DPG Deutsche Pfandsystem GmbH

Anlage 7 Anhang 3

IT-Prüfschema

Stand: 14. Juni 2016

(Inkrafttreten: 01. Oktober 2016)

zu den Teilnahmebedingungen

Inhaltsverzeichnis

1. Einleitung 4
1.1 Adressatenkreis 4
1.2 Anwendungshinweise 4
2. Leitlinie für die IT-Prüfung 4
2.1 Ablauf eines Audits 5
2.2 Ziel und Umfang eines Audits 5
2.4 Durchführung des Audits 7
2.5 Erstellen des Auditberichts 7
2.6 Zertifizierungsprozess 8
2.7 Wiederholungsaudit 8
3. Prüfschema für IT-Auditoren 8
3.1 Anforderungen an DPG-Rücknahmevorrichtungen 9
3.1.1 Zugriffskontrolle 9
3.1.2 Funktionsumfang 10
3.1.3 Erweiterter Schutz der Integrität von Objekten 10
3.1.4 Störmodus bei negativem Kompaktorsignal 11
3.1.5 Positives Kompaktorsignal als Voraussetzung für die Übermittlung der GTIN 12
3.1.6 Kontrollierter Versand gültiger Objekte 12
3.1.7 Korrekte Zeitstempel 12
3.1.8 Kontrolliertes Einspielen von Objekten 13
3.1.9 Erkennen von Wiedereinspielung 13
3.1.10 Verwendung anerkannter Zufallszahlengeneratoren 14
3.1.11 Autorisierter Versand gültiger Objekte an Forderungssteller 14
3.1.12 DPG-Automaten: Positive Rückmeldung des Kompaktors bei erfolgreicher Kompaktierung 14
3.1.13 Absenderüberprüfung des Generators für GTIN 15
3.1.14 Absenderüberprüfung der Kryptoinstanz für unsignierte Prozessdaten 15
3.1.15 Absenderüberprüfung der Kommunikation für Rohdatensätze 16
3.1.16 Generierung von Protokollen 16
3.2 Anforderungen an die Einsatzumgebung 17
3.2.1 Sicherheit in der Entwicklung, der Installation und im Anlauf des Systems 17
3.2.2 Kryptographische Algorithmen 18
3.2.3 Vertrauenswürdige und getestete Krypto- und Signaturkomponenten 18
3.2.4 Kenntnis über die Entwicklungen im Bereich eingesetzter kryptographischer Verfahren 18
3.2.5 Ersatz für verwendete kryptographischer Verfahren 19
3.2.6 Ersatz für verwendete kryptographischer Verfahren 19
4. Literatur 19
Anhang, Teil 1: 20
Anhang, Teil 2 23
Anhang, Teil 3: 32

Versionshistorie

Version	Datum	Geänderte Kapitel	Grund der Änderung	Geändert durch
0.8	24.03.2006	Alle	Erstellung	Diederich
0.82	07.04.2006	Alle 1.2	Redaktionell (QM) Anerkennung als IT-Prüfstelle	Diederich/ Maseberg
1.1	10.04.2006	Kapitel 2.8 Kapitel 3 Teil 2 (vormals Teil B)	Neu: Kapitel 2.8 Reauditierung Neue Struktur Produkt/Einsatzumgebung Zusammenführung der Anforderungen 1 und 5 aus Version 0.8 Anwendungshinweis bzgl. pos. Kompaktorsignal Anpassung an Kapitel 3 Ergänzung um Risikowerte für Instanzen	Diederich
1.2	10.04.2006	Kapitel 3	Fehlerkorrektur	Diederich
1.3	31.07.2006	Kapitel 2.5 2.6 Alle	Ergänzende Informationen zur Zusammenarbeit von Prüfern der IT und der Mechanik Neuer Sprachgebrauch: Statt Zertifizierung jetzt Zulassung (zur Differenzierung vom BSI) in allen Begriffen sowie statt Rezertifizierung nunmehr Reauditierung	Diederich
1.4	05.06.2007		Redaktionelle Überarbeitung	Dambacher
1.5	18.09.2009	Kapitel 1 Kapitel 2.2 2.3 2.4 Kapitel 3.1 3.2 3.3 Anhang Teil 1 Teil 2	Redaktionelle Überarbeitung " " " " " " " "	AG IT-Zertifizierer
1.6	30.05.2011	Teil 2 und 3 des Anhangs	Aufnahme neuer Signaturverfahren	DPG
1.7	10.09.2013	Kapitel 1-3 Anhang Teil 3	Redaktionelle Überarbeitung Redaktionelle Aktualisierung der Regelungen zum Signaturverfahren	DPG
1.7	14.06.2016		Redaktionelle Überarbeitung (GTIN-Strichcode durch EAN-Barcode ersetzt)	DPG

1. Einleitung

Das vorliegende Prüfschema für IT-Auditoren beschreibt die verbindliche Vorgehensweise, wie IT-Auditoren die IT-Prüfung durchführen müssen, die Teil der Zertifizierung von DPG-Automaten und Zählzentren durch von der DPG zugelassene Zertifizierungsstellen ("**Zertifizierungsstellen**") ist.

Die im Rahmen der IT-Prüfung zu überprüfenden "**Sicherheitstechnische(n) Anforderungen an die IT in DPG-Rücknahmevorrichtungen**" ("**IT-Anforderungen**") zur Zertifizierung von DPG-Automaten und Zählzentren sind in **Teil 1** des Anhangs in einer tabellarischen Gesamtübersicht zusammengefasst (nachfolgend: Anforderungsliste).

Das **unter Punkt 3** aufgeführte Prüfschema dient als Checkliste für die IT-Prüfung von DPG-Rücknahmevorrichtungen, die innerhalb des DPG-Systems zur Rücknahme von DPG-Verpackungen eingesetzt werden dürfen (vgl. **Teil 2** des Anhangs).

Zusätzlich zu den Anforderungen an die IT sind die Signaturvorgaben ("**Signaturvorgaben**") der DPG zu berücksichtigen (vgl. **Teil 3** des Anhangs).

1.1 Adressatenkreis

Dieses Dokument gilt als verbindliche Vorgabe für von Zertifizierungsstellen benannte IT-Auditoren. IT-Auditoren führen eine unabhängige Auditierung durch, um die Umsetzung der IT-Anforderungen durch einen Hersteller DPG-Rücknahmevorrichtungen oder in einem Zählzentrum zu bestätigen.

Hersteller von DPG-Rücknahmevorrichtungen und Zählzentrumbetreiber können sich mithilfe der dargestellten Anforderungen an die IT einen Überblick darüber verschaffen, welche Anforderungen bei einem Audit gestellt werden und welche Referenzdokumente zur Verfügung gestellt werden müssen.

1.2 Anwendungshinweise

Als IT-Auditoren werden nur vom Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierte Prüfstellen für IT-Sicherheit (Common Criteria) eingesetzt. Es liegt daher nahe, sich an den bestehenden Prüfschemata und Vorgaben des BSI zu orientieren. Der Aufbau dieses Dokumentes orientiert sich daher an ZertISO27001.

2. Leitlinie für die IT-Prüfung

Die in diesem Kapitel beschriebenen Leitlinien für die IT-Prüfung entsprechen weitestgehend den Audit-Prinzipien und dem Audit-Prozess gemäß ZertISO27001 Kapitel 2 und 3.

Im Rahmen einer BSI-Zulassung nach Common Criteria sind die folgenden vier universellen Prinzipien für eine Evaluation zu befolgen:

- Unvoreingenommenheit
- Objektivität
- Wiederholbarkeit
- Reproduzierbarkeit

Nachfolgend werden die Prinzipien des BSI-Prüfschemas für ISO 27001-Audits aus ZertISO27001 wiedergegeben, die für ein Audit im Rahmen einer ISO 27001-Zulassung erfüllt werden müssen:

Ethisches Verhalten:

Die Grundlage des Berufsbildes eines Auditors ist die Vertrautheit mit der Informationssicherheitstechnik.

Da im Umfeld IT-Sicherheit oft sensible Geschäftsprozesse und Daten zu finden sind, sind die Vertraulichkeit der Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen des Audits eine wichtige Arbeitsgrundlage.

Sachliche Darstellung:

Ein Auditor hat die Pflicht, sowohl seinem Auftraggeber als auch der Zertifizierungsstelle wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehört die wahrheitsgemäße und nachvollziehbare Darstellung des Sachverhalts in den Audit-Feststellungen, Audit-Schlussfolgerungen und dem Audit-Bericht. Die Ergebnisse des Audits müssen wiederholbar sein (bei unverändertem Sachstand).

Angemessene Sorgfalt:

Ein Auditor muss bei der Auditierung mit Sorgfalt vorgehen. Sein Urteilsvermögen ist unerlässliche Voraussetzung für sachgerechte und fundierte Audits.

Unabhängigkeit und Objektivität:

Die Grundlage für die Unparteilichkeit des Audits weist der Auditor in Form einer Unabhängigkeitserklärung nach. Dabei ist zu bestätigen, dass die Ergebnisse des Audit-Reportes auf eigenen Audits beruhen, weisungsfrei und unabhängig durchgeführt wurden. Dabei darf der Auditor in den letzten zwei Jahren nicht im Umfeld des Untersuchungsgegenstandes beratend tätig gewesen sein.

Alle Audit-Schlussfolgerungen müssen objektiv nachvollzogen werden können.

Nachweise:

Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Audit-Schlussfolgerungen in einem systematischen Audit-Prozess zu kommen, ist die eindeutige und folgerichtige Dokumentation der Ergebnisse. Die Audit-Nachweise müssen verifizierbar sein. Hierbei können die Ergebnisse auf Stichproben der verfügbaren Informationen beruhen, da ein Audit während eines begrenzten Zeitraumes und mit begrenzten Ressourcen vorgenommen wird. Die Auswahl der Stichproben muss relevant und in einem sinnvollen Umfang vorgenommen werden. (Quelle: ZertISO27001).

