swissbit®

Vorschlag für Hersteller-unabhängiges Prüfschema der TSE-Einsatzumgebung

Store. Secure. Trust.

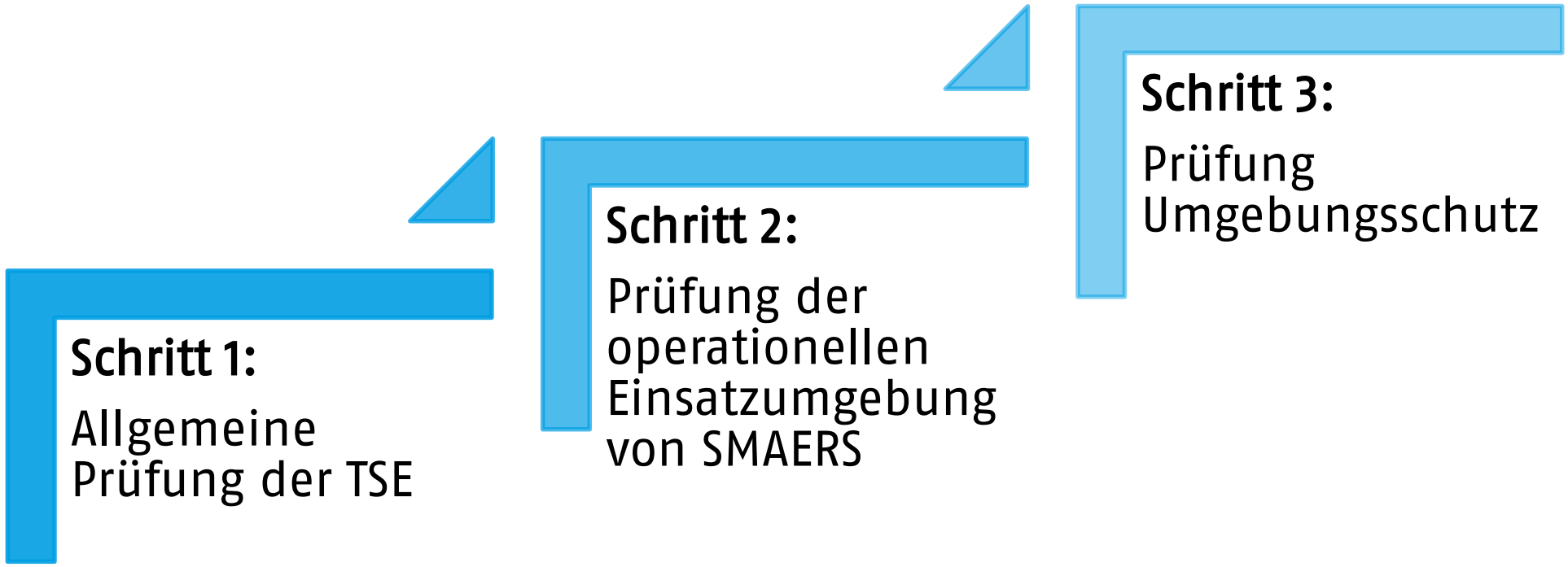
Scope

Die Prüfung der Einsatzumgebung der TSE erfordert technisches Verständnis und Kenntnis vieler Spezifikationen, insbesondere BSI SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0.

Aufgrund der Nachfrage aus dem Bundesfinanzministerium, die unserer Kenntnis nach auch an andere TSE Hersteller versandt wurde, mit der Fragestellung wie die Einsatzumgebung von TSEs geprüft werden können, ist folgendes Konzept entstanden, das wir als Vorschlag zur Verfügung stellen.

