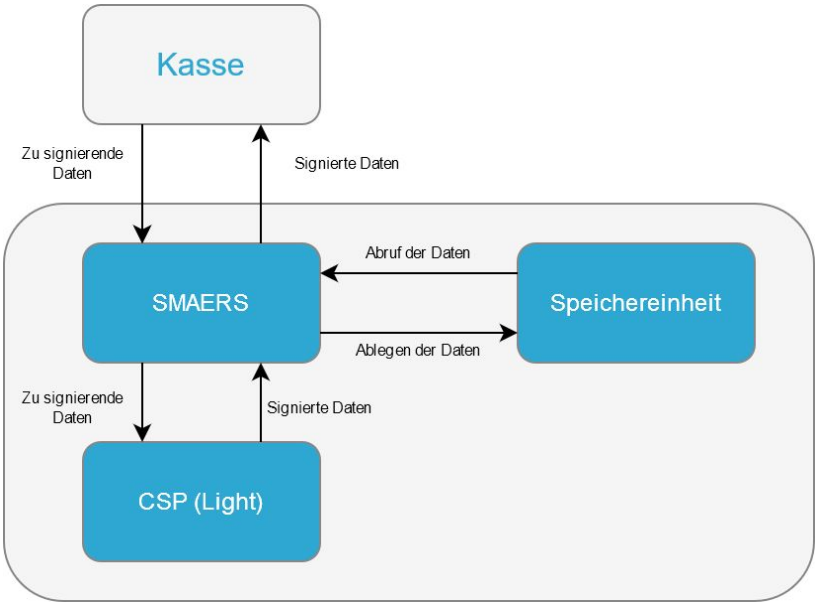
KassenSichV & Technische Sicherheitseinrichtung (TSE)

Elektronische Aufzeichnungssysteme, wie z.B. Registrierkassen oder ERP-Systeme mit Kassenfunktion, müssen mit einer technischen Sicherheitseinrichtung (TSE) gegen Manipulationen geschützt werden. Doch was genau ist eine TSE?

Komponenten und Funktionsweise einer TSE

Die TSE stellt die Schnittstellen zur Aufzeichnung von Transaktionen sowie den Export der abgesicherten Daten bereit. Mit den Komponenten SMAERS und CSP (Cryptographic Service Provider) werden die Daten kryptografisch signiert und somit gegen spätere Manipulation abgesichert. Ein aufsteigender Signatur-Zähler sowie ein Transaktions-Zähler verhindert hier auch das “Verschwinden” mancher Aufzeichnungen, da diese Lücken automatisiert erkannt werden können.

Die Grafik veranschaulicht den Aufbau einer TSE:



SMAERS (Security Module Application for Electronic Record Keeping Systems):
Das Sicherheitsmodul bereitet die abzusichernden Daten innerhalb einer Transaktion auf und kommuniziert direkt mit dem CSP, um die abzusichernden Daten zu signieren.

CSP (Cryptographic Service Provider):
Das Speichermedium erzeugt die Signaturen der abzusichernden Daten.

Die Anforderungen an die Module wurde vom BSI (Bundesamt für Sicherheit in der Informationstechnik) entwickelt und in Richtlinien und Schutzprofilen veröffentlicht.

Weiterführende Informationen:

