

Umsetzung der
Kassensicherungsverordnung –
Entwürfe des Bundesamtes für Sicherheit in
der Informationstechnik (BSI) zu den
Technischen Richtlinien;
Mündliche Anhörung

BERICHT ZUR VERANSTALTUNG VOM 27.3.2018 IM BMF, BERLIN



Michael Trmac

Multi Data Wedemann Vertriebs-GmbH · Oldenburg

MULTI DATA[®]

Das BMF lädt ein

Gespräche im Rahmen des „Kassengesetzes“

26. Mai 2016

Fachgespräch zum Schutz vor
Manipulation an digitalen
Grundaufzeichnungen

Verbände und Hersteller in
getrennten Veranstaltungen

16. Dezember 2016
§ „Kassengesetz“

7. September 2017

Fachgespräch KassenSichV
Technische Richtlinie und
Schutzprofile

Hersteller und Vertreter der
Landesfinanzbehörden

23. Februar 2018
Entwurf TR-03153
TR-03151

27. März 2018

Mündliche Anhörung

Umsetzung der
Kassensicherungsverordnung –
Entwürfe des Bundesamtes für
Sicherheit in der
Informationstechnik (BSI) zu den
Technischen Richtlinien

Hersteller und Verbände

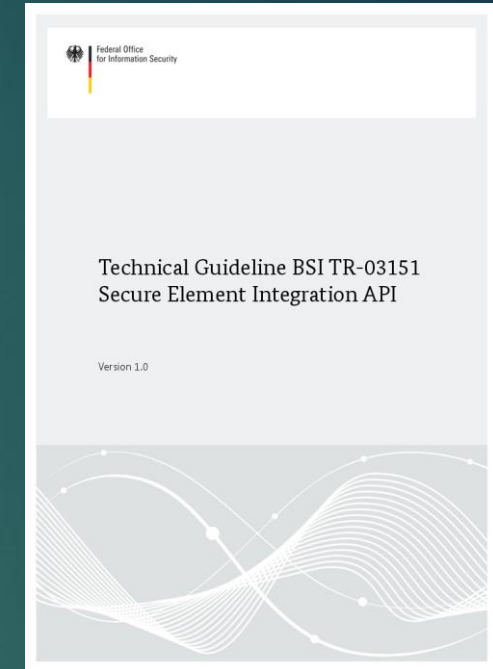
Schriftliche Anhörung

Im Vorfeld der mündlichen Anhörung, wurden einigen Herstellern und Verbänden am 26. Februar 2018 die Entwürfe der Technischen Richtlinien TR-3151 und TR-3153, sowie eine Übersicht der im Schutzprofil betrachteten Bedrohungen zur Stellungnahme zugeschickt.



BSI TR-03153

- Konkrete Vorgaben für die Technische Sicherheitseinrichtung
- Basiert auf BSI TR-03151



BSI TR-03151

- Allgemeine API zur Kapselung der Funktionalität eines Secure Elements
- Unabhängig von der konkreten Umsetzung

Erste Reaktionen

Nach der Veröffentlichung der Technischen Richtlinien konnte man die ersten Reaktionen aus dem Markt folgendermaßen kurz zusammenfassen

- ▶ in großen Teilen ungenau
- ▶ komplex
- ▶ praxisfern
- ▶ in der Realisierung zu teuer
- ▶ aufwändig zu kontrollieren

Mündliche Anhörung 27. März 2018

Die Teilnehmer (im Überblick, ohne
Anspruch auf Vollständigkeit)

- ▶ BMF: Fr. Fillinger, Fr. Dannewitz
- ▶ BSI: Herr Dr. Kügler, Herr Frank
- ▶ TÜV-IT
- ▶ Anbieter und Hersteller von (Kassen-) Soft- und Hardware
- ▶ Verbände

Gesamtzahl der Teilnehmer: Ca. 40 Personen

Ablauf der Anhörung

- ▶ 1. Powerpointpräsentation des BSI
 - ▶ Grundlegende Informationen
 - ▶ Gesetzliche Grundlagen, Aufgaben des BSI, Sicherheitsziele, Aufbau und Funktionsweise der TSE, Kryptografische Vorgaben, Ablauf der Zertifizierung
 - ▶ Fragen und Anmerkungen dazu
- ▶ 2. Powerpointpräsentation des BSI
 - ▶ Zusammenfassung häufiger Fragen und Kommentare mit entsprechenden Anmerkungen



Das Wichtigste im Überblick

- ▶ Die Technische Richtlinie befasst sich nur mit sicherheitsrelevanten Daten.
- ▶ Steuerfachliche Aspekte werden lt. BMF über einen Anwendungserlass geregelt.
- ▶ In diesem Zusammenhang wurde aus der Runde gefragt, was alles unter dem Grundbegriff „Andere Vorgänge“ zu verstehen ist.