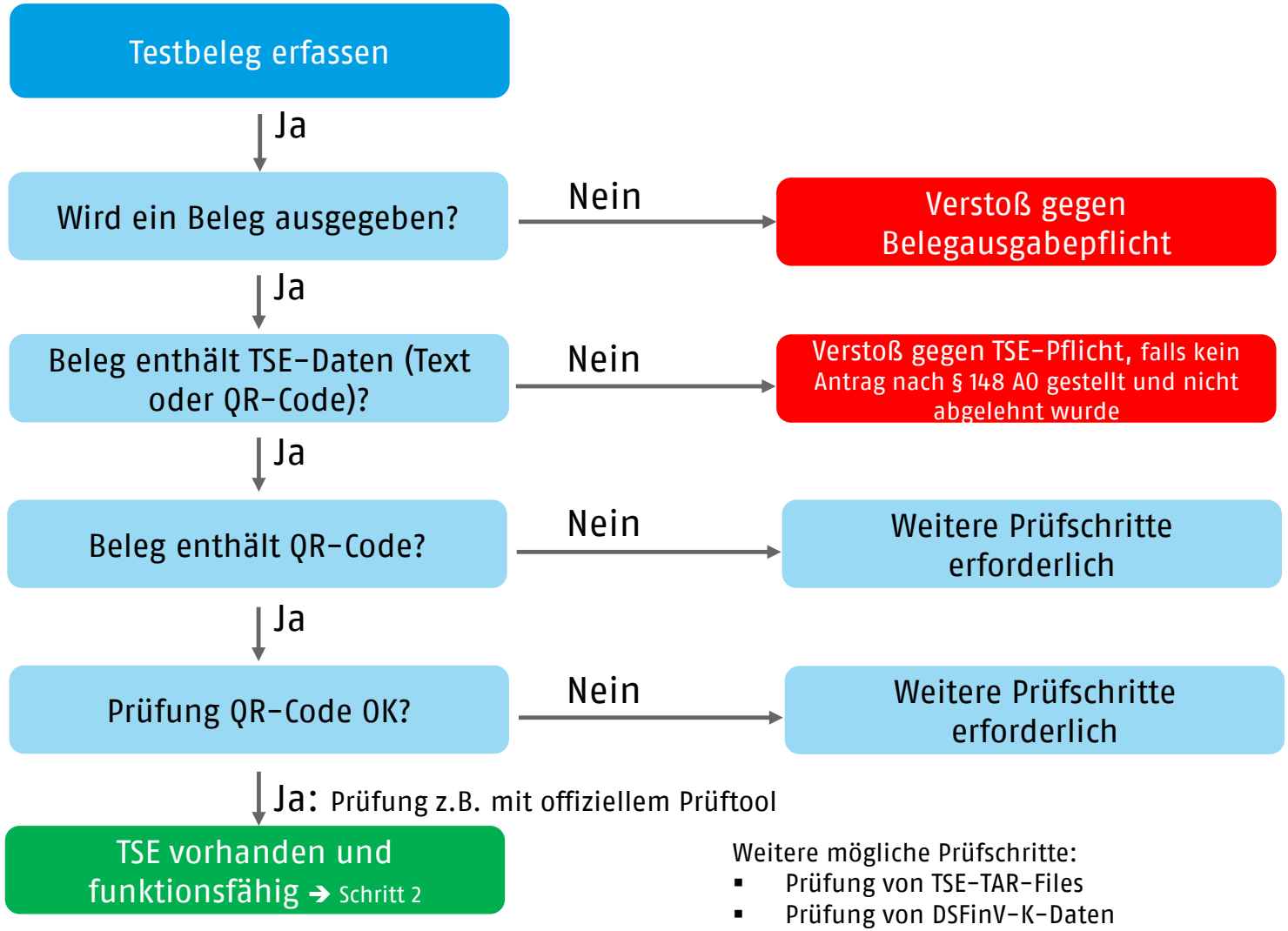
Es handelt sich dabei um einen Vorschlag und keinesfalls um eine amtliche oder bindende Verfahrensweise, sondern kann dem technisch versierten und autorisierten Prüfer oder während des Entwicklungsprozesses einem Kassenhersteller als Handreichung dienen.

Prüfung der TSE-Einsatzumgebung in drei einfachen Schritten.