2.1 Ablauf eines Audits

Der nachfolgend geschilderte Ablauf eines Audits entspricht dem Ablauf eines Audit-Prozesses gemäß ZertISO27001 Kapitel 3.1. Nachdem ein Antragssteller (Hersteller von DPG-Rücknahmevorrichtungen bzw. Zählzentrumbetreiber) alle Anforderungen an die IT erfüllt hat und alle relevanten Dokumente für einen entsprechenden Nachweis vorliegen, wird die erfolgreiche IT-Prüfung durch die Zertifizierungsstelle in der Prüfliste für DPG-Automaten bzw. Zählzentren bestätigt. Der IT-Auditor dokumentiert seine Prüfergebnisse in einem Prüfbericht für die Zertifizierungsstelle, als Grundlage für die Zertifizierung.

2.2 Ziel und Umfang eines Audits

Entsprechend ZertISO27001 können Ziel und Umfang einer IT-Prüfung wie folgt beschrieben werden:

Ziel der IT-Prüfung ist die unabhängige Überprüfung der Umsetzung der IT-Anforderungen durch einen IT-Auditor.Die Überprüfung umfasst sowohl eine Dokumentenprüfung als auch eine Umsetzungsprüfung der DPG-relevanten Anforderungen vor Ort.

Zuständigkeiten im Prüfprozess

Analog zu ZertISO27001 läuft die IT-Prüfung nach folgender Zuständigkeitsverteilung ab:

- Antragsteller (Hersteller DPG-Rücknahmevorrichtungen oder Zählzentrumbetreiber);

- IT-Auditor;
- Zertifizierungsstelle.

Die Rolle des Antragstellers lässt sich auf der Basis von ZertISO27001 und BSI 7125 wie folgt beschreiben, er

- initiiert den Audit-Prozess;
- beauftragt eine Zertifizierungsstelle;
- gewährt Zugang zur Entwicklungs- und Produktionsumgebung;
- stellt das betriebsbereite Produkt bzw. den Zugang zu demselben bereit;
- unterstützt den IT-Auditor bei der Vor-Ort-Prüfung;
- führt eigene Korrektheitstests durch;
- führt ggf. eigene Penetrationstests durch;
- stellt die erforderlichen Dokumente zur Verfügung (einschließlich Testergebnisse).

Die Rolle des IT-Auditors lässt sich auf der gleichen Basis spezifizieren (ZertISO27001, BSI 7125), der IT-Auditor:

- muss vom BSI anerkannt und von einer Zertifizierungsstelle als Kooperationspartner benannt sein;
- muss das für die Prüfung notwendige Fachwissen besitzen oder über dieses als Teil eines Audit-Teams verfügen (bei Einsatz eines Audit-Teams sind die Rollen und Zuständigkeiten vor Auditbeginn festzulegen);
- bleibt auch bei Einsatz eines Audit-Teams oder Erfüllungsgehilfen allein verantwortlich für die IT-Prüfung;
- muss unabhängig und neutral sein, d.h. er und die Mitglieder seines Audit-Teams dürfen nicht in den letzten 2 Jahren im Umfeld des zu auditierenden Produktes beratend tätig gewesen sein. Eine entsprechende Unabhängigkeitserklärung des Auditors und aller Audit-Teammitglieder muss vor Beginn des Verfahrens (vor dem Audit) bei der Zertifizierungsstelle vorgelegt werden;
- darf nicht fachlich weisungsgebunden sein.
- Die Zertifizierungsstelle muss dem Einsatz des IT-Auditors bzw. des Audit-Teams zustimmen.

Auf der Grundlage von [ZertISO27001] und [BSI 7125] ist die Rolle der DPG beschrieben. Die DPG

- ist im gesamten Verfahren eine unabhängige dritte Instanz, die die Gleichwertigkeit der Prüfungen und Prüfberichte gewährleistet;
- ist Schiedsstelle zwischen IT-Auditor und Antragsteller (Hersteller DPG-Rücknahmevorrichtungen bzw. Zählzentrumbetreiber);
- stellt Fachwissen über Kriterien und Prüfverfahren zur Verfügung;
- stellt Dokumente bzgl. Kriterien und Prüfverfahren zur Verfügung.

Aufgrund der Möglichkeit zur Anerkennung von Zertifizierungsstellen durch die DPG wird zusätzlich festgelegt, dass allein die DPG für folgende, zusätzliche Tätigkeiten zuständig ist und nicht die von ihr zugelassenen Zertifizierungsstellen:

- Änderung von bestehenden Dokumenten oder Erstellen neuer Dokumente im Zusammenhang mit der DPG-Zulassung.
- DPG-Zulassung.

2.4 Durchführung des Audits

Analog zu (ZertISO27001) kann eine IT-Prüfung wie folgt durchgeführt werden:

Nach der Umsetzung aller Anforderungen an die IT beauftragt der Hersteller DPG-Rücknahmevorrichtungen bzw. Zählzentrumbetreiber eine Zertifizierungsstelle damit, in einer unabhängigen Prüfung die Umsetzung der Anforderungen an die IT zu verifizieren. Diese beauftragt einen IT-Auditor mit der IT-Prüfung.

Die IT-Prüfung wird in zwei Teilschritten durchgeführt. Als Erstes werden die vom Antragsteller vorgelegten Dokumente gesichtet und anhand der Prüfkriterien verifiziert. Die Ergebnisse werden im IT-Audit-Report dokumentiert. Im zweiten Schritt bereitet der Auditor eine "Vor-Ort-Prüfung" bei dem Antragsteller vor und begutachtet stichprobenartig die Umsetzung der dokumentierten Sachverhalte. Mängel werden im IT-Audit-Report festgehalten. Der Antragsteller hat die Möglichkeit, diese Mängel in einer vom IT-Auditor festgelegten Frist zu beheben.

Im Rahmen der Prüfung ist eine Zusammenarbeit von IT-Prüfern und Mechanik-Prüfern zwingend. Diese Zusammenarbeit gewinnt insbesondere dann an Bedeutung, wenn Sicherheitsanforderungen an die IT durch Anforderungen an die Mechanik oder Anforderungen im Bereich Mechanik IT-gestützt erfüllt werden. Die Prüfer der Mechanik und der IT müssen sich daher mit den Anforderungen an den jeweils anderen Bereich soweit auseinandersetzen, dass die Auswirkungen auf den eigenen Prüfbereich eingeschätzt und Prüfaspekte im gemeinsamen Bereich von Mechanik und IT erkannt werden können. Neben der direkten Kommunikation der Prüfer untereinander stehen den Prüfern auf den passwortgeschützten Internetseiten der DPG weitere Informationen (Bsp. Zertifizierungsrichtlinien, Zertifizierer) zur Verfügung.

Sofern Prüfaspekte identifiziert werden, die sowohl vom Prüfer der Mechanik als auch vom Prüfer der IT getestet werden können, muss der Prüfaspekt entweder einem der beiden Prüfer zugeordnet werden oder von beiden Prüfern in gemeinsamer Verantwortung überprüft werden. In jedem Fall müssen solche Prüfaspekte in beiden Prüfberichten adressiert werden und in mindestens einem der beiden Prüfberichte nachvollziehbar dokumentiert sein.

Kommt der IT-Auditor zu einem positiven Prüfergebnis, wird dies in der Prüfliste für DPG-Rücknahmevorrichtungen bzw. Zählzentren vermerkt. Bei einem negativen Ergebnis muss die Zertifizierungsstelle hierüber informiert werden, um über die weitere Vorgehensweise zu entscheiden. Die Zertifizierungsstelle überprüft den IT-Prüfbericht auf Vollständigkeit, Nachvollziehbarkeit und Reproduzierbarkeit der Prüfergebnisse. Nachforderungen oder Nachfragen werden an den IT-Auditor gestellt, der die ggf. bestehenden Unklarheiten beseitigt. Nach positivem Abschluss des Prüfprozesses sendet die Zertifizierungsstelle an die DPG den Prüfbericht und das Zertifikat.

2.5 Erstellen des Auditberichts

Dieser Abschnitt wurde aus ZertISO27001 übernommen und an die Umstände der DPG-Zulassung angepasst.

Der IT-Prüfbericht enthält alle Prüfergebnisse des IT-Auditors. Prüfergebnisse, die aus der Kooperation mit Prüfern der Mechanik hervorgegangen sind, müssen im Text des Auditberichts als solche klar dargestellt werden.

Der IT-Prüfbericht richtet sich an den Antragsteller und die Zertifizierungsstelle. Die Ergebnisse des IT-Prüfberichts werden vom IT-Auditor und der Zertifizierungsstelle vertraulich behandelt und an die DPG, aber nicht an Dritte weitergegeben.

Anhand des IT-Prüfberichtes kann der Antragsteller Mängel oder Verbesserungsmöglichkeiten in der Umsetzung der Anforderungen an die IT erkennen.

2.6 Zertifizierungsprozess

Auch hier kann für die Zertifizierung der Prozess für Zulassungen nach ISO27001 auf der Basis von IT-Grundschutz übernommen werden (ZertISO27001):

Wenn der IT-Prüfbericht bei der Zertifizierungsstelle vorliegt, wird dieser von der Zertifizierungsstelle geprüft.

Der Prüfbericht darf sich nur auf Prüfungen des IT-Auditors (Dokumentenprüfungen und Audit) stützen, die zum Zeitpunkt der Übergabe des IT-Prüfberichts an die Zertifizierungsstelle nicht älter als drei Monate sind (Aktualität der Prüfgrundlagen und -ergebnisse).

Ein Zertifikat wird nur erteilt, wenn ein positives Prüfungsergebnis im Bereich Mechanik und IT vorliegt.

