zu versenden.
- Die Erzeugung des Zeitstempels und der Zeitstempel selbst darf nicht manipulierbar sein.
- Das unautorisierte Einspielen von GTIN in den Generator muss erkannt und verhindert werden. Entsprechende Reaktionen müssen auch für mehrfach eingespielte GTIN erfolgen.

2.6 Instanz Krypto (A7a, Z7a)

2.6.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Vertraulichkeit**	**Beschreibung**	**Risikowert (0-8)**
in Krypto: Signierung der Prozessdaten zu Rohdatensatz (sign./ unsign. Teil)	A7a Z7a	Prozessdaten, Rohdatensatz (sign./unsign. Teil), privater Schlüssel	Auslesen des privaten Schlüssels	unzureichender Zugriffsschutz des privaten Schlüssels	**7**
		Prozessdaten, Rohdatensatz (sign./unsign. Teil), privater Schlüssel	Auslesen des privaten Schlüssels	zusätzlich Manipulation der Stammdatenbank	**8**
		Prozessdaten, Rohdatensatz (sign./unsign. Teil), privater Schlüssel	Entschlüsselung des Signaturverfahrens	gewählte Signaturverfahren und Schlüssellängen unzureichend (DPG-Vorgabe: bis einschließlich 31.05.2022 RSA 1024, ECDSA P-192; seit 01.01.2012 sind ECDSA 224 (SHA224) und 256 (SHA256) möglich; seit 01.06.2012 ist für mit neuer Seriennummer in der Stammdatenbank angelegte DPG-Rücknahmevorrichtungen ECDSA 256 (SHA256) verpflichtend)[1]	**6**
		Prozessdaten, Rohdatensatz (sign./unsign. Teil), privater Schlüssel	Inhalt der Nachricht wird so nachgebildet, dass sich ein identischer Hashwert ergibt	unzureichendes Hash-Verfahren	**1**

[1] Vorgaben zur Einführung der neuen Signaturvorgaben siehe IT-Prüfschema Teil 3

2.6.2 Generische Sicherheitsanforderungen an die Instanz Krypto

Bedrohung bei Verletzung des Grundwertes Vertraulichkeit	Schwachstelle, Beschreibung	Generische Sicherheitsanforderung
Auslesen des privaten Schlüssels	unzureichender Zugriffsschutz des privaten Schlüssels	Schutz der Vertraulichkeit des privaten Schlüssels
Auslesen des privaten Schlüssels	unzureichender Zugriffsschutz des privaten Schlüssels, zusätzlich Manipulation der Stammdatenbank	Schutz der Vertraulichkeit des privaten Schlüssels UND Schutz der Integrität der Stammdatenbank
Entschlüsselung des Signaturverfahrens	gewählte Signaturverfahren[2] und Schlüssellängen unzureichend (DPG-Vorgabe: bis einschließlich 31.05.2022 RSA 1024, ECDSA P-192 (SHA1); seit 01.01.2012 sind ECDSA 224 (SHA224) und ECDSA 256 (SHA256) möglich; seit 01.06.2012 ist für mit neuer Seriennummer in der Stammdatenbank angelegte DPG-Rücknahmevorrichtungen ECDSA 256 (SHA256) verpflichtend)	Umschalten auf ausreichende Schlüssellängen und/oder sichere Signaturverfahren
Inhalt der Nachricht wird so nachgebildet, dass sich ein identischer Hashwert ergibt	unzureichendes Hash-Verfahren	Umschalten auf ausreichend sichere Hash-Verfahren

2.6.3 Detaillierung der Sicherheitsanforderungen

2.6.3.1 Schutz der Vertraulichkeit des privaten Schlüssels

Die folgenden Sicherheitsanforderungen gelten gleichermaßen für den Umgang mit dem privaten Schlüssel innerhalb wie außerhalb der DPG-Rücknahmevorrichtung. Somit wird sowohl die Erzeugung von Schlüsseln beim Hersteller außerhalb der DPG-Rücknahmevorrichtung mit anschließender Einbringung in die DPG-Rücknahmevorrichtung abgedeckt, als auch die Erzeugung und Handhabung von Schlüsseln innerhalb der DPG-Rücknahmevorrichtung.

