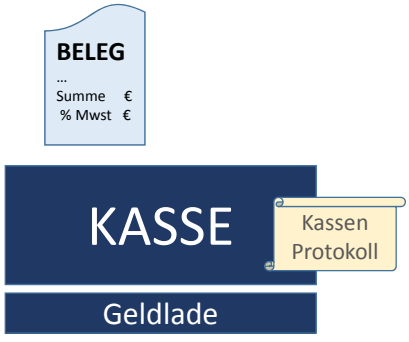
REGISTRIERKASSEN

Elektronische Signatur:
Sicherheitsanforderungen und Nachweise

Prof. Reinhard Posch

A-SIT

Registrierkassenkomponenten vor 2016



Ab 1.1.2016 legt das Gesetz eindeutig fest, wer eine Registrierkasse für Barumsätze verwenden muss.
Technische Anforderung in höherem Detail werden erst mit 1.1.2017 zwingend notwendig.
Es kann jedoch jederzeit eine Registrierkasse eingesetzt werden, die die Anforderungen 2017 erfüllt

Registrierkassenkomponenten ab 2017

UND DIES KOMMT AN ANFORDERUNGEN HINZU

Maschinenlesbarer CODE
Dieser Code enthält die wesentlichen Inhalte des Belegs, die Verkettung und die Signatur als Manipulationsschutz

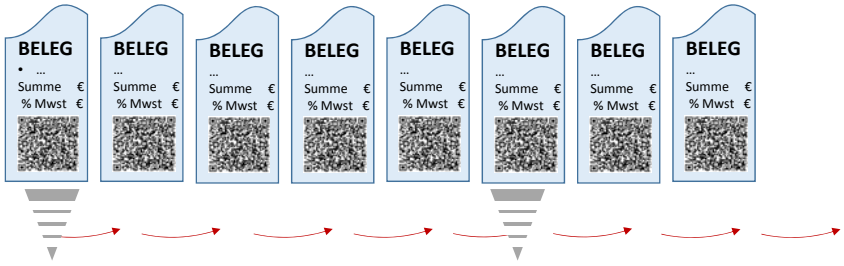
DATENERFASSUNGPROTOKOLL (DEP)

Dieses Protokollenthält die Daten der maschinenlesbaren Codes aller Belege und muss nach einem Standardformat exportiert werden können.

Sicherheitseinrichtung

Signaturkarte oder HSM zur Signierung der Belege

Wodurch ist der Manipulationsschutz gegeben?



- **Alle Belege eines DEP sind mit Hashwerten verkettet**
- **Jeder Beleg ist signiert**
- **Jeder Beleg enthält zusätzlich den verschlüsselten Wert des Umsatzzählers**
- **Startbeleg und Jahresbelege werden durch den Betrieb geprüft**

Die Prüfung der Belege hinterlässt in der Datenbank einen „nichtssagenden" Hashwert. Damit kann später **NUR** gemeinsam mit dem geprüften Beleg oder dem DEP nachgewiesen werden, ob der behauptete Beleg geprüft wurde.

Welche Sicherheitsverfahren werden eingesetzt?

- **HASHVERFAHREN** das sind Werte, die aus vorliegenden Daten (in diesem Fall Belege) einen "kurzen" Kontrollwert ermitteln, wobei es nicht gelingt, die Daten zu verändern, ohne dass dies auch im Hashwert eine Änderung hervorruft.
- **AES-VERSCHLÜSSELUNG** des Umsatzzählers. Der Unternehmer (die Kasse) wählt einen Geheimhaltungsschlüssel (AES 256) für die Verschlüsselung des Umsatzzählers.
- **SIGNATUR** elektronische Signatur zur Sicherstellung der Unverändertheit des gesamten Belegs inklusive der Verkettung und des Umsatzzählers. Es werden dazu elliptische Kurven nach dem Stand der Technik eingesetzt, um möglichst kurze Signaturwerte und nicht extrem große QR-Codes zu bekommen.