2.7 Wiederholungsaudit

Die formalen und insbesondere vertraglichen Aspekte eines Wiederholungsaudits ergeben sich aus der jeweiligen Zertifizierungsrichtlinie. Die wiederholte Prüfung der IT richtet sich dabei nach der Fälligkeit des Wiederholungsaudits für die Mechanik-Zulassung. Unabhängig davon ist die Gültigkeit der Prüfergebnisse für die IT und damit eine der Grundlagen für die Zertifizierung daran gebunden, dass die DPG-Rücknahmevorrichtung bzw. der Betrieb des Zählzentrums nicht in DPG-relevanten Bereichen verändert wird.

Bei wesentlichen Änderungen an der Software ist eine Impact-Analyse des Herstellers notwendig, in der dargelegt wird, was geändert wurde und welche Auswirkungen sich daraus hinsichtlich der Anforderungen des IT-Prüfschemas an die Software ergeben. Wesentliche Änderungen sind Änderungen, die eine Instanz des Prüfschemas (Teil 2 des Anhangs) berühren, für die Bedrohungen mit einem Risikowert größer gleich 5 (also Risikowert 5, 6, 7 oder 8) identifiziert wurden. Die Impact-Analyse wird von einer Prüfstelle für IT-Sicherheit durchgeführt und der Zertifizierungsstelle vorgelegt. Je nach Ergebnis der Impact-Analyse muss ggfs. eine erneute Erstzertifizierung durchgeführt werden.

Bei Änderungen mit niedrigerem Risikowert (1, 2, 3 oder 4) sind Herstellererklärungen zu erstellen, in denen die Änderungen dargestellt und hinsichtlich ihrer Auswirkungen für die IT-Sicherheit nachvollziehbar dokumentiert werden.

3. Prüfschema für IT-Auditoren

Die Anforderungen an die IT in DPG-Rücknahmevorrichtungen geben einen Rahmen für Sicherheitsziele vor und bilden so die Grundlage für die IT-Prüfung. Die Umsetzung dieser Anforderungen wird im Rahmen der IT-Prüfung geprüft und bewertet, um die Sicherheitseigenschaften eines IT-Systems zu bestimmen. Durch die IT-Prüfung kann ferner eine Aussage darüber getroffen werden, inwieweit darauf vertraut werden kann, dass die Sicherheitseigenschaften dazu geeignet sind, Sicherheitsziele zu erfüllen, mit denen die Anforderungen an die IT umgesetzt werden sollen.

Die Prüftiefe zielt daher vor allem auf die Nachvollziehbarkeit der getroffenen Maßnahmen hinsichtlich der gestellten Anforderungen und der vom Hersteller durchgeführten Analysen, Prozesse und Tests in den Bereichen Entwicklung/Herstellung, Installation und Inbetriebnahme ab. Ferner sind alle Maßnahmen zu betrachten, die der Hersteller von DPG-Rücknahmevorrichtungen ergriffen hat, um einen sicheren Betrieb zu unterstützen, insbesondere zur Information der Betreiber der DPG-Rücknahmevorrichtungen. Um IT-Auditoren und Herstellern eine Orientierungshilfe bei der Prüfung bzw. Umsetzung der Anforderungen zu geben, werden zu jeder Anforderung einige Prüfmerkmale in Form von Maßnahmen oder Nachweisen genannt, die zu einer Umsetzung der Anforderung beitragen können.

Diese Anforderungen sind in den „Sicherheitstechnischen Anforderungen an die IT in DPG-Rücknahmevorrichtungen“ spezifiziert. Die Spezifikation richtet sich in ihrer Struktur am zugrunde gelegten Modell für Prozesse innerhalb einer DPG-Rücknahmevorrichtung und basiert auf einer ISO/IEC CD 13335-2 Risikoanalyse.

In diesem Kapitel werden alle Anforderungen an die IT aufgeführt, dabei wurden gleiche Anforderungen für unterschiedliche Teilaspekte des IT-Systems zusammengefasst. Jeder Abschnitt enthält eine Tabelle mit Beispielen für verallgemeinerte Begriffe. Eine tabellarische Gesamtübersicht über die Anforderungen findet sich in Teil 1 des Anhangs.

3.1 Anforderungen an DPG-Rücknahmevorrichtungen

3.1.1 Zugriffskontrolle

Der Zugriff auf Teile des IT-Systems soll grundsätzlich kontrolliert erfolgen, d.h. Operationen sollen von bestimmten Einheiten eines IT-Systems nur auf bestimmte Objekte durchgeführt werden können. Die diesbezüglichen nachfolgend geschilderten Anforderungen basieren auf dem Begriff „unbefugter Zugriff“, wobei der Begriff „befugter Zugriff“ definiert wurde als Zugriff, der zur Erfüllung einer Aufgabe unbedingt erforderlich ist. Die Anforderung wurde mehrfach gestellt und wie folgt zusammengefasst:

Anforderung 1

Es darf in den Instanzen kein unbefugter Zugriff auf die Objekte möglich sein.

Instanzen	Objekte
Prüfung Steuerung Prüfinstanz Generator Krypto Kommunikation	Objekte: - Artikelstammdaten - Programme - GTIN - EAN-Barcode - DPG-Markierung - Automatenstammdaten - Prozessdaten[1] - Zufallszahlengenerator - Privater Schlüssel - Rohdatensätze (mit signiertem und unsigniertem Teil) - Headerdatensatz

Tabelle 1: Beispiel für Instanzen und Objekte

Prüfmerkmale

Eine Zugriffskontrolle kann auf unterschiedliche Art und Weise implementiert werden. Die Prüfmerkmale müssen daher sprachlich so allgemein abgefasst werden, dass sie unabhängig von einer bestimmten Lösung anwendbar sind. Hierzu sind einige wenige Begriffsdefinitionen erforderlich:

Subjekt — Eine Einheit im Bereich des zu prüfenden IT-Systems, die im IT-System Operationen ausführen lassen kann. Beispiele für solche *Subjekte sind Programme, Benutzer, Dienste, Skripte*.

Objekt — Eine Einheit im Bereich des zu prüfenden IT-Systems, die Informationen enthält oder empfängt und auf der Subjekte Operationen ausführen

[1] Unsignierte Prozessdaten: Positionsnummer, Hersteller DPG-Rücknahmevorrichtung, Seriennummer DPG-Rücknahmevorrichtung, GTIN, Zeitstempel (Datum/Uhrzeit), Rücknahmestelle, ggf. Sacknummer.

lassen. Beispiele für *Objekte sind Dateien, Programme, Geräte oder Daten* (Artikelstammdaten, Rohdatensatz, Passwort, Signatur).

Zugriff — Eine Operation zwischen Subjekten und Objekten.

Sicherheitsattribute — Attribute, die bei der Spezifikation von Zugriffsregeln verwendet werden, zum Beispiel Benutzeridentität, Rolle, Tageszeit, Ort, ACL.

Mit Hilfe dieser Begriffe lassen sich folgende, allgemeine Merkmale einer Zugriffskontrolle abfragen:

- Werden in einer Sicherheitsrichtlinie alle Subjekte, Objekte, Operationen und Sicherheitsattribute der Zugriffskontrolle beschrieben?
- Werden in einer Sicherheitsrichtlinie Regeln festgelegt, welche Operationen zwischen Subjekten und Objekten zur Erfüllung einer Aufgabe zulässig sind?
- Werden alle Regeln einer Sicherheitsrichtlinie hinsichtlich ihrer Notwendigkeit nachvollziehbar begründet?
- Setzen die Sicherheitsfunktionen des IT-Systems die Sicherheitsrichtlinie für die Zugriffskontrolle für alle Subjekte, Objekte und Operationen durch, die der Zugriffskontrolle unterliegen?

3.1.2 Funktionsumfang

Einige Anforderungen sehen vor, dass nur die spezifizierten und durch die DPG freigegebenen Funktionen ausgeführt werden können und diesbezüglich eine geeignete Überprüfung durchzuführen ist. Diese Forderungen wurden für verschiedene Instanzen gestellt und wie folgt zusammengefasst:

Anforderung 2

Die Programme dürfen für bestimmte, von der DPG benannte Systemteile 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.

Instanzen	Objekte
Prüfung der Instanzen: - Prüfung - Steuerung - Prüfinstanz - Generator - Kommunikation	Programme

Tabelle 2: Beispiel für Instanzen und Objekte

Prüfmerkmale

Liegt eine funktionale Spezifikation vor, die für die relevanten Systemteile den Vorgaben der DPG entspricht?

Liegen Testberichte für die relevanten Systemteile vor?

3.1.3 Erweiterter Schutz der Integrität von Objekten

Daten im IT-System sind vor unautorisierten und unbeabsichtigten Veränderungen zu schützen. Zudem müssen Veränderungen erkannt werden und eine entsprechende Reaktion im IT-System auslösen.

Die Integrität bestimmter Daten und Signale wird in fast allen Kapiteln der Anforderungen an die IT gefordert. Die Mechanismen zur Sicherung der Integrität bilden somit eine wichtige Kompo-

nente der IT-Sicherheit. Die in den Anforderungen verwendeten Formulierungen unterscheiden sich dabei durch den adressierten Teil der IT sowie die zu schützenden Objekte und werden wie folgt zusammengefasst:

Anforderung 3

Die Objekte der Instanzen (s. Tabelle 3) müssen gegen Manipulation geschützt werden. Veränderungen an den Objekten müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen.

Instanzen	Objekte
Prüfung Steuerung Prüfinstanz Generator Krypto Kommunikation Sensor-Prüfung Kompaktor-Steuerung Prüfungs-Generator Generator-Krypto Krypto-Kommunikation	Objekte: - Programme - Relavante Daten für die Sicherung der Integrität von Objekten - Kompaktorsignal - GTIN - EAN-Barcode - Prozessdaten - Rohdatensatz (mit signiertem und unsigniertem Teil)

Tabelle 3: Beispiel für Instanzen und Objekte

Prüfmerkmale

Wie sind Integritätsfehler im IT-System definiert?