Schritte 1 und 2: Prüfung der TSE allgemein und operationelle Einsatzumgebung

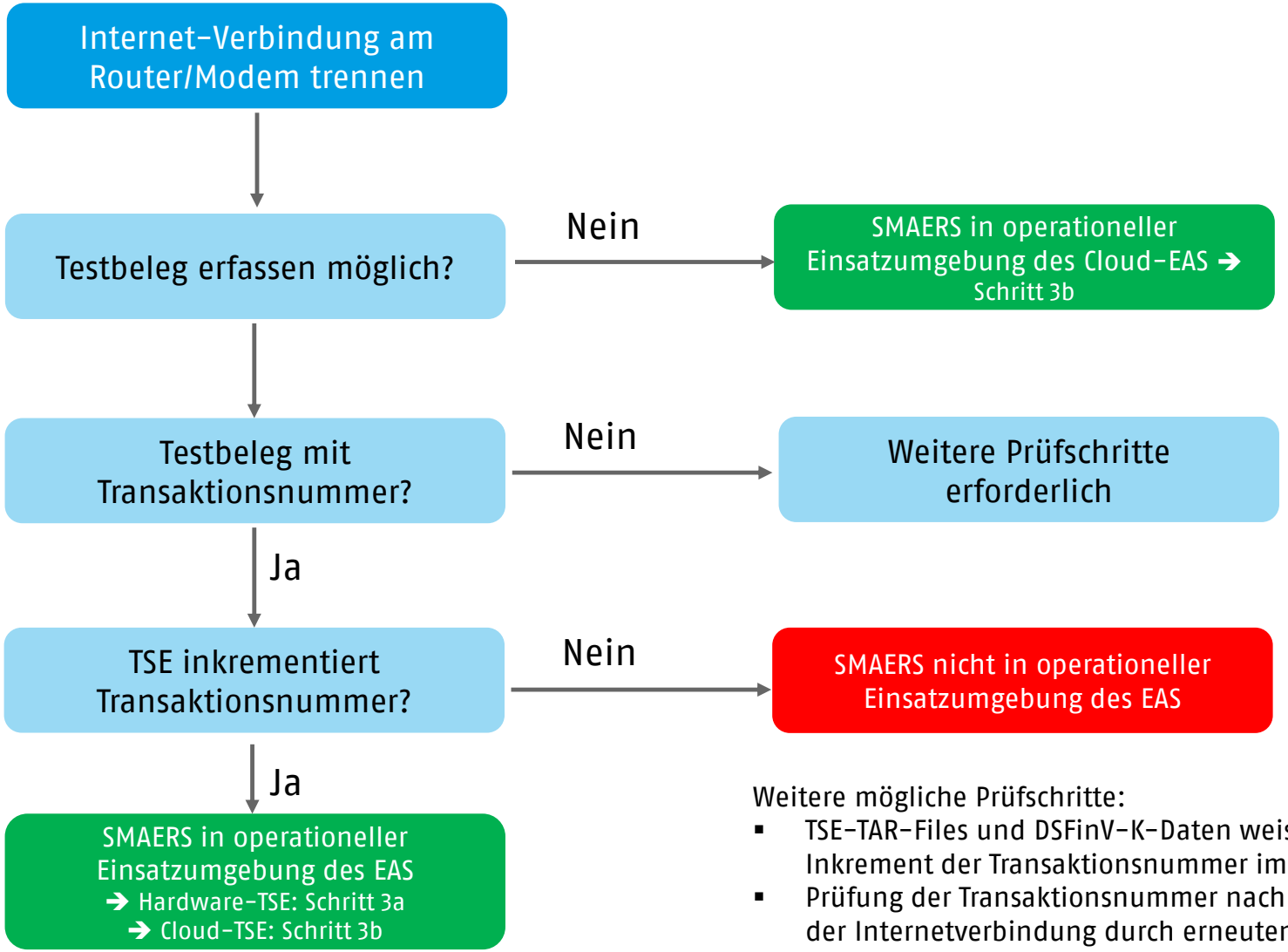
Schritt 1: Prüfung TSE allgemein



Weitere mögliche Prüfschritte:

- Prüfung von TSE-TAR-Files
- Prüfung von DSFinV-K-Daten
- Prüfung von Verträgen und weiteren Unterlagen zur TSE-Integration

Schritt 2: Prüfung, ob SMAERS in operationeller Einsatzumgebung des EAS betrieben wird



Weitere mögliche Prüfschritte:

- TSE-TAR-Files und DSFinV-K-Daten weisen Inkrement der Transaktionsnummer im Offline-Fall aus?
- Prüfung der Transaktionsnummer nach Wiederherstellung der Internetverbindung durch erneuten Testbeleg

swissbit®

Schritt 3: Prüfung Umgebungsschutz der Architekturen gemäß BSI-Schutzprofil

Definition: Aufzeichnungssystem (EAS bzw. ERS) vs. Eingabegerät

swissbit®

Aufzeichnungssystem

Funktion:

- Autarke Vergabe der Rechnungsnummer
- Verarbeitung und (Zwischen-) Speicherung von Transaktionsdaten
- Berechnung der MwSt.
- Erstellung eines legalen Beleges (z.B. Bestellung, Rechnung und Lieferschein) inkl. der Parameter (Ausweisung der MwSt., Steuernummern, Name und Anschrift des Gewerbetreibenden)

Eingabegerät

Funktion:

- Dateneingabe
- Datenanzeige
- Funktioniert nur mit Verbindung zum Host

Auszug aus FAQ des BMF:

Mobile Endgeräte sind dahingehend zu unterscheiden, ob sie selbst ein (Teil eines) Aufzeichnungssystem(s) sind, oder als Eingabegerät zu qualifizieren sind.

Kann das Gerät offline, ohne Anbindung an eine andere zentrale, die Aufzeichnungen führende Kasse betrieben werden, handelt es sich um ein selbständiges Aufzeichnungssystem und ist selbst unmittelbar an eine TSE anzubinden.

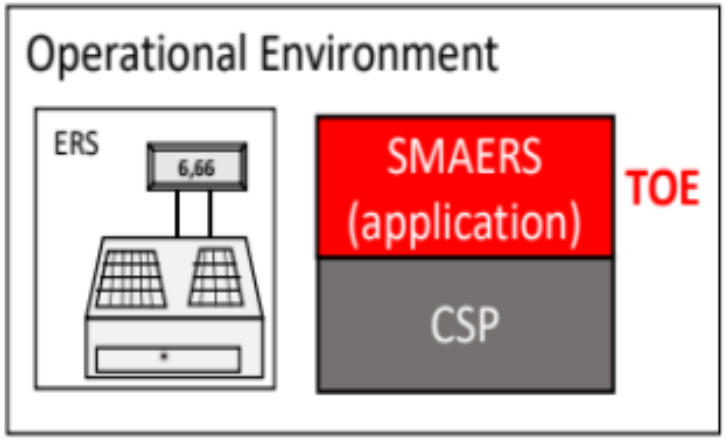
Gehen die Funktionen des Geräts hingegen nicht über die Funktionen z.B. einer Tastatur hinaus, handelt es sich um ein Eingabegerät. In diesem Fall werden die erfassten Daten unmittelbar nach Erfassung an ein mit einer TSE verbundenes Aufzeichnungssystem übergeben.

Schritt 3 a): Lokales Aufzeichnungssystem mit lokaler TSE

Prüfschritte Umgebungsschutz bei Hardware TSE

Lokales Aufzeichnungssystem

- Betriebssystem unter Wartung*?
- Schutz vor Schad-Software vorhanden?



Quelle: SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0, S. 17

* Wird für das Betriebssystem vom Hersteller noch Support gewährleistet?