Lebenszyklus privater Signaturschlüssel	Bedrohung	Schwachstelle	Sicherheitsanforderungen
Generierung von Zufallszahlen[3]	1. Erzeugung nicht zufälliger Zahlen	Ausnutzung von Regelmäßigkeiten für Angriffe zur Erlangung des privaten Schlüssels	Verwendung von Zufallszahlengeneratoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils SoM-hoch Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
	2. Auslesen von Zufallszahlen	Erlangen des privaten Schlüssels durch Berechnung desselben auf Basis der verwendeten Zufallszahl	Schutz des Zufallszahlengenerators vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu reali-

[2] Vorgaben zur Einführung der neuen Signaturvorgaben siehe IT-Prüfschema Teil 3.

[3] Zufallszahlen sind zur Schlüsselerzeugung erforderlich.

Lebenszyklus privater Signaturschlüssel	Bedrohung	Schwachstelle	Sicherheitsanforderungen
			sieren Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
	3. Manipulation von Zufallszahlen	Setzen des privaten Schlüssels durch Vorbestimmung der zur Schlüsselgenerierung verwendeten Zufallszahl	Schutz des Zufallszahlengenerators vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
Transport von Zufallszahlen und Speicherung der Zufallszahlen und sichere Löschung von Zufallszahlen	1. Auslesen von Zufallszahlen	Erlangen des privaten Schlüssels durch Berechnung desselben auf Basis der verwendeten Zufallszahl	Schutz des Zufallszahlengenerators vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
	2. Manipulation von Zufallszahlen	Setzen des privaten Schlüssels durch Vorbestimmung der zur Schlüsselgenerierung verwendeten Zufallszahl	Schutz des Zufallszahlengenerators vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
Generierung eines Schlüsselpaares und Administration der Schlüssel (Schlüsselmanagement inkl. Generierung neuer Schlüssel, sofern möglich)	1. Erzeugung „schwacher“ oder „fehlerhafter“ Schlüssel	Erlangen des privaten Schlüssels durch Kryptoanalyse	Einsatz von kryptographisch korrekten - Algorithmen, deren - Implementierungen sowie den - zugehörigen Parametersätzen. RSA: gem. Bundesanzeiger für die Anwendung im SigG Bereich (nur noch bis einschließlich 31.05.2022 gültig; vom 01.06.2012 an nicht mehr gültig für mit neuer Seriennummer in der Stammdatenbank angelegte DPG-Rücknahmevorrichtungen)[4] ECDSA: Verwendung einer Kurve, die bekanntermaßen keine Schwachstellen aufweist; Schlüssel muss eine echte Zufallszahl sein Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
	2. Auslesen des privaten Schlüssels	Erlangen des privaten Schlüssels durch - direktes Auslesen - Side-Channel-Attacken oder	Schutz des Schlüssels vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu reali-

[4] Vorgaben zur Einführung der neuen Signaturvorgaben siehe IT-Prüfschema Teil 3.