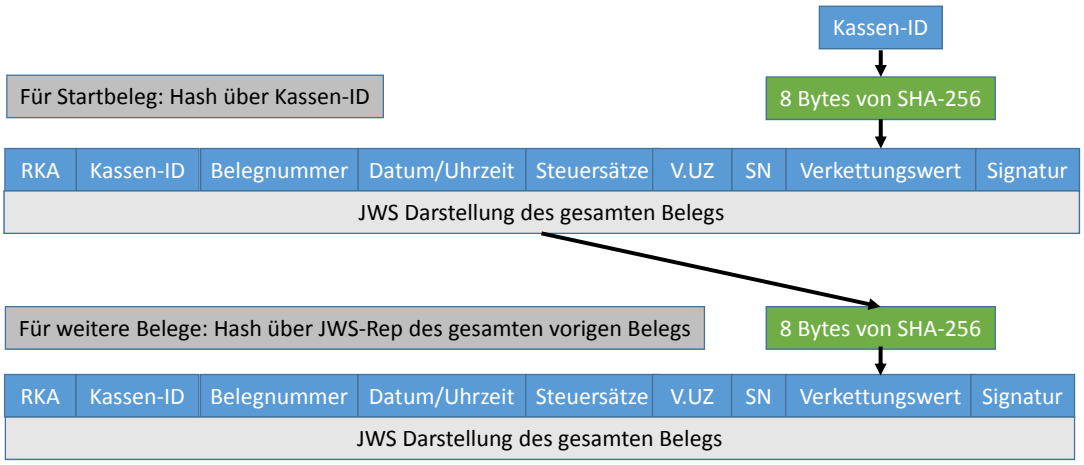
Darstellung des Belegs

_R1-AT0_DEMO-CASH-BOX524_366600_2015-12-17T11:23:44_31,94_38,23_0,00_0,00_24,73_hBYsrFMgTd0=_47be737cb1f6d1f1_z3sjuZjdSNM=_7QMJ+7WgAzJ0ETiFY+1hzgggr1JuHDhZL5Hshor/27Guysi/H22dIv5m+H4DH6J5y5hGMgo6FmpWKBKag/C9DQ==

RKA	Kassen-ID	Belegnummer	Datum/Uhrzeit	Steuersätze	V.UZ	SN	Verkettungswert	Signatur

R1-AT0	DEMO-CASH-BOX524	366600	2015-12-17T11:23:44	31,94_38,23_0,00_0,00_24,73	hBYsrFMgTd0
47be737cb1f6d1f1	z3sjuZjdSNM				
7QMJ+7WgAzJ0ETiFY+1hzgggr1JuHDhZL5Hshor/27Guysi/H22dIv5m+H4DH6J5y5hGMgo6FmpWKBKag/C9DQ==					

HASHVERFAHREN – Verkettung



VERSCHLÜSSELUNG DES UMSATZZÄHLERS

RKA	Kassen-ID	Belegnummer	Datum/Uhrzeit	Steuersätze	V.UZ	SN	Verkettungswert	Signatur

_R1-AT0_DEMO-CASH-BOX524_366600_2015-12-17T11:23:44_31,94_38,23_0,00_0,00_24,73_hBYsrFMgTd0=_47be737cb1f6d1f1_z3sjuZjdSNM=_7QMJ+7WgAzJ0ETiFY+1hzgggr1JuHDhZL5Hshor/27Guysi/H22dIv5m+H4DH6J5y5hGMgo6FmpWKBKag/C9DQ==

Startbeleg	Summe 0	Verschlüsselt: Wert 0
Beleg 1	Summe 10	Verschlüsselt: Wert 10
Beleg 2	Summe 30	Verschlüsselt: Wert 40
Beleg 3 (Training)	Summe 100	Zeichenkette „TRA“
Beleg 4	Summe 100	Verschlüsselt: Wert 140
Beleg 5 (Storno)	Summe -30	Zeichenkette „STO“
Jahresbeleg	Summe 0	Verschlüsselt: Wert 110

Kasse	Umsatzzähler 0
Kasse	Umsatzzähler 10
Kasse	Umsatzzähler 40
Kasse	Umsatzzähler 40
Kasse	Umsatzzähler 140
Kasse	Umsatzzähler 110
Kasse	Umsatzzähler 110

VERSCHLÜSSELUNG DES UMSATZZÄHLERS

- **Verfahren: AES-256 ICM/CTR**
  Wahl von ICM/CTR, weil damit verschlüsselter Wert nur so lange wie Inputdaten (sonst Blocklänge: 16 Bytes)
- **Emulation mit CFB/ECB Modus einfach**
  (falls ICM/CTR nicht verfügbar)
- **AES-256 Schlüssel wird in Finanzonline hinterlegt**
- **Verschlüsselter Umsatzzähler in QR-Code kann von Dritten nicht entschlüsselt werden**