Technische Richtlinie - BSI TR-03153

Komponenten der TSE - SMAERS

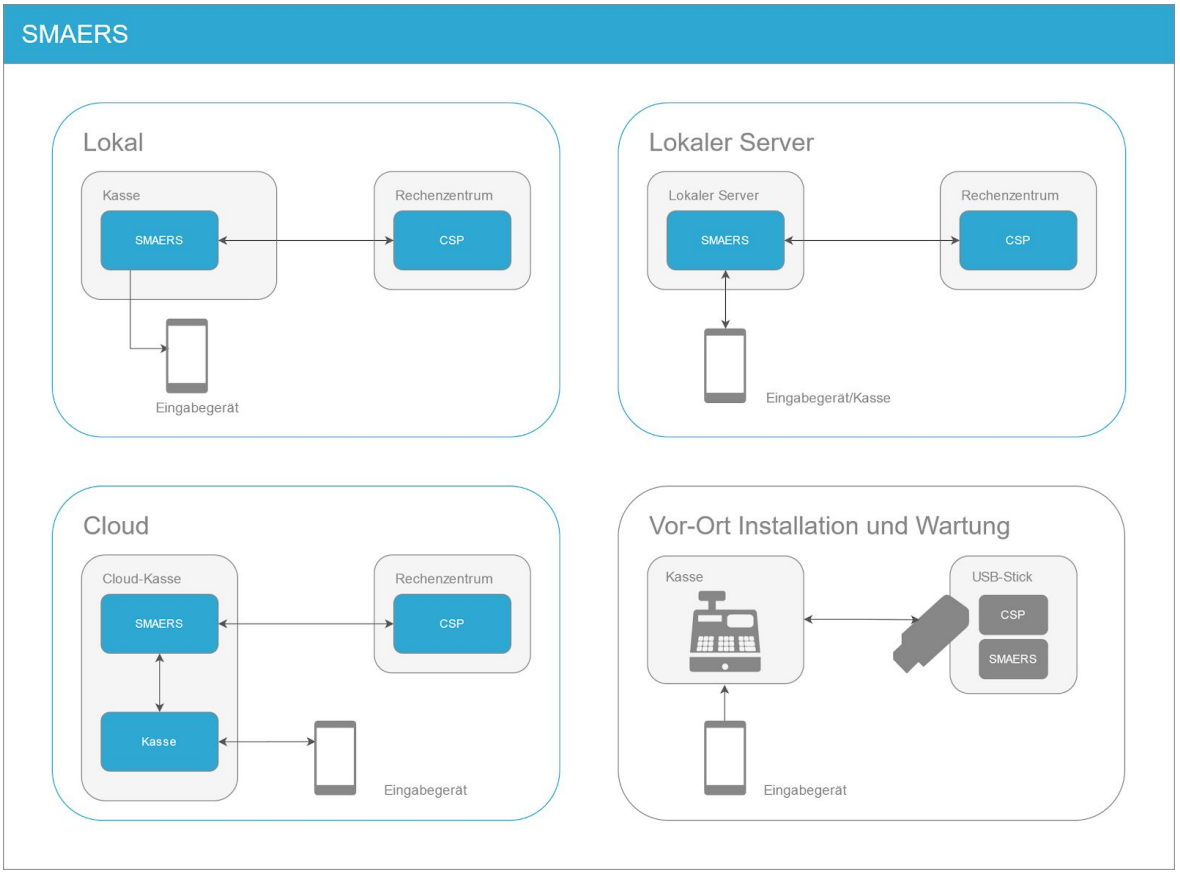
Eine Komponente der TSE (technische Sicherheitseinrichtung) ist die SMAERS (Security Module Application *for* Electronic Record Keeping System) Komponente. Es ist ein Sicherheitsmodul, das die abzusichernden Daten innerhalb einer Transaktion aufbereitet. Dieses Modul muss in das Kassensystem des Steuerpflichtigen integriert werden.

Wo muss das SMAERS betrieben werden?

Die SMAERS Komponente muss am Aufzeichnungssystem, dem ERS (Electronic Record Keeping System), betrieben werden. Die Daten stammen von Aufzeichnungssystemen und deren Eingabegeräten wie beispielsweise einer Tastatur oder einer App auf einem Tablet. Im Signaturprozess sprechen SMAERS und CSP (Cryptographic Service Provider) miteinander. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) zertifiziert die Komponenten wie die SMAERS nach bestimmten Schutzprofilen. Die SMAERS Komponente muss am ERS betrieben werden und daraus ergeben sich drei verteilte Betriebsvarianten und eine Vor-Ort Variante.

Betriebsvarianten

In diesen Varianten kann die SMAERS Komponente betrieben werden und entspricht den Anforderungen des BSI.