“ ...und ich sage Ihnen eines:
Jeder Tastendruck wird in
Zukunft protokolliert werden ”

AUS DER ANTWORT VON FRAU DANNEWITZ (BMF) AUF DIE FRAGE, WAS MIT „ANDEREN VORGÄNGEN“ GEMEINT SEI.

Die Uhr im Sicherheitsmodul

- ▶ muss keine Echtzeituhr sein. Ein „regelmäßiger Abgleich“ mit der Kasse (z.B. beim Einschalten) ist ausreichend
- ▶ im Prinzip soll die Uhr im Sicherheitsmodul einfach nur die Zeit nach oben zählen können, wenn Sie mit Strom versorgt und gestellt ist
- ▶ ein Setzen der Uhrzeit im Sicherheitsmodul erfordert Administratorrechte
- ▶ jedes Stellen der Uhrzeit soll von der TSE geloggt werden

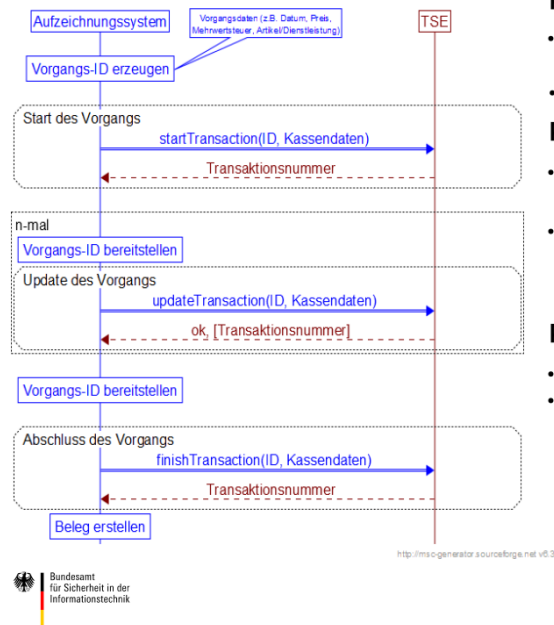
Eine Uhr wird lt. BSI bei sogenannten „Javacards“ im kommenden Javastandard 3.1 unterstützt. Wann dieser Standard voraussichtlich verfügbar sein wird, blieb offen.

Das Zentrale Thema Vorgang

Praxisbezogene Nachfragen zu länger andauernden und / oder geräteübergreifenden Vorgängen konnten nicht konkret beantwortet werden.

Anwendungsfälle oder Ablaufbeispiele lagen nicht vor.

Ablauf der Protokollierung



Phase 1: Beginn der Transaktion (StartTransaction):

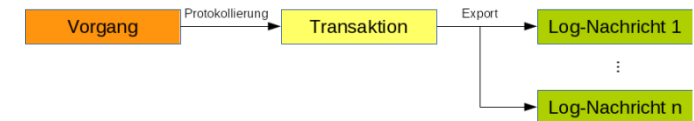
- Unmittelbar mit Beginn eines Vorgangs startet das Aufzeichnungssystem eine Transaktion in der TSE
- Die TSE erzeugt eine Log-Nachricht und speichert die abgesicherten Daten.

Phase 2: Aktualisierung der Transaktion (UpdateTransaction)

- Bei Aktualisierung des Vorgangs sendet das Aufzeichnungssystem die aktualisierten Daten an die TSE.
- Die TSE (TSE entscheidet)
 - übernimmt die Daten für einen späteren Absicherungsschritt oder
 - erzeugt eine Log-Nachricht und speichert die abgesicherten Daten.