Lebenszyklus privater Signatur-schlüssel	Bedrohung	Schwachstelle	Sicherheitsanforderungen
		- durch andere Angriffe, für die der jeweilige Algorithmus und seine Implementierung nach dem aktuellen Stand der Technik anfällig ist.	sieren. Neben der Möglichkeit, den privaten Schlüssel vor Ort auszutauschen, ist ein Austausch des privaten Schlüssels unter Nutzung gesicherter Kommunikationskanäle möglich. Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
	3. Manipulation des privaten Schlüssels	Setzen des privaten Schlüssels durch Vorbestimmung der Schlüsseldaten (dieser Angriff erfordert gleichzeitig auch das Setzen des öffentlichen Schlüssels!)	Schutz des Schlüssels vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren. Neben der Möglichkeit, den privaten Schlüssel vor Ort auszutauschen, ist ein Austausch des privaten Schlüssels unter Nutzung gesicherter Kommunikationskanäle möglich. Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)
Speicherung des Schlüsselpaares und Transport und Verarbeitung des Schlüsselpaares und sichere Löschung des Schlüsselpaares	1. Auslesen des privaten Schlüssels	Erlangen des privaten Schlüssels durch - direktes Auslesen - Side-Channel-Attacken oder - durch andere Angriffe, für die der jeweilige Algorithmus und seine Implementierung anfällig ist.	Schutz des Schlüssels vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren. Neben der Möglichkeit, den privaten Schlüssel vor Ort auszutauschen, ist ein Austausch des privaten Schlüssels unter Nutzung gesicherter Kommunikationskanäle möglich. Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten).
	2. Manipulation des privaten Schlüssels	Setzen des privaten Schlüssels durch Vorbestimmung der Schlüsseldaten (dieser Angriff erfordert gleichzeitig auch das Setzen des öffentlichen Schlüssels!)	Schutz des Schlüssels vor unberechtigtem Zugriff: Dies ist durch bauliche, organisatorische, personelle oder technische Maßnahmen oder eine Kombination derselben zu realisieren. Neben der Möglichkeit, den privaten Schlüssel vor Ort auszutauschen, ist ein Austausch des privaten Schlüssels unter Nutzung gesicherter Kommunikationskanäle möglich. Ferner ist die Sicherheitsmaßnahme „Nachweis“ umzusetzen (s. Beschreibung unten)

Beschreibung der Sicherheitsmaßnahme „**Nachweis**“:

Für die Komponenten innerhalb der DPG-Rücknahmevorrichtung[5], welche den privaten Schlüssel oder Bestandteile davon oder Rohdaten zur Bildung der Schlüssel (wie z.B. Zufallszahlen) verwenden, sind folgende Nachweise zu erbringen:

[5] Gilt beispielsweise für Fälle, in denen die Schlüsselerzeugung und das Schlüsselhandling vollständig in der DPG-Rücknahmevorrichtung durchgeführt wird. Werden Teile davon außerhalb der DPG-Rücknahmevorrichtung durchgeführt, sind für die betroffenen Komponenten noch zusätzlich die Nachweise für Komponenten außerhalb der DPG-Rücknahmevorrichtung zu erbringen (s. Text weiter unten).

- Nachweis der grundsätzlichen Vertrauenswürdigkeit der Komponenten

sowie

- Nachweis der Resistenz der Komponenten gegenüber den jeweils genannten Angriffen.

Für Komponenten außerhalb der DPG- Rücknahmevorrichtung[6], welche den privaten Schlüssel oder Bestandteile davon oder Rohdaten zur Bildung der Schlüssel (wie z.B. Zufallszahlen) verwenden, sind folgende Nachweise zu erbringen:

- Nachweis der grundsätzlichen Vertrauenswürdigkeit der Komponenten

sowie

- Nachweis der Resistenz der Komponenten gegenüber den jeweils genannten Angriffen.

Setzt ein Hersteller von DPG-Rücknahmevorrichtungen zur Sicherung der außerhalb der DPG-Rücknahmevorrichtung liegenden Komponenten Maßnahmen baulicher, organisatorischer oder personeller Art ein, so ist deren Wirksamkeit in regelmäßigen Abständen von einer geeigneten, unabhängigen Instanz prüfen zu lassen.