1) SMAERS läuft auf der Kasse und signiert im sicheren Rechenzentrum *(CSP wird fernverbunden betrieben).*
2) SMAERS läuft auf einem Server in der jeweiligen Filiale und signiert auf einem entfernten CSP im sicheren Rechenzentrum.
3) Kasse mit SMAERS läuft in der Cloud und signiert auf einem entfernten CSP *(in einem sicheren Rechenzentrum).*
4) Manuelle TSE-Installation (SMAERS und CSP) und Wartung direkt an der Kasse (z.B. USB-Stick, SD-Karte).

BSI Schutzprofile

Das bisher zertifizierte Schutzprofil (v 0.7.5) ermöglichte eine sinnvolle Umsetzung nur für Hardware-token (Variante 4). Cloudbasierte-TSE (Varianten 1-3) werden im Schutzprofil (ab v 0.9.1) erstmals umsetzbar berücksichtigt, dieses lag jedoch nur als Entwurf vor und ist am 28.07.2020 in finaler Version 1.0 vom BSI ausgestellt worden.

Speziell moderne Kassensysteme, die auf cloudbasierte TSE angewiesen sind, haben auf die Freigabe des Schutzprofils gewartet.

Weiterführende Informationen:

SMAERS Schutzprofil BSI-CC-PP-0105-V2-2020

Komponenten der TSE - Der CSP

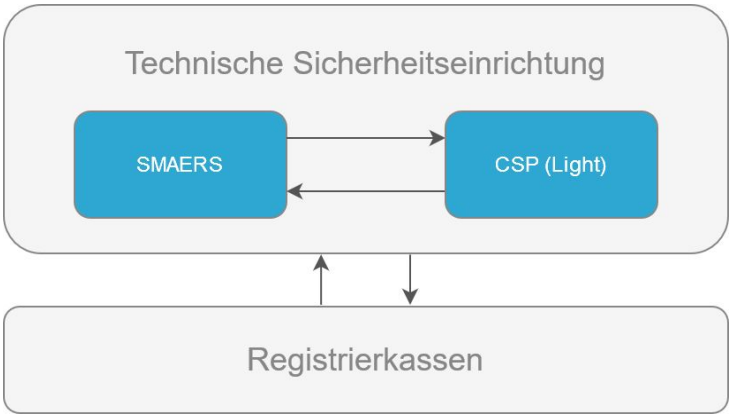
Eine Sicherheits-Komponente der TSE (technische Sicherheitseinrichtung) ist der CSP (Cryptographic Service Provider). Hierbei handelt es sich um die Signatur-Einheit, welche mit kryptographischen Verfahren die abzusichernden Daten entsprechend verarbeitet. Damit werden unerkannte Manipulationen verhindert. Im Signaturprozess sprechen SMAERS (Security Module Application for Electronic Record Keeping System) und CSP über gesicherte Kanäle miteinander.

Definition CSP-L laut BSI

Ein CSP-L stellt “durch die Anwendung von kryptografischen Verfahren die Integrität und Authentizität sowie die Vollständigkeit der elektronischen Aufzeichnung sicher.” (Das CSP-L Schutzprofil BSI-CC-PP-0111-2019.) Stark vereinfacht: Ein CSP-L ist zuständig für die Erstellung der Signatur über einen Beleg.

CSP und CSP-L

Hochleistungs-Signatureinheiten werden über das Schutzprofil der CSP-L definiert. Hierbei handelt es sich um spezialisierte Server-Systeme in hochsicheren Rechenzentren.



Im Gegensatz zum CSP-L ist ein CSP meist ein Chip, welcher nicht effizient im Netzverbund betrieben werden kann. Ein CSP Chip ist vorwiegend für einzelne Kassen geeignet.

Die netzwerkfähige Variante des CSP-L wurde entwickelt, damit es durch Clustering skalierbar ist, einen höheren Datendurchsatz ermöglicht und höhere Ausfallsicherheit gewährleistet.

Beide Varianten sind durch Schutzprofile des BSI (Bundesamt für Sicherheit in der Informationstechnik) definiert.