Anhand welcher Attribute der zu schützenden Objekte werden Integritätsfehler überwacht?

Überwachen die Sicherheitsfunktionen des IT-Systems alle Objekte auf definierte Integritätsfehler anhand der definierten Objektattribute?

Sind Aktionen festgelegt, die bei Erkennen eines Integritätsfehlers ausgelöst werden sollen?

Lösen die Sicherheitsfunktionen bei jedem Integritätsfehler die festgelegten Aktionen aus?

3.1.4 Störmodus bei negativem Kompaktorsignal

Das Kompaktorsignal informiert darüber, ob die Zerstörung der DPG-Verpackung erfolgreich war und stellt somit die Grundlage für die Erstellung eines Rohdatensatzes und damit einer Forderung dar. Es ist daher unbedingt erforderlich, dass eine DPG-Rücknahmevorrichtung bei negativem Signal vom Kompaktor den Betrieb einstellt.

Anforderung 4

Die Programme zur Verarbeitung des Signals vom Kompaktor müssen derart arbeiten, dass die DPG-Rücknahmevorrichtung bei einem negativen Signal in den Störmodus übergeht.

Prüfmerkmale

Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen ein negatives Signal vom Kompaktor erzeugt wird?

Deckt die Testdokumentation alle Umstände ab, unter denen ein negatives Signal vom Kompaktor erzeugt wird?

3.1.5 Positives Kompaktorsignal als Voraussetzung für die Übermittlung der GTIN

Die GTIN darf ausschließlich dann an den Generator übergeben werden, wenn aufgrund eines positiven Kompaktorsignals von einer erfolgreichen Kompaktierung der DPG-Verpackung ausgegangen werden kann.

Anforderung 5

Die GTIN darf nur bei positivem Signal des Kompaktors (= erfolgreiche Kompaktierung der DPG-Verpackung) an den Generator übergeben werden.

Prüfmerkmal

Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen ein positives Signal vom Kompaktor erzeugt wird?

Deckt die Testdokumentation alle Umstände ab, unter denen ein positives Signal vom Kompaktor erzeugt wird?

3.1.6 Kontrollierter Versand gültiger Objekte

Das IT-System muss für bestimmte Systemteile einen kontrollierten Versand von gültigen Objekten im IT-System ermöglichen bzw. im Umkehrschluss den willkürlichen Versand gültiger Objekte im IT-System verhindern.

Anforderung 6

Es darf nicht möglich sein, willkürlich gültige Objekte von einer Instanz an eine andere Instanz zu versenden.

Instanzen	Objekte
Prüfinstanz Generator	Objekte: - GTIN - Prozessdaten

Tabelle 4: Beispiel für Instanzen und Objekte

Prüfmerkmale

Welche Voraussetzungen müssen für den Versand gültiger Objekte innerhalb des IT-Systems erfüllt sein?

Welche Funktionen werden vom IT-System bereitgestellt, um diese Voraussetzungen zu kontrollieren?

Welcher Kontrolle unterliegen die Funktionen?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für den Versand gültiger Objekte innerhalb des IT-Systems durchzusetzen?

3.1.7 Korrekte Zeitstempel

Eine korrekte Zeitangabe ist insbesondere für die Erzeugung von Rohdatensätzen und die Protokollierung von Ereignissen erforderlich. Der Zeitstempel muss daher aus einer zuverlässigen Quelle stammen und darf nicht durch äußere Einflüsse oder unbefugte Zugriffe verändert werden können.

Anforderung 7

Die Erzeugung des Zeitstempels und der Zeitstempel selbst darf nicht manipulierbar sein.

Prüfmerkmale

Stellen die Sicherheitsfunktionen des IT-Systems einen verlässlichen Zeitstempel zur Verfügung?

Werden Änderungen der Zeiteinstellung protokolliert?

Wird das Bereitstellen von Zeitstempeln protokolliert?

3.1.8 Kontrolliertes Einspielen von Objekten

Zur in Kapitel 3.1.6 dargestellten Forderung nach einem kontrollierten Versand von Objekten bildet die kontrollierte Annahme von Objekten das Gegenstück. Einige bestimmte Systemteile müssen in der Lage sein, vor der Annahme von Objekten eine Autorisierung für das Einspielen vorzunehmen.

Anforderung 8

Das unautorisierte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.

Instanzen	Objekte
Generator Krypto Kommunikation	Objekte: - GTIN - Prozessdaten - Rohdatensätze (mit signiertem und unsigniertem Teil)

Tabelle 5: Beispiel für Instanzen und Objekte

Prüfmerkmale

Welche Eigenschaften müssen vorliegen, damit über die Zulässigkeit des Einspielens entschieden werden kann?

Welche Einheit im System muss diese Eigenschaften aufweisen?

Unter welchen Bedingungen wird das Einspielen eines Objekts in eine Instanz akzeptiert und unter welchen Bedingungen wird es verweigert?

Werden festgelegte Kontrollen für das Einspielen von Objekten in Instanzen von den Sicherheitsfunktionen des IT-Systems durchgesetzt?

3.1.9 Erkennen von Wiedereinspielung

Das IT-System muss in der Lage sein, die wiederholte Verwendung identifizierter Objekte zu erkennen und geeignete Maßnahmen zu treffen.

Anforderung 9

Das wiederholte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.

Instanzen	Objekte
Generator Krypto Kommunikation	Objekte: - GTIN - Prozessdaten - Rohdatensatz (mit signiertem und unsigniertem Teil)

Tabelle 6: Beispiel für Instanzen und Objekte

Prüfmerkmale

Wie werden Objekte markiert, die zum ersten Mal eingespielt werden? Wie werden Objekte identifiziert, die nicht zum ersten Mal eingespielt werden?

Welche Aktionen stehen für den Fall einer erkannten Wiedereinspielung zur Verfügung?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die Vorgaben zur Identifikation von wieder eingespielten Objekten durchzuführen?

Lösen die Sicherheitsfunktionen des IT-Systems bei Erkennung von Wiedereinspielung die vorgegebenen Aktionen aus?

3.1.10 Verwendung anerkannter Zufallszahlengeneratoren

Zur Verhinderung von Angriffen auf den privaten Schlüssel, ist ein geeigneter Zufallszahlengenerator zu verwenden. Die DPG orientiert sich hierbei an den Kriterien des BSI und setzt vom BSI anerkannte Zufallszahlengeneratoren voraus.

Anforderung 10

Es müssen Zufallszahlengeneratoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils mit SoM-hoch, verwendet werden.

Prüfmerkmal

Kann der Hersteller nachweisen, dass er Zufallszahlengeneratoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils SoM-hoch, einsetzt?

Wie wird sichergestellt, dass dieser Zufallszahlengenerator in korrekter Weise und unverändert implementiert wird?

3.1.11 Autorisierter Versand gültiger Objekte an Forderungssteller

Das IT-System muss für bestimmte Systemteile eine Autorisierung des Versands von gültigen Objekten ermöglichen.

Anforderung 11

Das unautorisierte Aussenden von Objekten an den Rücknehmer/Forderungssteller muss erkannt und verhindert werden.

Instanzen	Objekte
Kommunikation	Rohdatensätze (mit signiertem und unsigniertem Teil)

Tabelle 7: Beispiel für Instanzen und Objekte

Prüfmerkmale

Welche Merkmale werden für die Autorisierung zum Versand gültiger Objekte an Rücknehmer/Forderungssteller verwendet?

Sind Richtlinien für den Versand gültiger Objekte an Rücknehmer/Forderungssteller definiert, in denen autorisiertes und unautorisiertes Versenden spezifiziert wird?

Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen?

Welcher Kontrolle unterliegen die Funktionen?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Richtlinien für den Versand gültiger Objekte an Rücknehmer/Forderungssteller bzw. Forderungstellerdienstleister umzusetzen?

3.1.12 DPG-Automaten: Positive Rückmeldung des Kompaktors bei erfolgreicher Kompaktierung

Die Generierung von Rohdatensätzen darf ausschließlich nach erfolgreicher Zerstörung der DPG-Verpackung erfolgen. Ausgangspunkt hierfür ist die positive Rückmeldung des Kompaktors, welche somit nur bei erfolgreicher Kompaktierung erfolgen darf.

Anforderung 12

Eine positive Rückmeldung des Kompaktors darf nur bei einer erfolgreichen Kompaktierung erfolgen.

Prüfmerkmale

Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen eine positive Rückmeldung vom Kompaktor erzeugt wird?

Deckt die Testdokumentation alle Umstände ab, unter denen eine positive Rückmeldung vom Kompaktor erzeugt wird?

Anwendungshinweis

Die DPG hat die folgende Umsetzung skizziert und betrachtet diese als Äquivalent zu einer positiven Rückmeldung des Kompaktors, die ausschließlich im Fall einer erfolgreichen Kompaktierung erfolgt:

Ein Sensor muss die Eingabe einer DPG-Verpackung feststellen können. Ein zweiter Sensor ist unmittelbar vor dem Kompaktor angebracht, so dass die DPG-Verpackung nach Passieren des Sensors nicht entfernt werden kann, ohne diesen Sensor ein weiteres Mal auszulösen. Der Kompaktor muss mit einem Sensor versehen sein, der die erfolgreiche Inbetriebnahme des Kompaktors bestätigt. Falls alle drei Sensoren den Weg der DPG-Verpackung nachvollziehbar signalisieren und der zweite Sensor nicht vor dem Kompaktor ein weiteres Mal ausgelöst wurde, besteht hinreichend Anlass zu der Annahme, dass die DPG-Verpackung zerstört wurde. Die Hersteller von DPG-rücknahmevorrichtungen sind nicht dazu verpflichtet, dies in genau der beschriebenen Art und Weise umzusetzen, da jede Lösung akzeptiert wird, die nachvollziehbar äquivalent zur beschriebenen Lösung ist und die in geeigneter Weise dokumentiert ist.