2.6.3.2 Umschalten auf ausreichende Schlüssellängen und/oder sichere Signaturverfahren

	Bedrohung	**Schwachstelle**	**Sicherheitsanforderungen**
	1. Entschlüsselung des Signaturverfahrens (der verwendete Algorithmus ist unabhängig von der eingesetzten Schlüssellänge als unsicher einzustufen)	Die Ergebnisse einer kryptographischen Berechnung können unter Ausnutzung einer Schwachstelle im Algorithmus erzielt werden[7]	Bei nachweislich erfolgter Entschlüsselung des eingesetzten Algorithmus, Information an die DPG und Abstimmung der weiteren Vorgehensweise (z.B. systemweiter Austausch des Algorithmus)
	2. Schwachstelle in der Implementierung eines Signaturverfahrens (der verwendete Algorithmus ist mathematisch als sicher einzustufen, aber die gewählte Implementierung wird angreifbar)	Bei einer bestimmten Art der Implementierung eines Algorithmus können Ergebnisse einer kryptographischen Berechnung unter Ausnutzung einer Schwachstelle im Algorithmus erzielt werden[8]	Wurde eine wirksame Schwachstelle der eingesetzten Implementierung entdeckt, Austausch der Implementierung oder Einsatz eines alternativen nach aktuellen Stand der Technik sicheren Algorithmus (inkl. dessen sicherer Implementierung und sicherer Parametersätze)
	3.„Alterung“ der gewählten Schlüssellänge (Aufgrund steigernder Rechenleistung potentieller für Angriffe einsetzbarer Rechnersysteme ist die Verwendung von Schlüsseln unterhalb einer bestimmten Länge nicht mehr als sicher einzustufen)	Der private Schlüssel kann von ausreichend leistungsstarken Rechnersystemen mittels einer Brute-Force-Attacke ermittelt werden	Marktbeobachtung. Ggf. in Abstimmung mit der DPG Definition eines Umstiegszenarios

[6] Gilt beispielsweise für Fälle, in denen die Schlüsselerzeugung und das Schlüsselhandling vollständig außerhalb der DPG-Rücknahmevorrichtung durchgeführt wird. Werden Teile davon in der DPG-Rücknahmevorrichtung durchgeführt, sind für die betroffenen Komponenten noch zusätzlich die Nachweise für Komponenten in der DPG-Rücknahmevorrichtung zu erbringen (S. Text weiter oben).
[7] …auch ohne, dass der private Schlüssel vorliegt.
[8] …auch ohne, dass der private Schlüssel vorliegt.

2.6.3.3 Umschalten auf ausreichend sichere Hash-Verfahren

	Bedrohung	Schwachstelle	Sicherheitsanforderungen
	Entschlüsselung des Hash-Verfahrens (der Einsatz des Hash-Algorithmus ist als unsicher einzustufen[9])	Die Korrektheit einer Signatur kann angezweifelt werden, weil ihr unterschiedliche Eingangsdaten zu Grunde liegen können	Bei nachweislich erfolgter Entschlüsselung des eingesetzten Hash-Algorithmus, Information an die DPG und Abstimmung der weiteren Vorgehensweise (z.B. systemweiter Austausch des Algorithmus).

2.7 Instanz Kommunikation (A8a, Z8a)

In der Kommunikation wird der Headerdatensatz generiert.

2.7.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
in Kommunikation: Generierung des Headerdaten-satzes	A8a Z8a	Rohdatensatz (sign./unsig-nierter Teil), Headerdaten-satz, Automa-tenstammdaten	Fehlerhafte Angaben im Headerdatensatz	Kommunikations-instanz ist fehlerhaft	**1**
in Kommunikation: Erzeugung von separaten NoRead-Datei	Z8a	NoRead-Daten, Automatensta mmdaten	Fehlerhafte Angaben in NoRead-Datei	Kommunikations-instanz ist fehlerhaft	**1**

2.7.2 Detaillierung der Schutzanforderungen

- Zur Sicherstellung der Integrität der Rohdatensätze (mit signiertem und unsigniertem Teil) sind unter anderem die Vertraulichkeit der privaten Schlüssel und die Angemessenheit der Kryptoverfahren entscheidend. Die Anforderungen hierzu sind in Kapitel 2.6 definiert.
- Die Daten in der Kommunikation (Automatenstammdaten, Rohdatensatz (mit signierten und unsignierten Teil), Headerdatensatz, NoRead-Daten) müssen gegen unberechtigte Veränderung und unberechtigten Zugriff geschützt sein.
- Ein unbefugter Zugriff auf die Programme der Kommunikation muss verhindert werden. Dies gilt während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und deren Betrieb. Die Programme dürfen keine unerwünschten Funktionen ausführen können, d.h. sie dürfen nur die spezifizierten und durch die DPG freigegebenen Funktionen ausführen können. Dieses ist durch geeignete Mittel zu verifizieren.

[9] Beispielsweise, weil so genannte Kollisionen gefunden wurden (bei verschiedenen Eingangsdaten ergibt sich ein und derselbe Hashwert).