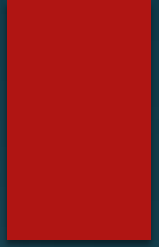
Phase 3: Beendigung der Transaktion (FinishTransaction)

- Mit Abschluss des Vorgangs beendet das Aufzeichnungssystem die Transaktion in der TSE
- Die TSE erzeugt eine Log-Nachricht und speichert die abgesicherten Daten



Einige weitere Antworten

- ▶ Auf die Anmerkung aus der Runde, dass eine auf der TR basierenden Lösung sicherlich nicht für die ursprünglich angepeilten 10,- € verfügbar sein wird, antwortete das BMF, dass ihm keine Erkenntnisse vorlägen, dass es teurer werden könnte.
- ▶ Eine rein softwarebasierende Sicherheitseinrichtung ist laut BSI höchstwahrscheinlich nicht zertifizierungsfähig.
- ▶ Die TR wird voraussichtlich jährlich aktualisiert. Dabei werden auch Prognosen über die zu benötigten Schlüssellängen gegeben, die dann für neue TSEs gelten sollen. Die Gültigkeitsdauer für die Zertifikate wird mit 5 Jahren angegeben.
- ▶ Das INSIKA-Verfahren wird explizit eingeschlossen, die notwendigen Änderungen vorausgesetzt.



- ▶ Die Schutzprofile werden verteilt, wenn deren Evaluierung abgeschlossen ist. Die Vergabe dieser Überprüfung wird vom Beschaffungsamt geregelt. Einen genauen Termin für die Fertigstellung liegt noch nicht vor, eventuell ist ein Vorabverteilung denkbar. Mit inhaltlichen Änderungen ist aber im Rahmen des Evaluierungsverfahrens zu rechnen.
- ▶ Hinsichtlich des Zeitplans geht das BSI davon aus, dass es einige termingerechte Implementierungen geben wird.

Aus der Praxis...

Die praxisbezogenen Fragen aus der Runde lassen Rückschlüsse auf die großen Unsicherheiten zu, die sich im Rahmen der Einführung der Sicherheitseinrichtung ergeben.

Praktisch keine der Fragen konnte abschließend beantwortet werden.

- ▶ Wie ist das Verfahren bei Nichtverfügbarkeit der TSE?
- ▶ Wie soll das Meldeverfahren bei Verbundsystemen aussehen?
- ▶ Wie ist die Handhabung der Seriennummern?

Die häufigsten Fragen der schriftlichen Anhörung

- ▶ **Dokumentationen (Zusammenhänge, Verfügbarkeiten)**
- ▶ **Gestaltung des Belegs**
 - ▶ Der Beleg ist nicht Bestandteil der Technischen Richtlinie (TR)
- ▶ **unklare Begriffsdefinitionen**
 - ▶ werden überarbeitet und geschärft
- ▶ **Taxonomie / Datenformat der Kassendaten**
 - ▶ Die TR bezieht sich ausschließlich auf die Sicherungsebene
 - ▶ Das Datenformat der Vorgangsdaten ist im Wesentlichen unabhängig vom Sicherungsformat
- ▶ **Speicher TSE / Datenexport** (Externe Aufbewahrung; Wann darf gelöscht werden)
 - ▶ Entweder Speicherung in der TSE und Export über einheitliche Datenschnittstelle (EDS) oder externe Speicherung (Datenträger, Cloud...) im einheitlichen Datenformat (EDS) für die Kassennachschau
- ▶ **Seriennummer, Fehlerhandling, Signaturvalidierung**

Die letzte Folie der Anhörung

Ein Beispiel...

Wohin mit Zahlungsart?

Kommentare zur Zahlungsart:

- Es kann mehrere Zahlungsarten geben?
- Grund für explizite Hervorhebung?

Auflösung:

- Zu klären...

Wichtige Aussagen

- ▶ An vielen Stellen wurde vom BSI immer wieder auf die Technologieoffenheit der Technischen Richtlinie hingewiesen. Eine detaillierte(re) Regelung sei ganz bewusst nicht vorgenommen worden.
- ▶ Es wird keine Referenzapplikation geben, mit der die Hersteller ggf. Ihre Anwendungen überprüfen könnten.

Alles klar?

- ▶ Einige Teilnehmer der Runde machten in ihren abschließenden Bemerkungen deutlich, dass die Anhörung mehr Fragen aufgeworfen als beantwortet hätte.