Schritt 3 b): Cloud-TSEs mit lokalem EAS oder Cloud EAS

swissbit®

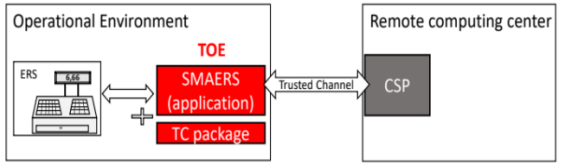
Prüfschritte Umgebungsschutz bei Cloud-TSE

Wo befindet sich der Einsatzort der SMAERS? (zentral in der Cloud oder lokal installiert in der Filiale)

- Rechte- und Rollenkonzept vorhanden am Einsatzort der SMAERS?
- Betriebssystem unter Wartung am Einsatzort der SMAERS?
- Schutz vor Schad-Software vorhanden und aktuell am Einsatzort der SMAERS?
- Schutz der SMAERS-Komponente (TPM oder vergleichbarer Schutz) vorhanden am Einsatzort der SMAERS?

Befinden sich SMAERS und EAS in der selben Einsatzumgebung?

- Bei zentraler SMAERS:
  - Sind lokal nur Eingabegeräte vorhanden?
  - Können lokale Komponenten autark arbeiten (offline-Modus)?
- Bei lokaler SMAERS:
  - Ist der Umgebungsschutz lokal umgesetzt?