- Die Programme der Kommunikation müssen sich gegen Manipulation schützen. Veränderungen an den Programmen müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen, müssen erfolgen (z.B. Einstellung des Betriebs). Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Das unautorisierte Aussenden von Rohdatensätzen (mit signiertem und unsigniertem Teil) bzw. NoRead-Daten an den Forderungssteller muss erkannt und verhindert werden.

3. Anforderungen an die Kommunikation zwischen den Instanzen

3.1 Sensor – Prüfung (A1, Z1)

Der gelesene EAN-Barcode und die DPG-Markierung werden vom Sensor an die Prüfinstanz (kann Automatensteuerung oder auch Kamera sein) übergeben.

3.1.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	**Schwachstelle**	**Risiko**
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe des gelesenen EAN-Barcodes und der DPG-Markierung von Sensor an Prüfinstanz (kann Automatensteuerung oder auch Kamera sein)	A1 Z1	GTIN, DPG-Markierung	Vortäuschen der DPG-Markierung	einfacher Zugang zur Übertragungsstrecke und zur Codierung	**1**
		GTIN, DPG-Markierung	Änderung der GTIN auf einen einzigen Erstinverkehrbringer	einfacher Zugang zur Übertragungsstrecke und zur GTIN	**1**

3.1.2 Detaillierung der Schutzanforderungen

- Das Flag der DPG-Markierung muss auf der Übertragungsstrecke zwischen Sensor und Prüfung gegen unberechtigte Veränderung geschützt werden.
- Die GTIN ist während der Übertragung zwischen Sensor und Prüfung mit geeigneten Mitteln gegen unberechtigte Veränderung zu schützen.[10]

3.2 Prüfung – Steuerung (A2)

Es wurden keine Risiken ermittelt.

3.3 Prüfung – Generator (Z2)

Es wurden keine Risiken ermittelt.

[10] Auf die Anforderung nach Erkennung möglicher Veränderung wird an dieser Stelle aufgrund der niedrigen Risikokennzahl verzichtet.

3.4 Kompaktor – Steuerung (A4)

Der Kompaktor leitet ein Signal an die Steuerung.

3.4.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe eines Signals vom Kompaktor an die Steuerung	A4	Signal	Manipulation des Signals in ein positives Signal	Manipulation durch schreibenden Zugriff auf Kompaktierer	**5**

3.4.2 Detaillierung der Schutzanforderungen

- Eine positive Rückmeldung des Kompaktors darf nur bei einer erfolgreichen Kompaktierung erfolgen.
- Das Signal des Kompaktors muss auf dem Übertragungsweg zwischen Kompaktor und Steuerung derart geschützt sein, dass eine unberechtigte Veränderung des Signals nicht möglich ist.
- Veränderungen an dem Signal während der Übertragung müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen. Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.

3.5 Steuerung – Prüfung (A5)

Es wurden keine Risiken ermittelt.

3.6 Prüfung – Generator (A6, Z6)

Die GTIN wird von der Prüfinstanz an den Generator übertragen.

3.6.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe GTIN von Prüfinstanz an	A6 Z6	GTIN	Einspielen von beliebigen GTIN in Generator	Zugang zur Übertragungsstrecke	**7**

Generator					

3.6.2 Detaillierung der Schutzanforderungen

- Die GTIN darf nur bei einer positiven Rückmeldung des Kompaktors (=erfolgreiche Kompaktierung der DPG-Verpackung) von der Prüfinstanz an den Generator weiter geleitet werden.
- Die GTIN muss auf dem Übertragungsweg zwischen Prüfinstanz und Generator derart geschützt sein, dass eine unberechtigte Veränderung nicht möglich ist.
- Veränderungen an der GTIN während der Übertragung müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen. Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Der Generator darf nur GTIN weiter verarbeiten, die zweifelsfrei aus der Prüfinstanz stammen.

3.7 Generator – Krypto (A7, Z7)

Die unsignierten Prozessdaten werden vom Generator an die Kryptoinstanz übergeben.