3.1.13 Absenderüberprüfung des Generators für GTIN

Im Rahmen der internen Kommunikation des IT-Systems ist sicherzustellen, dass ausschließlich die Prüfinstanz GTIN zur Erzeugung von Prozessdaten an den Generator sendet.

Anforderung 13

Der Generator darf nur GTIN weiter verarbeiten, die zweifelsfrei aus der Prüfinstanz stammen.

Prüfmerkmale

Welche Merkmale werden für die Identifikation des Absenders verwendet?

Existieren Vorgaben für die Überprüfung des Absenders von GTIN, in denen positive und negative Prüfergebnisse spezifiziert werden?

Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen?

Welcher Kontrolle unterliegen die Funktionen?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von GTIN umzusetzen?

3.1.14 Absenderüberprüfung der Kryptoinstanz für unsignierte Prozessdaten

Im Rahmen der internen Kommunikation des IT-Systems ist sicherzustellen, dass bis zur Verarbeitung des Rohdatensatzes eine Überprüfung des Absenders der erhaltenen Daten durchgeführt wird.

Anforderung 14

Die Kryptoinstanz darf nur Prozessdaten weiter verarbeiten, die zweifelsfrei aus dem Generator stammen.

Prüfmerkmale

Welche Merkmale werden für die Identifikation des Absenders verwendet?

Existieren Vorgaben für die Überprüfung des Absenders von Prozessdaten, in denen positive und negative Prüfergebnisse spezifiziert werden?

Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen?

Welcher Kontrolle unterliegen die Funktionen?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von Prozessdaten umzusetzen?

3.1.15 Absenderüberprüfung der Kommunikation für Rohdatensätze

Im Rahmen der internen Kommunikation des IT-Systems ist sicherzustellen, dass bis zur Verarbeitung des Rohdatensatzes eine Überprüfung des Absenders der erhaltenen Daten durchgeführt wird. Anforderung und Prüfmerkmale gestalten sich dementsprechend analog zu den Kapiteln 3.1.1 und 3.1.2.

Anforderung 15

Die Kommunikation darf nur Rohdatensätze (mit signiertem und unsigniertem Teil) weiter verarbeiten, die zweifelsfrei aus der Kryptoinstanz stammen.

Prüfmerkmale

Welche Merkmale werden für die Identifikation des Absenders verwendet?

Existieren Vorgaben für die Überprüfung des Absenders von Rohdatensätzen, in denen positive und negative Prüfergebnisse spezifiziert werden?

Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen?

Welcher Kontrolle unterliegen die Funktionen?

Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von Rohdatensätzen umzusetzen?

3.1.16 Generierung von Protokollen

Ein Bestandteil der Kontrolle des ordnungsgemäßen Zustandes eines IT-Systems ist das Führen und regelmäßige Kontrollieren von Protokollen für sicherheitsrelevante Ereignisse. Protokolle können dazu beitragen, Verstöße gegen Sicherheitsrichtlinien zu entdecken und aufzuklären.

Anforderung 16

Innerhalb der DPG-Rücknahmevorrichtung sind alle sicherheitsrelevanten Daten zu protokollieren und zu speichern, die notwendig sind, um sicherheitsrelevante Zwischenfälle zu entdecken und aufzuklären.

Prüfmerkmale

Liegt eine Definition aller sicherheitsrelevanten Zwischenfälle vor, die beschreibt, was bei Eintritt des jeweiligen Zwischenfalls zu protokollieren ist?

Sind Protokollierungsgrade definiert (z.B. minimal, detailliert)?

Sind die Sicherheitsfunktionen in der Lage, für folgende Ereignisse eine Protokollaufzeichnung zu generieren:

- Starten und Beenden der Protokollierungsfunktion,
- Alle protokollierbaren Ereignisse für den gewählten Protokollierungsgrad,

- Datum und Uhrzeit eines Ereignisse,
- Art des Ereignisses,
- Identität des Ereignisses.

Können die Sicherheitsfunktionen darüber hinaus weitere Ereignisse protokollieren? Falls ja, wie sind diese festgelegt?

Sind die Sicherheitsfunktionen in der Lage, jedes protokollierbare Ereignis mit der Identität desjenigen Benutzers oder derjenigen Einheit im IT-System zu verknüpfen, der bzw. die dieses Ereignis verursacht hat?

3.2 Anforderungen an die Einsatzumgebung

3.2.1 Sicherheit in der Entwicklung, der Installation und im Anlauf des Systems

Nicht alle Anforderungen an die IT lassen sich durch die IT selbst lösen. Hierzu gehört die Forderung nach Sicherheit während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und des Einsatzes der DPG-Rücknahmevorrichtungen zur Rücknahme von DPG-Verpackungen. Die Anforderung betrifft somit nicht mehr Instanzen, sondern Bereiche der Herstellung und Auslieferung. Einen besonderen Aspekt nimmt hier die Zugriffskontrolle ein, durch die Manipulationen an Teilen des Systems in den genannten Phasen verhindert werden sollen. Analog zu 0 wurde auch hierbei der Begriff „unbefugter Zugriff“ verwendet.

Anforderung 17

Kein unbefugter Zugriff auf Objekte während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und des Einsatzes der DPG-Rücknahmevorrichtung zur Rücknahme von DPG-Verpackungen möglich.

Instanzen	Objekte
Entwicklung Installation Anlauf	Programme Datenbank (für Stammdaten) Zufallszahlengenerator

Tabelle 8: Beispiel für Bereiche und Objekte

Prüfmerkmale

Liegt eine Dokumentation zur Sicherheit bei der Entwicklung vor, in der alle

- materiellen
- organisatorischen
- personellen und
- weiteren Sicherheitsmaßnahmen beschrieben wurden,

die zum Schutz der Vertraulichkeit und Integrität des IT-Systems in der Entwicklung, der Installation und dem Anlauf erforderlich sind?

Ist dokumentiert, dass diese Sicherheitsmaßnahmen während der Entwicklung, der Installation und dem Anlauf befolgt wurden?

Begründet die Dokumentation, inwiefern die Sicherheitsmaßnahmen den erforderlichen Schutz zu Erhaltung der Vertraulichkeit und Integrität des IT-Systems gewährleisten?

Mit welchen Maßnahmen wird der sichere Einsatz von DPG-Rücknahmevorrichtungen zur Rücknahme von DPG-Verpackungen vom Hersteller DPG-Rücknahmevorrichtungen unterstützt?

Liegt eine Dokumentation vor, die den Endanwender in die Lage versetzt, das System sicher zu betreiben?

3.2.2 Kryptographische Algorithmen

Die Verwendung kryptographischer Algorithmen basiert auf nicht bewiesener, absoluter Sicherheit. Es ist daher erforderlich, die Entwicklungen im Bereich kryptographischer Algorithmen fortlaufend zu verfolgen um zu erkennen, wann die eingesetzten Algorithmen in ihrer Anwendung verstärkt oder die Algorithmen in Abstimmung mit der DPG ausgetauscht werden müssen.

Anforderung 18

Es sind nach den Signaturvorgaben der DPG kryptographisch korrekte Algorithmen, deren Implementierungen sowie die zugehörigen Parametersätze einzusetzen.

Prüfmerkmale

Entsprechen die eingesetzten kryptographischen Algorithmen den Signaturvorgaben der DPG?

Wie wird sichergestellt, dass der Zufallszahlengenerator in korrekter Weise, unverändert entsprechend implementiert wird?

Entsprechen die in Verbindung mit den kryptographischen Algorithmen eingesetzten Parameter den Signaturvorgaben der DPG?

3.2.3 Vertrauenswürdige und getestete Krypto- und Signaturkomponenten

Die Komponenten für den Einsatz des privaten Schlüssels sowie zu Bildung der Schlüssel müssen vertrauenswürdig und gestestet sein.

Anforderung 19

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

Prüfmerkmale

Ist für alle Komponenten, die mit dem privaten Schlüssel arbeiten oder bei der Bildung des Schlüssels eingesetzt werden, nachvollziehbar, auf welcher Grundlage diesen Komponenten vertraut wird (insbesondere bei nicht selbst produzierten Komponenten)?

Wurden für alle Komponenten aus der vorangegangenen Frage dokumentierte Tests durchgeführt, so dass deren Resistenz gegenüber Bedrohungen gem. den „Sicherheitstechnischen Anforderungen an die IT in DPG-Rücknahmevorrichtungen“ Kap. 2.6.3.1 nachvollziehbar ist?

3.2.4 Kenntnis über die Entwicklungen im Bereich eingesetzter kryptographischer Verfahren

Voraussetzung für das Kapitel 3.2.2 ist das fortlaufende Verfolgen der Entwicklungen im Bereich kryptographischer Algorithmen, um zu erkennen, wann die eingesetzten Algorithmen in ihrer Anwendung verstärkt oder die Algorithmen ausgetauscht werden müssen.

Anforderung 20

Ständige Beobachtung des aktuellen Standes der IT-Technik von kryptographischen Verfahren.

Prüfmerkmal

Wer ist für die Beobachtung des aktuellen Technikstandes für kryptographische Verfahren verantwortlich?

Wieviel Zeit wird in welchem Zeitraum für die Beobachtung des aktuellen Technikstandes aufgewendet?

3.2.5 Ersatz für verwendete kryptographische Verfahren

Für den Fall, dass sich aufgrund neuer Erkenntnisse die eingesetzten kryptographischen Verfahren als unsicher erweisen, müssen diese in möglichst kurzer Zeit ersetzt werden, um den Zeitraum für Attacken gegen das dann unsichere Verfahren möglichst klein zu halten.

Anforderung 21

Eingesetzte kryptographische Verfahren müssen in kurzer Zeit ersetzt werden, wenn sie gebrochen wurden.

Prüfmerkmale

Ist ein Verfahren zum Austausch kryptographischer Verfahren geplant und dokumentiert?

Wie schnell können eingesetzte kryptographische Verfahren ausgetauscht werden?