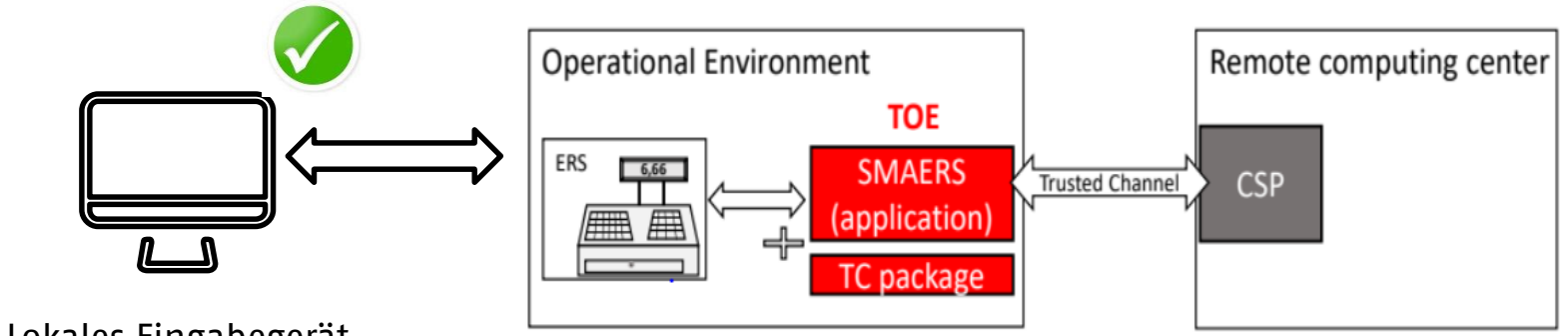


Quelle: SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0, S. 17

Betrieb von Cloud-Aufzeichnungssystemen

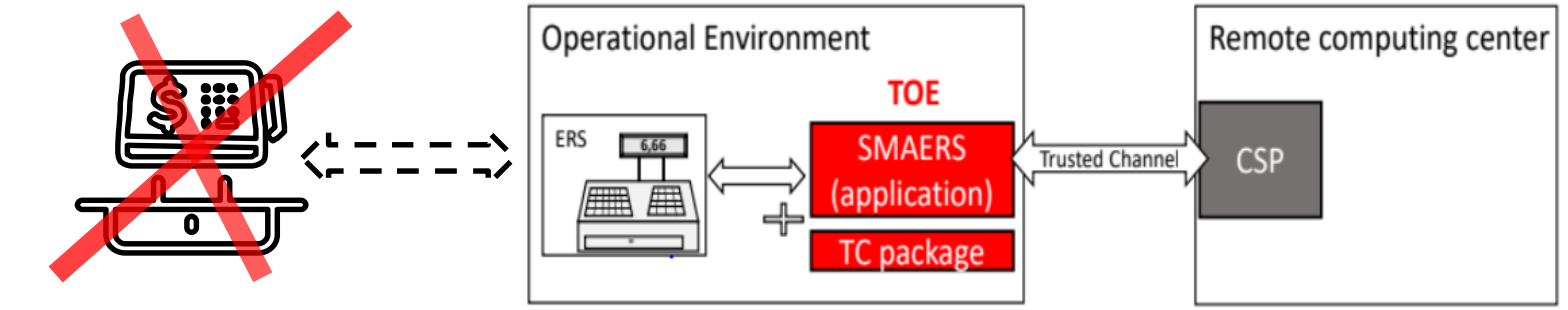
swissbit®

Zulässiger Betrieb



Lokales Eingabegerät

Nicht zulässiger Betrieb



Lokales Aufzeichnungssystem

swissbit®

Selbstauskunft der IT-Abteilung des Steuerpflichtigen zur Nachbereitung der Prüfung

1. Welches Betriebssystem und welche Betriebssystemversion kommt in der Laufzeitumgebung der SMAERS Komponente zum Einsatz? (Hinweis: Bei Hardware TSE ist die Frage bezüglich des direkt angeschlossenen Rechners zu verstehen.)
2. Ist das Betriebssystem der Laufzeitumgebung der SMAERS Komponente in Wartung durch den Hersteller oder mit einem Wartungsvertrag dokumentierbar belegt? (Hinweis: Bei Hardware TSE ist die Frage bezüglich des direkt angeschlossenen Rechners zu verstehen.)
3. Wo befindet sich die Laufzeitumgebung der SMAERS SW bspw. auf der Kassenplattform selbst oder auf einem separaten Rechner? (Hinweis: Bei Hardware TSE ist die Frage bezüglich des direkt angeschlossenen Rechners zu verstehen.)
4. Ist die TSE eine „Hardware TSE“ oder eine „Cloud-TSE“? (Hinweis: Als Cloud TSE ist eine über eine Internet-basierte Verbindung bereitgestellte Signaturlösung zu verstehen. Als „Hardware TSE“ ist ein steckbare Komponente im Formfaktor microSD, SD oder USB zu verstehen.)
5. Wer ist der Hersteller der TSE und wie lautet die TR Zertifizierungs-ID?

Fragen bei Einsatz einer Cloud-TSE:

6. Ist das Kassensystem ohne Internetverbindung einsatzfähig?
7. Wird die SMAERS SW in einer virtualisierten Umgebung (Docker, Virtualbox, VmWare, ...) betrieben?
8. Sind die Daten der Laufzeitumgebung der SMAERS SW verschlüsselt?
9. Durch wen genau kann die Laufzeitumgebung der SMAERS SW administriert werden?
10. Wer hat schreibenden Zugriff und kann somit Einfluss auf den Programmlauf oder Zugriff auf die verschlüsselten Daten der SMAERS SW nehmen?
11. Ist ein Antivirenschutz implementiert? Wenn ja, welche Version?
12. Ist ein TPM vorhanden und in Verwendung?
13. Wie wird der ordnungsgemäße Betrieb der TSE sichergestellt? Liegt das Guidance Manual aus der TSE Zertifizierung dazu vor?
14. Wurden Ausnahmen zum Betrieb basierend auf dem Guidance Manual dokumentiert und wie lauten die Ausnahmen (sofern vorhanden)?
15. Wurde ein Antrag gemäß AO 148 gestellt und wie lautet die Begründung für die Verzögerung?