Weiterführende Informationen:

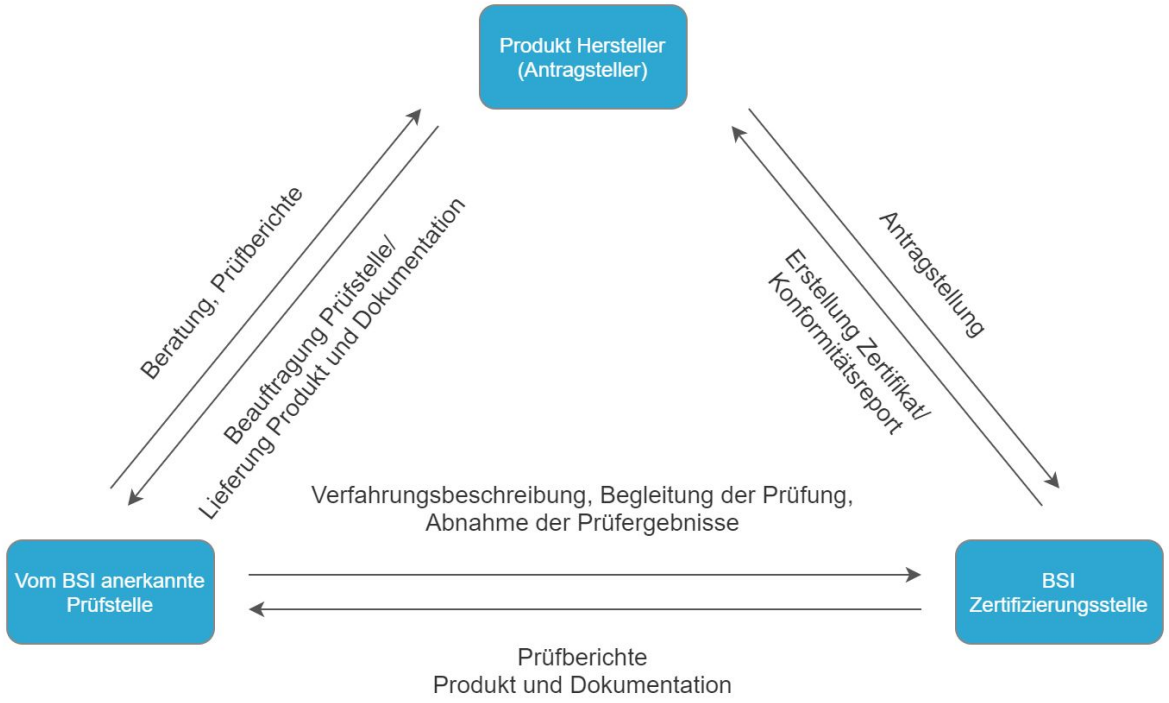
Protection Profile Cryptographic Service Provider Light (CSPL) - BSI-CC-PP-0111-2019
Protection Profile Cryptographic Service Provider Light - Time Stamp Service and Audit
Protection Profile Cryptographic Service Provider Light Time Stamp Service and Audit - Clustering

Zertifizierung der technischen Sicherheitseinrichtung

Die Anforderungen an die Komponenten **SMAERS** (Security Module Application for Electronic Record Keeping System) und **CSP** (Cryptographic Service Provider) werden durch Schutzprofile vorgegeben. Die Erfüllung der Vorgaben für jede Komponente werden im Zuge einer Zertifizierung sichergestellt.

Was ist ein Schutzprofil?

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) spezifiziert in Schutzprofilen, welche technischen Anforderungen zu erfüllen sind, um das Ziel der KassenSichV zu erreichen. In den Schutzprofilen werden Sicherheitsziele und Anforderungen nach Sicherheitsfunktionen der Komponenten beschrieben. Jedoch erfolgt die produktspezifische Konkretisierung durch den Hersteller.



Wie erfolgt eine Zertifizierung?

Die Einhaltung der Schutzprofile bei den Komponenten werden durch einen Evaluator (ein vom BSI akkreditiertes Unternehmen) geprüft. Anschließend wird der Evaluationsbericht zur Überprüfung an das BSI weitergereicht. Ist die TSE korrekt nach den geltenden Vorgaben umgesetzt, wird diese zertifiziert. Das BSI stellt die Zertifizierung aus. Diese muss alle fünf Jahre erneuert werden.

Weiterführende Informationen:

Schutz vor Manipulationen an digitalen Grundaufzeichnungen (S. 21)