Sind im Fall eines Austauschs kryptographischer Verfahren neue Verfahren zu implementieren und installieren?

Ist im Fall eines Austauschs eines kryptographischen Verfahrens ein Ersatzverfahren implementiert und installiert?

3.2.6 Ersatz für verwendete kryptographischer Verfahren

Für den Fall, dass sich aufgrund neuer Erkenntnisse die eingesetzten Parametersätze für kryptographischen Verfahren als unzureichend herausstellen, müssen diese in möglichst kurzer Zeit angepasst werden, um den Zeitraum für Attacken gegen das dann unsichere Verfahren möglichst klein zu halten.

Anforderung 22

Eingesetzte kryptographische Verfahren müssen in angemessener Zeit nach den Signaturvorgaben der DPG angepasst werden.

Prüfmerkmale

Ist ein Verfahren zur Aktualisierung der Parametersätze verwendeter kryptographischer Verfahren geplant und dokumentiert?

Wie schnell können die Parametersätze eingesetzter kryptographische Verfahren aktualisiert werden?

4. Literatur

[Anforderungen] DPG Deutsche Pfandsystem GmbH, „Sicherheitstechnische Anforderungen an die IT in DPG-Rücknahmevorrichtungen“ in der jew. aktuellen Version.

[Signaturvorgaben] Martin Bartosch, Cynops GmbH, Signaturvorgaben im Rahmen des Pfandsystems der Deutschen Pfandsystem GmbH in der aktuellen Version.

[ZertISO27001] Bundesamt für Sicherheit in der Informationstechnik, Zulassung nach ISO 27001 auf der Basis von IT-Grundschutz, Prüfschema für ISO 27001-Audits, 01.02.2006

[BSI 7125] Bundesamt für Sicherheit in der Informationstechnik, BSI-Zulassung Verfahrensbeschreibung, Januar 1998

Anhang, Teil 1:

Übersicht über die Anforderungen an die IT in DPG-Rücknahmevorrichtungen (Anforderungsliste)

In der nachfolgenden Tabelle werden alle Anforderungen gemäß [Kapitel 3] aufgeführt, dabei wurden gleiche Anforderungen für unterschiedliche Teilaspekte des IT-Systems zusammengefasst.

Lfd. Nr.	Anforderung	Betroffene Instanzen Übertragungswege	Betroffene Elemente	Kapitel
1	In den Instanzen und auf den Übertragungswegen muss die Integrität der Objekte sichergestellt sein.	Prüfung Steuerung Prüfinstanz Generator Kommunikation Sensor-Prüfung Kompaktor-Steuerung Prüfung-Generator Generator-Krypto Krypto-Kommunikation	Objekte: – Artikelstammdaten – Signal des Kompaktors – GTIN – EAN-Barcode – DPG-Markierung – Automatenstammdaten – Prozessdaten – Rohdatensätze (mit signiertem und unsigniertem Teil) – Flag der DPG-Markierung – Kompaktorsignal	2.1.2 2.3.2 2.4.2 2.5.2 2.7.2 3.1.2 3.4.2 3.6.2 3.7.2 3.8.2 3.9.2
2	Es darf in den Instanzen kein unbefugter Zugriff auf die Objekte möglich sein.	Prüfung Steuerung Prüfinstanz Generator Krypto Kommunikation	Objekte: – Artikelstammdaten – Programme – GTIN – DPG-Markierung – Automatenstammdaten – Prozessdaten – Zufallszahlengenerator – Privater Schlüssel – Rohdatensätze (mit signiertem und unsigniertem Teil) – Headerdatensatz	2.1.2 2.3.2 2.4.2 2.5.2 2.6.3.1 2.7.2
3	Kein unbefugter Zugriff auf Objekte während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und des Einsatzes der DPG-Rücknahmevorrichtung zur Rücknahme von DPG-Verpackungen.	Entwicklung, Installation, Anlauf	Objekte: – Programme – Stammdatenbank – Zufallszahlengenerator	2.1.2 2.3.2 2.4.2 2.5.2 2.6.3.1 2.6.3.2 2.7.2
4	Die Programme dürfen für bestimmte, von der DPG benannte Systemteile 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.	Entwicklung der Instanzen: Prüfung Steuerung Prüfinstanz Generator Kommunikation	Programme	2.1.2 2.3.2 2.4.2 2.5.2 2.7.2
5	Die Objekte der Instanzen müssen gegen Manipula-	Prüfung Steuerung	Objekte: – Programme,	2.1.2 2.3.2

Lfd. Nr.	Anforderung	Betroffene Instanzen Übertragungswege	Betroffene Elemente	Kapitel
	tion geschützt werden. Veränderungen an den Objekten müssen erkannt werden. Entsprechende Reaktionen auf Integritäts-verletzungen müssen erfolgen.	Prüfinstanz Generator Kompaktor-Steuerung Prüfung-Generator Krypto-Kommunikation	– relevante Daten für die Sicherung der Integrität von Objekten – Kompaktorsignal – GTIN – Prozessdaten – Rohdatensatz (mit signiertem und unsigniertem Teil)	2.4.2 2.5.2 3.4.2 3.6.2 3.7.2 3.8.2 3.9.2
6	Die Programme zur Verarbeitung des Signals vom Kompaktor müssen derart arbeiten, dass der Automat bei einem negativen Signal in den Störmodus übergeht.	Steuerung		2.3.2
7	Der GTIN darf nur bei positivem Signal des Kompaktors (= erfolgreiche Kompaktierung der DPG-Verpackung) an den Generator übergeben werden.	Prüfinstanz		2.4.2 2.5.2
8	Es darf nicht möglich sein, willkürlich gültige Objekte von einer Instanz an eine andere Instanz zu versenden.	Prüfinstanz Generator	Objekte: – GTIN – Prozessdaten	2.4.2 2.5.2
9	Die Erzeugung des Zeitstempels und der Zeitstempel selbst dürfen nicht manipulierbar sein.	Generator		2.5.2
10	Das unautorisierte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.	Generator Krypto Kommunikation	Objekte: – GTIN – Prozessdaten – Rohdatensätze (mit signiertem und unsigniertem Teil)	2.5.2 3.6.2 3.7.2 3.8.2 3.9.2
11	Das wiederholte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.	Generator Krypto Kommunikation	Objekte: – GTIN – Prozessdaten – Rohdatensatz (mit signiertem und unsigniertem Teil)	2.5.2 3.6.2 3.7.2 3.8.2 3.9.2
12	Es müssen Zufallszahlen-generatoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils SoM-hoch, verwendet werden.	Entwicklung		2.6.3.1
13	Einsatz von kryptographisch korrekten - Algorithmen, deren - Implementierungen sowie den - zugehörigen Parametersätzen.	Entwicklung		2.6.3.1

Lfd. Nr.	Anforderung	Betroffene Instanzen Übertragungswege	Betroffene Elemente	Kapitel
14	Für die Komponenten innerhalb des Automaten, welche den privaten Schlüssel oder Bestandteile davon oder Rohdaten zur Bildung der Schlüssel (wie z.B. Zufallszahlen) verwenden, sind Nachweise zu erbringen.	Entwicklung	Nachweise – Grundsätzliche Vertrauenswürdigkeit der Komponenten. – Resistenz der Komponenten gegenüber den Bedrohungen gem. [Anforderungen] Kap. 2.6.3.1.	2.6.3.1
15	Ständige Beobachtung des aktuellen Technikstandes eingesetzter kryptographischer Verfahren	Entwicklung	Kryptographische Verfahren – Signaturverfahren – Hash-Algorithmus	2.6.3.3
16	Eingesetzte Kryptographische Verfahren müssen in kurzer Zeit ersetzt werden, wenn sie gebrochen wurden.	Entwicklung Betrieb	Kryptographische Verfahren – Signaturverfahren – Hash-Algorithmus	2.6.3.3
17	Eingesetzte Kryptographische Verfahren müssen in angemessener Zeit nach den Signaturvorgaben der DPG angepasst werden.	Entwicklung Betrieb	Kryptographische Verfahren – Signaturverfahren – Hash-Algorithmus	2.6.3.3
18	Das unautorisierte Aussenden von Objekten an den Forderungssteller muss erkannt und verhindert werden.	Kommunikation	Rohdatensätzen (mit signiertem und unsigniertem Teil)	2.7.2
19	DPG-Automat: Eine positive Rückmeldung des Kompaktors darf nur bei einer erfolgreichen Kompaktierung erfolgen.	Kompaktor-Steuerung		2.4.2
20	Der Generator darf nur GTIN weiter verarbeiten, die zweifelsfrei aus der Prüfinstanz stammen.	Prüfinstanz-Generator	GTIN	3.6.2
21	Die Kryptoinstanz darf nur Prozessdaten weiter verarbeiten, die zweifelsfrei aus dem Generator stammen.	Generator-Krypto	Prozessdaten	3.7.2
22	Die Kommunikation darf nur Rohdatensätze (mit signiertem und unsigniertem Teil) weiter verarbeiten, die zweifelsfrei aus der Kryptoinstanz stammen.	Krypto-Kommunikation	Rohdatensätze	3.8.2
23	Innerhalb des Automaten sind alle sicherheitsrelevanten Daten zu protokollieren und zu speichern, die notwendig sind, um sicherheitsrelevante Zwischenfälle zu entdecken und aufzuklären.	Alle	Alle	4

Tabelle 9: Anforderungen an die IT in DPG-Rücknahmevorrichtungen

Anhang, Teil 2:
Prüfliste: IT-Anforderungen an DPG-Rücknahmevorrichtungen

Lfd. Nr.	Anforderung	Ort[2]	Risikowert (Instanz)	Prüfmerkmal	Votum
1	Es darf in den Instanzen kein unbefugter Zugriff auf die Objekte möglich sein.	P und O	4 (Prüfung) 5 (Steuerung) 7 (Prüfinstanz) 7 (Generator) 7 (Krypto) 1 (Kommunikation) 2 (Sensor-Prüfung) 5 (Kompaktor-Steuerung) 7 (Prüfung-Generator) 7 (Generator-Krypto) 8 (Krypto-Komm.)	Werden in einer Sicherheitsrichtlinie alle Subjekte, Objekte, Operationen und Sicherheitsattribute der Zugriffskontrolle beschrieben? Werden in einer Sicherheitsrichtlinie Regeln festgelegt, welche Operationen zwischen Subjekten und Objekten zur Erfüllung einer Aufgabe zulässig sind? Werden alle Regeln einer Sicherheitsrichtlinie hinsichtlich ihrer Notwendigkeit nachvollziehbar begründet? Setzen die Sicherheitsfunktionen des IT-Systems die Sicherheitsrichtlinie für die Zugriffskontrolle für alle Subjekte, Objekte und Operationen durch, die der Zugriffskontrolle unterliegen?	
2	Die Programme dürfen für bestimmte, von der DPG benannte Systemteile 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.	P	4 (Prüfung) 5 (Steuerung) 7 (Prüfinstanz) 8 (Krypto) 1 (Kommunikation)	Liegt eine funktionale Spezifikation vor, die für die relevanten Systemteile den Vorgaben der DPG entspricht? Liegen Testberichte für die relevanten Systemteile vor?	