swissbit®

Hilfe und Erläuterung zur Durchführung der Prüfung

Prüfung zertifizierte TSE

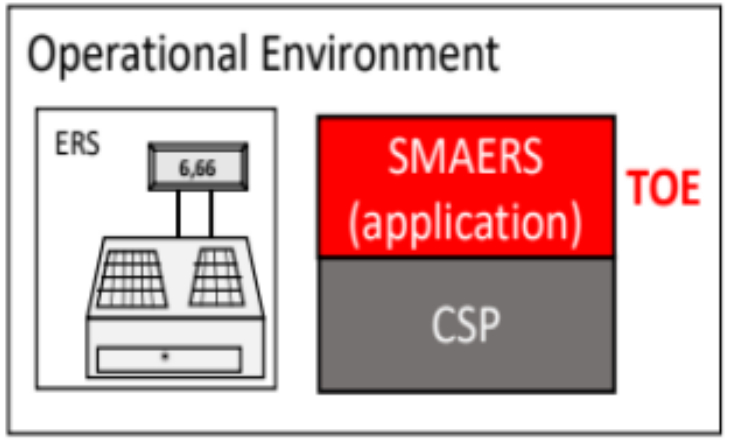
swissbit®

- Anhand von Belegdaten ist nicht ersichtlich, welche TSE integriert wurde
- Unter Verwendung des offiziellen Prüftools der Finanzverwaltung kann der TSE-Hersteller ermittelt werden
- Alternativ ist eine Prüfung von Vertragsunterlagen zur TSE-Integration erforderlich
- Die verwendete TSE kann in der Liste der zertifizierten TSE des BSI aufgeführt sein
  (Die Liste erhebt nicht den Anspruch auf Vollständigkeit, da die Veröffentlichung optional ist):

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifizierte-Produkte-nach-TR/Technische_Sicherheitseinrichtungen/TSE.html
- Die Zertifizierung muss gültig sein (Prüfung Gültigkeitsdatum)
- Kann für die TSE ein BSI Zertifikat vorgewiesen werden oder befindet sich die TSE auf der Liste der zertifizierten TSE, bedeutet das, dass alle erforderlichen Teilzertifizierungen erfolgreich durchlaufen wurden.
- Eine weitergehende Prüfung von Zertifizierungsunterlagen ist daher i.d.R. nicht erforderlich

a) Lokale Kasse mit lokaler TSE

- Die TSE-Komponenten CSP und SMAERS sind in einer physischen Einheit verbaut (Hardware-TSE) UND
- EAS, TSE und Netzwerk befinden sich unter der physischen Kontrolle des Steuerpflichtigen UND
  - Die TSE ist direkt mit dem Aufzeichnungssystem verbunden
    ODER
  - Die TSE befindet sich im lokalen Netzwerk des Steuerpflichtigen

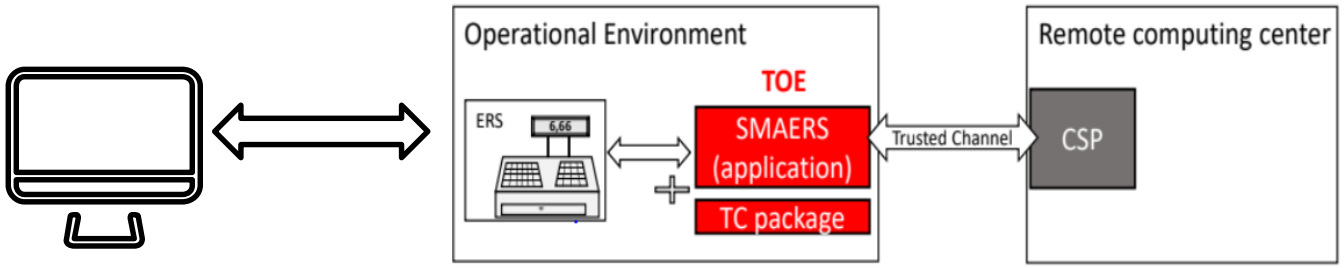


Quelle: SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0

swissbit®

b) Cloud-Kasse und lokales Eingabegerät mit Cloud-TSE

- EAS und SMAERS-Komponente befinden sich in der selben Betriebsumgebung (Rechenzentrum) UND
- Die TSE-Komponenten CSP und SMAERS sind über einen sicheren Kanal miteinander verbunden UND
- Lokales Eingabegerät besitzt keinen Offline-Modus