3.7.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	**Schwachstelle**	**Risiko**
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe der Prozessdaten von Generator an Krypto	A7 Z7	Prozessdaten	willkürliche Einspielung von Prozessdaten in Krypto (s. A6/Z7)	unzureichende Absicherung externer Schnittstellen	**7**
		Prozessdaten	willkürliche Einspielung von Prozessdaten in Krypto (s. A6/Z7)	unzureichende Prüfung der Einspielung von unautorisierten Programmen	**7**

3.7.2 Detaillierung der Schutzanforderungen

- Die Prozessdaten müssen auf dem Übertragungsweg zwischen Generator und Kryptoinstanz derart geschützt sein, dass ihre unberechtigte Veränderung nicht möglich ist.
- Veränderungen an den unsignierten Prozessdaten während der Übertragung müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen (z. B. Einstellung des Betriebs). Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Die Kryptoinstanz darf nur Prozessdaten weiter verarbeiten, die zweifelsfrei aus dem Generator stammen.

- Das unautorisierte Einspielen von Prozessdaten in die Kryptoinstanz muss erkannt und verhindert werden. Entsprechende Reaktionen müssen auch für wieder eingespielte Prozessdaten erfolgen.

3.8 Krypto – Kommunikation (A8, Z8)

Der Rohdatensatz (mit signiertem und unsigniertem Teil) wird von der Kryptoinstanz an die Kommunikation übergeben.

3.8.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	**Schwachstelle**	**Risiko**
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe des Rohdatensatzes (sign./unsign. Teil) von Krypto an Kommunikation	A8 Z8	Rohdatensatz (sign./unsign. Teil)	Einspielen gefälschter Rohdatensätze (sign./unsign.Teil)	unzureichende Vertraulichkeit des privaten Schlüssels	**8**

3.8.2 Detaillierung der Schutzanforderungen

- Zur Verhinderung des Einspielens von gefälschten Rohdatensätzen (mit signiertem und unsigniertem Teil) sind unter anderem die Vertraulichkeit der privaten Schlüssel und die Angemessenheit der Kryptoverfahren entscheidend. Die Anforderungen hierzu sind in Kapitel 2.6 definiert.
- Der Rohdatensatz (mit signiertem und unsigniertem Teil) muss auf dem Übertragungsweg zwischen Kryptoinstanz und Kommunikation derart geschützt sein, dass eine unberechtigte Veränderung des Rohdatensatzes (mit signiertem und unsigniertem Teil) nicht möglich ist.
- Veränderungen an den Rohdatensätzen (mit signiertem und unsigniertem Teil) während der Übertragung müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen (z. B. Funktionsunterbrechung). Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Die Kommunikation darf nur Rohdatensätze (mit signiertem und unsigniertem Teil) weiter verarbeiten, die zweifelsfrei aus der Krypto-Instanz stammen.
- Das unautorisierte Einspielen von Rohdatensätzen (mit signiertem und unsigniertem Teil) in die Kommunikation muss erkannt und verhindert werden. Entsprechende Reaktionen müssen auch für wieder eingespielte Rohdatensätze (mit signiertem und unsigniertem Teil) erfolgen.

3.9 Generator – Kommunikation (Z7b)

Der Prozessdatensatz wird vom Generator an die Kommunikation übergeben.

3.9.1 Übersicht aus der Risikobewertung

			Bedrohung bei Verletzung des Grundwertes…	Schwachstelle	Risiko
Prozessschritt	**Referenznummer**	**Werte**	**Integrität**	**Beschreibung**	**Risikowert (0-8)**
Übergabe der Prozessdaten von Generator an Kommunikation	Z7b	Prozessdaten	willkürliche Einspielung von Prozessdaten in Kommunikation	unzureichende Absicherung externer Schnittstellen	**1**
		Prozessdaten	willkürliche Einspielung von Prozessdaten in Kommunikation	unzureichende Prüfung der Einspielung von unautorisierten Programmen	**1**

3.9.2 Detaillierung der Schutzanforderungen

- Der Prozessdatensatz muss auf dem Übertragungsweg zwischen Generator und Kommunikation derart geschützt sein, dass eine unberechtigte Veränderung des Prozessdatensatzes nicht möglich ist.
- Veränderungen während der Übertragung müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen. Die für die Sicherung der Integrität relevanten Informationen müssen ebenfalls gegen Manipulation gesichert sein.
- Die Kommunikation darf nur Prozessdaten verarbeiten, die zweifelsfrei aus der Generatorinstanz stammen.
- Das unautorisierte Einspielen von in die Kommunikation muss erkannt und verhindert werden. Entsprechende Reaktionen müssen auch für wieder eingespielte Prozessdatensätze erfolgen.