[2] Nur relevant für die Zertifizierung von Zählzentren; hierzu auch ZertRL für Zählzentren (P = standortunabhängig, O = standortabhängig)

Lfd. Nr.	Anforderung	Ort[2]	Risikowert (Instanz)	Prüfmerkmal	Votum
3	Die Objekte der Instanzen müssen gegen Manipulation geschützt werden. Veränderungen an den Objekten müssen erkannt werden. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen.	P	4 (Prüfung) 5 (Steuerung) 7 (Prüfinstanz) 8 (Krypto) 7 (Generator) 1 (Kommunikation) 2 (Sensor-Prüfung) 5 (Kompaktor-Steuerung) 7 (Prüfung-Generator) 7 (Generator-Krypto) 8 (Krypto-Komm.)	Wie sind Integritätsfehler im IT-System definiert? Anhand welcher Attribute der zu schützenden Objekte werden Integritätsfehler überwacht? Überwachen die Sicherheitsfunktionen des IT-Systems alle Objekte auf definierte Integritätsfehler anhand der definierten Objektattribute? Sind Aktionen festgelegt, die bei Erkennen eines Integritätsfehlers ausgelöst werden sollen? Lösen die Sicherheitsfunktionen bei jedem Integritätsfehler die festgelegten Aktionen aus?	
4	Die Programme zur Verarbeitung des Signals vom Kompaktor müssen derart arbeiten, dass der Automat bei einem negativen Signal in den Störmodus übergeht.	O	5 (Steuerung)	Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen ein negatives Signal vom Kompaktor erzeugt wird? Deckt die Testdokumentation alle Umstände ab, unter denen ein negatives Signal vom Kompaktor erzeugt wird?	
5	Die GTIN darf nur bei positivem Signal des Kompaktors (= erfolgreiche Kompaktierung der DPG-Verpackung) an den Generator übergeben werden.	O	7 (Prüfinstanz)	Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen ein positives Signal vom Kompaktor erzeugt wird? Deckt die Testdokumentation alle Umstände ab, unter denen ein positives Signal vom Kompaktor erzeugt wird?	

Lfd. Nr.	Anforderung	Ort[2]	Risikowert (Instanz)	Prüfmerkmal	Votum
6	Es darf nicht möglich sein, willkürlich gültige Objekte von einer Instanz an eine andere Instanz zu versenden.	P	7 (Prüfinstanz) 7 (Generator)	Welche Voraussetzungen müssen für den Versand gültiger Objekte innerhalb des IT-Systems erfüllt sein? Welche Funktionen werden vom IT-System bereitgestellt, um diese Voraussetzungen zu kontrollieren? Welcher Kontrolle unterliegen die Funktionen? Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für den Versand gültiger Objekte innerhalb des IT-Systems durchzusetzen?	
7	Die Erzeugung des Zeitstempels und der Zeitstempel selbst dürfen nicht manipulierbar sein.	P und O	7 (Generator)	Stellen die Sicherheitsfunktionen des IT-Systems einen verlässlichen Zeitstempel zur Verfügung? Werden Änderungen der Zeiteinstellung protokolliert? Wird das Bereitstellen von Zeitstempeln protokolliert?	
8	Das unautorisierte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.	P	7 (Generator) 7 (Generator-Krypto) 8 (Krypto-Komm.)	Welche Eigenschaften müssen vorliegen, damit über die Zulässigkeit des Einspielens entschieden werden kann? Welche Einheit im System muss diese Eigenschaften aufweisen? Unter welchen Bedingungen wird das Einspielen eines Objekts in eine Instanz akzeptiert und unter welchen Bedingungen wird es verweigert? Werden festgelegte Kontrollen für das Einspielen von Objekten in Instanzen von den Sicherheitsfunktionen des IT-Systems durchgesetzt?	
9	Das wiederholte Einspielen von Objekten in Instanzen muss erkannt und verhindert werden.	P	7 (Generator) 7 (Generator-Krypto) 1 (Kommunikation)	Wie werden Objekte markiert, die zum ersten Mal eingespielt werden? Wie werden Objekte identifiziert, die nicht zum ersten Mal eingespielt werden? Welche Aktionen stehen für den Fall einer erkannten Wiedereinspielung zur Verfügung?	

Lfd. Nr.	Anforderung	Ort[2]	Risikowert (Instanz)	Prüfmerkmal	Votum
				Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die Vorgaben zur Identifikation von wieder eingespielten Objekten durchzuführen? Lösen die Sicherheitsfunktionen des IT-Systems bei Erkennung von Wiedereinspielung die vorgegebenen Aktionen aus?	
10	Es müssen Zufallszahlengeneratoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils SoM-hoch, verwendet werden.	P	8 (Krypto)	Kann der Hersteller nachweisen, dass Zufallszahlengeneratoren nach BSI AIS 20, K3 (deterministisch), bzw. AIS 31, P2 (phys. Zufall), jeweils SoM-hoch, eingsetzt werden? Wie wird sichergestellt, dass der Zufallszahlengenerator korrekt und unverändert implementiert wird?	
11	Das unautorisierte Aussenden von Objekten an den Forderungssteller muss erkannt und verhindert werden.	P und O	1 (Kommunikation)	Welche Merkmale werden für die Autorisierung zum Versand gültiger Objekte an Forderungssteller verwendet? Sind Richtlinien für den Versand gültiger Objekte an Forderungssteller definiert, in denen autorisiertes und unautorisiertes Versenden spezifiziert wird? Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen? Welcher Kontrolle unterliegen die Funktionen? Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Richtlinien für den Versand gültiger Objekte an Forderungssteller umzusetzen?	
12	DPG-Automat: Eine positive Rückmeldung des Kompaktors darf nur bei einer erfolgreichen Kompaktierung erfolgen.	O	5 (Kompaktor-Steuerung)	Kann anhand der Dokumentation nachvollzogen werden, unter welchen Umständen eine positive Rückmeldung vom Kompaktor erzeugt wird? Deckt die Testdokumentation alle Umstände ab, unter denen eine positive Rückmeldung vom Kompaktor erzeugt wird?	

Lfd. Nr.	Anforderung	Ort	Risikowert (Instanz)	Prüfmerkmal	Votum
13	Der Generator darf nur GTIN weiter verarbeiten, die zweifelsfrei aus der Prüfinstanz stammen.	P	7 (Prüfung-Generator)	Welche Merkmale werden für die Identifikation des Absenders verwendet?	
				Existieren Vorgaben für die Überprüfung des Absenders von GTIN, in denen positive und negative Prüfergebnisse spezifiziert werden? Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen? Welcher Kontrolle unterliegen die Funktionen? Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von GTIN umzusetzen?	
14	Die Kryptoinstanz darf nur Prozessdaten weiter verarbeiten, die zweifelsfrei aus dem Generator stammen.	P	7 (Generator-Krypto)	Welche Merkmale werden für die Identifikation des Absenders verwendet? Existieren Vorgaben für die Überprüfung des Absenders von Prozessdaten, in denen positive und negative Prüfergebnisse spezifiziert werden? Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen? Welcher Kontrolle unterliegen die Funktionen? Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von Prozessdaten umzusetzen?	

Lfd. Nr.	Anforderung	Ort	Risikowert (Instanz)	Prüfmerkmal	Votum
15	Die Kommunikation darf nur Rohdatensätze (mit signiertem und unsigniertem Teil) weiter verarbeiten, die zweifelsfrei aus der Kryptoinstanz stammen.	P	8 (Krypto-Komm.)	Welche Merkmale werden für die Identifikation des Absenders verwendet? Existieren Vorgaben für die Überprüfung des Absenders von Rohdatensätzen, in denen positive und negative Prüfergebnisse spezifiziert werden? Welche Funktionen werden vom IT-System bereitgestellt, um diese Merkmale zu prüfen?	
				Welcher Kontrolle unterliegen die Funktionen?	
				Sind die Sicherheitsfunktionen des IT-Systems in der Lage, die dokumentierten Vorgaben für die Identifikation des Absenders von Rohdatensätzen umzusetzen?	
16	Innerhalb der DPG-Rücknahmevorrichtung sind alle sicherheitsrelevanten Daten zu protokollieren und zu speichern, die notwendig sind, um sicherheitsrelevante Zwischenfälle zu entdecken und aufzuklären.	P und O	ohne eigenen Risikowert	Liegt eine Definition aller sicherheitsrelevanten Zwischenfälle vor, die beschreibt, was bei Eintritt des jeweiligen Zwischenfalls zu protokollieren ist? Sind Protokollierungsgrade definiert (z.B. minimal, detailliert)? Sind die Sicherheitsfunktionen in der Lage, für folgende Ereignisse eine Protokollaufzeichnung zu generieren: --- Starten und Beenden der Protokollierungsfunktion --- Alle protokollierbaren Ereignisse für den gewählten Protokollierungsgrad --- Datum und Uhrzeit eines Ereignisse --- Art des Ereignisses --- Identität des Ereignisses	