Eingabegerät

Grafik basiert auf SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0

relevante Quellen zum Verständnis:

FAQ des BMF zu „fernverbundenen TSE“ und „mobile Endgeräte“

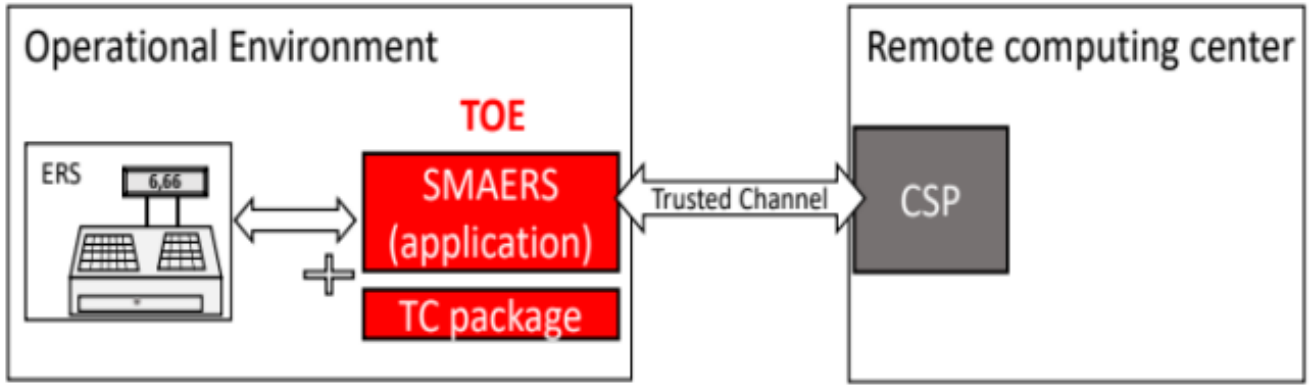
FAQ des BSI zu „Sind auch Cloud Lösungen möglich?“

Klarstellungen und Anwendungshinweise zu BSI TR-03153 und BSI-CC-PP-0105-V2-2020 des BSI Kap. 2.2.1

swissbit®

Lokales Aufzeichnungssystem mit Cloud-TSE

- EAS und SMAERS-Komponente befinden sich in der selben Betriebsumgebung UND
- Die TSE-Komponenten CSP und SMAERS sind über einen sicheren Kanal miteinander verbunden UND
- Das EAS ist direkt oder über lokale Netzwerkkomponenten des Steuerpflichtigen mit der SMAERS-Komponente verbunden.



Quelle: SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020 Version 1.0

relevante Quellen zum Verständnis:

FAQ des BMF zu „fernverbundenen TSE“ und „mobile Endgeräte“

FAQ des BSI zu „Sind auch Cloud Lösungen möglich?“

Klarstellungen und Anwendungshinweise zu BSI TR-03153 und BSI-CC-PP-0105-V2-2020 des BSI Kap. 2.2.1

Der Vorschlag des Prüfkonzepts stellt keine rechtlich bindende Beratung dar.

Abweichungen oder Erweiterung vom hierin beschriebenen Sachstand sind möglich, erhöhen jedoch gegebenenfalls das Risiko eines nicht konformen Betriebs der TSE.

FAQ des BSI: An wen kann ich mich bei weiteren Fragen zu dem Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen wenden?

Ansprechpartner für das Gesetz ist das zuständige Bundesministerium der Finanzen.

Aktuelle technische Informationen finden Sie unter "Schutz vor Manipulation an digitalen Grundaufzeichnungen". Hier werden auch die relevanten Technischen Richtlinien und Schutzprofile veröffentlicht.

Kontakt für weitergehende **technische** Fragen: registrierkassen@bsi.bund.de

Ansprechpartner für weitergehende Fragen zum Ablauf eines Zertifizierungsverfahrens können Sie finden unter Produktzertifizierung.

swissbit®

Reliable Storage &

Embedded IoT Solutions