4. Weitere Anforderungen

In diesem Kapitel sind Anforderungen definiert, die prozessübergreifend gültig sind.

- Innerhalb der DPG-Rücknahmevorrichtung sind alle sicherheitsrelevanten Daten zu protokollieren und zu speichern, die notwendig sind, um sicherheitsrelevante Zwischenfälle zu entdecken und aufzuklären.
- Bezüglich der Signaturvorgaben ist das Dokument „Signaturvorgaben im Rahmen des Pfandsystems der Deutschen Pfandsystem GmbH, Version 2.0“ umzusetzen; bezüglich der sicherheitstechnischen Anforderungen sind die in diesem Dokument definierten Anforderungen umzusetzen.

5. Anhänge

5.1 Glossar

AIS	Anwendungshinweise und Informationen zum Schema
Artikelstammdaten	siehe „Schnittstellenbeschreibung Einwegpfand, Artikelstammdaten“ in der jeweils aktuellen Fassung
Automatenstammdaten	Siehe „Schnittstellenbeschreibung Einwegpfand, Automaten“ in der jeweils aktuellen Fassung
CC	Common Criteria
Headerdatensatz	Nachrichten-Referenz, Nachrichten-Typ, Nachrichten-Version, Nachrichten-Datum, Nachrichten-Sender, Nachrichten-Empfänger, Nachrichtenfunktion
Rohdatensatz (mit signiertem und unsigniertem Teil)	Positionsnummer, Hersteller DPG-Rücknahmevorrichtungen, Seriennumer DPG-Rücknahmevorrichtung, GTIN, Zeitstempel (Datum/Uhrzeit), **Signatur**, Rücknahmestelle, ggf. Sacknummer
SigG	Signaturgesetz
Prozessdaten	Positionsnummer, Hersteller DPG-Rücknahmevorrichtungen, Seriennummer DPG-Rücknahmevorrichtung, GTIN, Zeitstempel (Datum/Uhrzeit), Rücknahmestelle, ggf. Sacknummer

5.2 Verpflichtung aufgrund von Vorgaben in anderen Dokumenten mit Bezug zu sicherheitstechnischen Anforderungen an die IT in DPG-Rücknahmevorrichtungen

- Prozessdokumentation eines bundeseinheitlichen Rücknahmesystems für Getränke-Einwegverpackungen in der aktuellen Version
- AIS 20
- AIS 31
- Signaturvorgaben im Rahmen des Pfandsystems der DPG Deutsche Pfandsystem GmbH, in der aktuellen Version

5.3 Übersicht Erzeugung signierter Rohdatensatz

Übersicht - Mögliche Fälle bei Auslesung einer Verpackung

Fall	1.	2.	3.	4.	5.
Lesbarkeit EAN-Barcode	möglich	möglich	möglich	**nicht möglich**	möglich
GTIN in Stamm-datenbank	vorhanden	**nicht vorhanden oder nicht gültig**	vorhanden	-	**gesperrt**
DPG- Markierung	erfolgreich	-	**nicht erfolgreich**	-	-
Ergebnis	Rohdatensatz (mit Signatur)	NoRead ohne Signatur	NoRead ohne Signatur	NoRead ohne Signatur	NoRead ohne Signatur

Ein Rohdatensatz darf nur noch erzeugt werden, wenn

- die GTIN durch Auslesung des EAN-Barcodes erkannt wurde,
- die GTIN in der Stammdatenbank gültig hinterlegt ist und
- die Überprüfung der DPG-Markierung erfolgreich ist.

In allen anderen Fällen wirft die DPG-Rücknahmevorrichtung die Verpackung aus, bzw. im Zählzentrum kann ein NoRead-Datensatz (Prozessdatensatz als Zählbericht) erzeugt werden.