Stellungnahme des DFKA e.V.

Der DFKA e.V. reagierte schriftlich am 3. April 2018 mit einem Email an Herrn Dr. Misera.

Deutscher Fachverband für Kassen- und Abrechnungssystemtechnik



Bundesministerium der Finanzen
Unterabteilung IV A
Dr. Hans-Ulrich Misera
11016 Berlin

Berlin, 03.04.2018

Nur per E-Mail an: Hans-Ulrich.Misera@bmf.bund.de

Umsetzung der Kassensicherungsverordnung – Entwürfe des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu den Technischen Richtlinien; Mündliche Anhörung am 27.03.2018

Sehr geehrter Herr Dr. Misera,

seit dem Inkrafttreten des Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen hat der DFKA e.V. in verschiedenen Schreiben und Meldungen wiederholt auf zu erwartende Probleme bei der Umsetzung hingewiesen, vor allem auf solche, die sich erheblich auf Zeitplan und Kosten auswirken werden.¹

Da für die Umrüstung der Bestandssysteme mindestens ein Jahr benötigt wird und die Integration der Sicherheitseinrichtung durch die Anbieter etwa ein halbes Jahr erfordert, müsste das Konzept des BSI innerhalb von drei Monate soweit in die Praxis umgesetzt worden sein, dass lauffähige Sicherheitseinrichtungen zur Verfügung stehen.² Die Zertifizierung müsste zum Beginn der Umrüstungsphase (also in neun Monaten) abgeschlossen sein. Beides ist vollkommen unrealistisch, Verzögerungen sind also unausweichlich.

Während der im Betreff genannten Anhörung wurde allerdings offensichtlich, dass die Verzögerungen ganz erheblich ausfallen werden – es sich also nicht um Monate, sondern um Jahre handeln wird – oder das Projekt sogar insgesamt scheitern wird.

Unsere diesbezüglichen Befürchtungen wurden bestätigt und teilweise noch übertroffen. Hierzu lediglich einige Beispiele:

¹ Z.B. <http://dfka.net/bewertung-des-gesetzes-zum-schutz-vor-manipulationen-an-digitalen-grundaufzeichnungen/>, <http://dfka.net/umsetzung-der-kassensicherungsverordnung-die-zeit-wird-knapp/> und Schreiben an PStS Dr. Michael Meister vom 18.01.2018

² Für eine Implementierung und Praxistests muss eine Zertifizierung noch nicht vorliegen. In diesem Fall muss allerdings ausgeschlossen sein, dass im Rahmen des Zertifizierungsverfahrens noch nennenswerte technische Veränderungen vorgenommen werden.

Deutscher Fachverband für Kassen- und Abrechnungssystemtechnik im Lagerfeld und Bergfeld (den) Zahlungsverkehr e.V.
Friedrichstraße 10-12, 10117 Berlin

Tel.: +49(0)30 42096620
Fax: +49(0)30 42096621
Homepage: www.dfka.de
Email: info@dfka.de

Vorsitz:
Rüdiger F. Hesel
Udo Stanislaus

Amtesgasse Berlin-Corvettenburg
Registernummer: VR203008
St.Nr.: 271033XG282
Ums-ID: DE28145844

VR Bank Altenburger Land eG
BANK: BIC: 3305 3000 0000 7710 01
BIC: GENODE33SLR

Die Stellungnahme in der Zusammenfassung

- ▶ Hinweis auf zu erwartende Probleme bei der Umsetzung hinsichtlich Zeitplan und Kosten
- ▶ Lauffähige, zertifizierte Sicherheitseinrichtungen in der zur Verfügung stehenden Zeit zu bekommen ist unrealistisch
 - ▶ Die Annahme wird durch Beispiele aus der Anhörung untermauert
- ▶ Das Konzept wird als „praxisfern, komplex, lückenhaft und unausgereift“ bezeichnet.
- ▶ Die Struktur des Projektes selber weist -nach Auffassung des DFKA e.V.- eine Vielzahl an Risikofaktoren auf, die in der Summe zum vollständigen Scheitern führen könnten.
- ▶ **Das BMF wird aufgefordert, alternative Wege zu prüfen.**



Vielen Dank für Ihre
Aufmerksamkeit!