				Können die Sicherheitsfunktionen darüber hinaus weitere Ereignisse protokollieren? Falls ja, wie sind diese festgelegt? Sind die Sicherheitsfunktionen in der Lage, jedes protokollierbare Ereignis mit der Identität desjenigen Benutzers oder derjenigen Einheit im IT-System zu verknüpfen, der bzw. die dieses Ereignis verursacht hat?	
17	Kein unbefugter Zugriff auf Objekte während der Entwicklung, der Einspielung in die DPG-Rücknahmevorrichtung und deren Einsatz zur Rücknahme von DPG-Verpackungen.	P und O	4 (Prüfung) 5 (Steuerung) 7 (Prüfinstanz) 7 (Generator) 8 (Krypto) 1 (Kommunikation)	Liegt eine Dokumentation zur Sicherheit bei der Entwicklung vor, in der alle --- materiellen --- organisatorischen --- personellen und --- weiteren Sicherheitsmaßnahmen beschrieben wurden,	
				die zum Schutz der Vertraulichkeit und Integrität des IT-Systems in der Entwicklung, der Installation und dem Anlauf erforderlich sind? Ist dokumentiert, dass diese Sicherheitsmaßnahmen während der Entwicklung, der Installation und dem Anlauf befolgt wurden? Begründet die Dokumentation, inwiefern die Sicherheitsmaßnahmen den erforderlichen Schutz zur Erhaltung der Vertraulichkeit und Integrität des IT-Systems gewährleisten? Mit welchen Maßnahmen wird der sichere Einsatz der DPG-Rücknahmevorrichtung zur Rücknahme von DPG-Verpackungen von ihrem Hersteller unterstützt? Liegt eine Dokumentation vor, die den Endanwender in die Lage versetzt, das System sicher zu betreiben?	

Lfd. Nr.	Anforderung	Ort	Risikowert (Instanz)	Prüfmerkmal	Votum
18	Einsatz von nach den Signaturvorgaben der DPG kryptographisch korrekten Algorithmen, deren Implementierungen sowie den zugehörigen Parmetersätzen.	P	8 (Krypto-Signatur) 1 (Krypto-Hash)	Entsprechen die eingesetzten kryptographischen Algorithmen den Signaturvorgaben der DPG? (DPG-Vorgabe: bis einschließlich 31.05.2022 RSA 1024 (SHA1), ECDSA 192 (SHA1); seit 01.01.2012 ECDSA 224 (SHA224) und 256 (SHA256) möglich; für vom 01.06.2012 an mit neuer Seriennummer in der Stammdatenbank hinterlegten DPG-Rücknahmevorrichtungen ist ECDSA 256 (SHA256) verpflichtend.) Wie wird sichergestellt, dass der Zufallszahlengenerator in korrekter Weise, unverändert und nach den Signaturvorgaben der DPG entsprechend implementiert wird? Entsprechen die in Verbindung mit den kryptographischen Algorithmen eingesetzten Parameter den Signaturvorgaben der DPG?	
19	Für die Komponenten innerhalb des Automaten, welche den privaten Schlüssel oder Bestandteile davon oder Rohdaten zur Bildung der Schlüssel (wie z.B. Zufallszahlen) verwenden, sind Nachweise bezüglich deren Vertrauenswürdigkeit zu erbringen.	P und O	8 (Krypto)	Ist für alle Komponenten, die mit dem privaten Schlüssel arbeiten oder bei der Bildung des Schlüssels eingesetzt werden, nachvollziehbar, auf welcher Grundlage diesen Komponenten vertraut wird (insbesondere bei nicht selbst produzierten Komponenten)? Wurden für alle Komponenten aus der vorangegangenen Frage dokumentierte Tests durchgeführt, so dass deren Resistenz gegenüber Bedrohungen gem. [Anforderungen] Kap. 2.6.3.1 nachvollziehbar ist?	
20	Ständige Beobachtung des aktuellen Technikstandes eingesetzter kryptographischer Verfahren	P	8 (Krypto)	Wer ist für die Beobachtung des aktuellen Technikstandes für kryptographische Verfahren verantwortlich? Wieviel Zeit wird in welchem Zeitraum für die Beobachtung des aktuellen Technikstandes aufgewendet?	

Lfd. Nr.	Anforderung	Ort	Risikowert (Instanz)	Prüfmerkmal	Votum
21	Eingesetzte kryptographische Verfahren müssen in kurzer Zeit ersetzt werden, wenn sie gebrochen wurden.	P	8 (Krypto)	Ist ein Verfahren zum Austausch kryptographischer Verfahren zum Ersatz kryptographischer Verfahren geplant und dokumentiert? Wie schnell können eingesetzte kryptographische Verfahren ausgetauscht werden? Sind im Fall eines Austauschs kryptographischer Verfahren neue Verfahren zu implementieren und installieren? Ist im Fall eines Austauschs eines kryptographischen Verfahrens ein Ersatzverfahren implementiert und installiert?	
22	Eingesetzte kryptographische Verfahren müssen in angemessener Zeit den Signaturvorgaben der DPG angepasst werden.	P	8 (Krypto)	Ist ein Verfahren zur Aktualisierung der Parametersätze verwendeter kryptographischer Verfahren geplant und dokumentiert? Wie schnell können die Parametersätze eingesetzter kryptographische Verfahren aktualisiert werden?	

Tabelle 1: Übersicht über die Prüfmerkmale an die IT in DPG-Rücknahmevorrichtungen

Anhang, Teil 3:
Signaturvorgaben im DPG-System

Regelungen zur Einführung der Signaturverfahren ECDSA 224 (SHA224) und ECDSA 256 (SHA256)

Innerhalb des DPG-Systems gelten für die Erzeugung von Rohdatensätzen folgende, auf Empfehlungen des BSI basierende Signaturverfahren:

- RSA 1024 (SHA1) (bis einschl. 31.05.2022)
- ECDSA 192 (SHA1) (bis einschl. 31.05.2022)
- ECDSA 224 (SHA224) (vom 01.01.2012 an)
- ECDSA 256 (SHA256) (vom 01.01.2012 an)

Bei der Verwendung der zugelassenen Signaturverfahren gelten folgende Regelungen:

- Seit dem 01.12.2011 dürfen Hersteller von DPG-Rücknahmevorrichtungen Automatenstammdaten für neue DPG-Rücknahmevorrichtungen3 in der Stammdatenbank mit dem Signaturverfahren ECDSA 256 (SHA 256) hinterlegen. Eine Inbetriebnahme / Referenzierung von DPG-Rücknahmevorrichtungen mit dem Signaturverfahren ECDSA 256 (SHA 256) ist seit 01.01.2012 zugelassen.
- Seit 01.01.2012 können bereits in der Stammdatenbank mit dem Signaturverfahren ECDSA 192 (SHA1) oder RSA 1024 eingetragene DPG-Rücknahmevorrichtungen auf den Betrieb mit dem Signaturverfahren ECDSA 256 (SHA 256) oder ECDSA 224 (SHA 224) umgestellt werden.
- Seit 01.06.2012 ist für die erstmalige Referenzierung einer DPG-Rücknahmevorrichtung in der Stammdatenbank das Signaturverfahren ECDSA 256 (SHA 256) verpflichtend.
- Vom 01.06.2022 an müssen alle DPG-Rücknahmevorrichtungen auf den Betrieb mit ECDSA 256 (SHA 256) oder ECDSA 224 (SHA 224) umgestellt sein.
- Alle sowohl vom Rücknehmer referenzierten als auch vom Hersteller DPG-Rücknahmevorrichtungen in der Stammdatenbank hinterlegten, noch nicht referenzierten DPG-Rücknahmevorrichtungen, die mit Ablauf des 31.05.2022 noch mit dem Signaturverfahren RSA 1024 bzw. ECDSA 192 (SHA1) in der Stammdatenbank hinterlegt sind, werden mit Gültig ab Datum 01.06.2022 automatisch durch die DPG gesperrt.
- Wenn Umstände eintreten, aufgrund derer ein im DPG-System eingesetztes Signaturverfahren bzw. ein dabei verwendeter Algorithmus von der DPG als nicht mehr sicher bewertet wird, erfordert der Betrieb des DPG-Systems eine von den vorgenannten Fristen abweichende Änderung des Signaturverfahrens. Wenn der Beirat der DPG einer solchen Änderung nach sorgfältiger Prüfung ihrer Auswirkung auf das DPG-System zugestimmt hat, müssen alle im Markt befindlichen DPG-Rücknahmevorrichtungen mit diesen Signaturverfahren auf ein höherwertiges Signaturverfahren umgerüstet werden. In einem solchen Fall gilt für die Vertragsänderung und das Verfahren dieser Änderung Ziffer 9.6 der Teilnahmebedingungen bzw. XI.5 der Zulassungsvereinbarung mit Herstellern von DPG-Automaten, Großzählautomaten und Zählzentren bzw. Ziffer IX.5 der Zulassungsvereinbarung mit Zählzentrumbetreibern.

[3] Eine neue DPG-Rücknahmevorrichtung weist eine Seriennummer auf, die vom Hersteller der DPG-Rücknahmevorrichtung noch nicht in der DPG-Stammdatenbank hinterlegt ist.

Konsequenzen für die IT-Zertifizierung

Bei Wiederholungszertifizierungen für DPG-Rücknahmevorrichtungen, die mit ECDSA 192 (SHA1) bzw. RSA 1024 betrieben werden, ist zu beachten, dass diese Signaturverfahren vom 01.06.2022 an nicht mehr im DPG-System zugelassen sind.

Die Signaturvorgaben können bei der DPG angefordert werden.