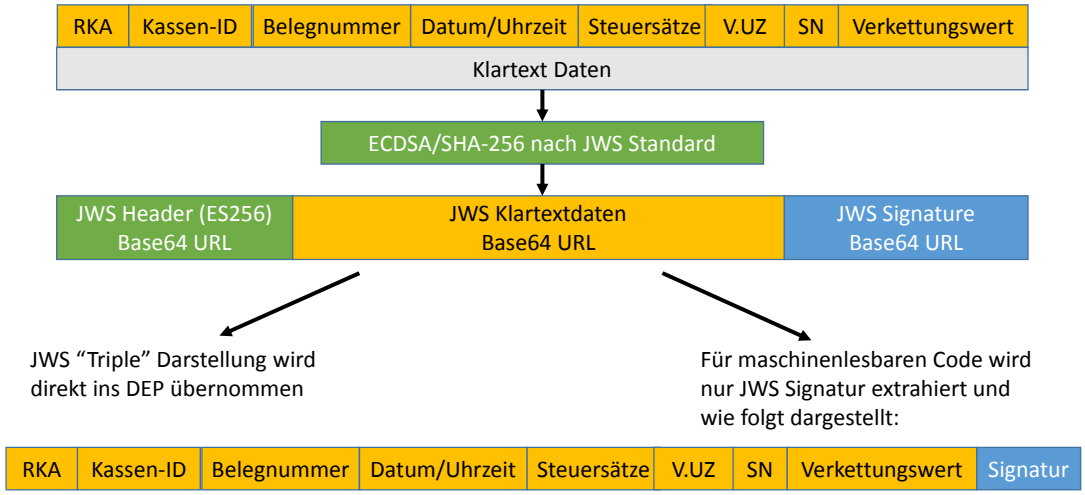
SIGNATUR 1

Darstellung der Signatur im maschinenlesbaren Code (QR-Code)

RKA	Kassen-ID	Belegnummer	Datum/Uhrzeit	Steuersätze	V.UZ	SN	Verkettungswert	Signatur

_R1-AT0_DEMO-CASH-BOX524_366600_2015-12-17T11:23:44_31,94_38,23_0,00_0,00_24,73_hBYsrFMgTd0=_47be737cb1f6d1f1_z3sjuZjdSNM=_7QMJ+7WgAzJ0ETiFY+1hzgggr1JuHDhZL5Hshor/27Guysi/H22dIv5m+H4DH6J5y5hGMgo6FmpWKBKag/C9DQ==

Signatur 2



JWS "Triple" Darstellung wird direkt ins DEP übernommen

Für maschinenlesbaren Code wird nur JWS Signatur extrahiert und wie folgt dargestellt:

JWS Header wird für QR-Code Darstellung verworfen, kann aber für Prüfung rekonstruiert werden.

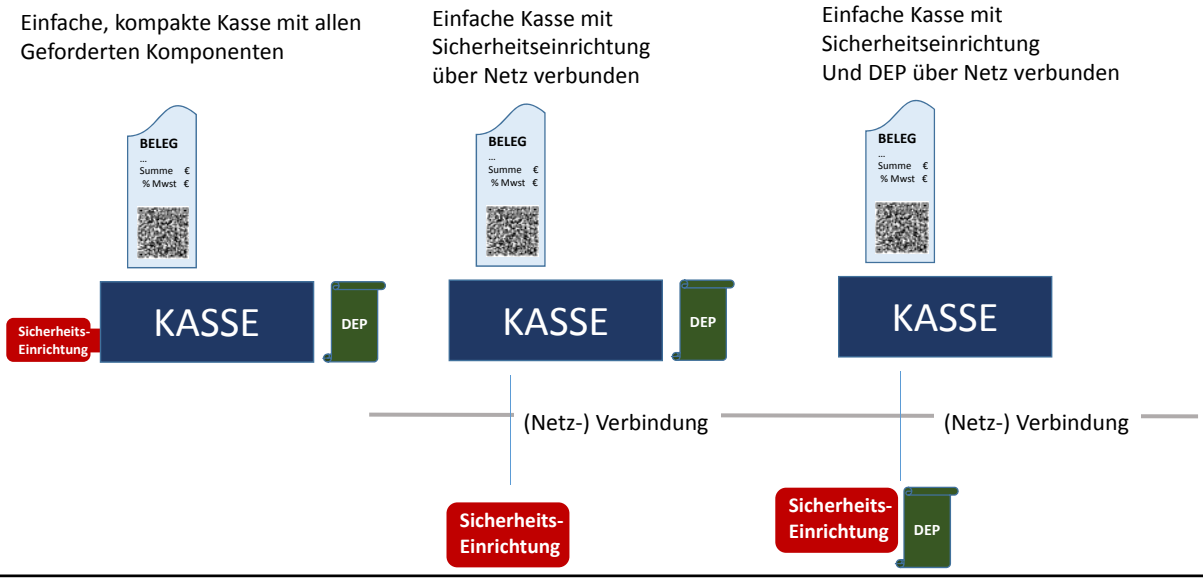
Welche Manipulationen werden dadurch verhindert?

- **Verkettung**
  - Nachträgliches Einfügen/Entfernen von Belegen nicht möglich
- **Signatur**
  - Zuordnung zu Unternehmen das den Beleg erstellt hat (**Authentizität**)
  - Beleg/QR-Code kann nachträglich nicht verändern werden (**Integrität**)
- **Verschlüsselung des Umsatzzählers**
  - **Vertraulichkeit** des Umsatzzählers durch AES-Verschlüsselung gewährleistet

DER MUSTERCODE

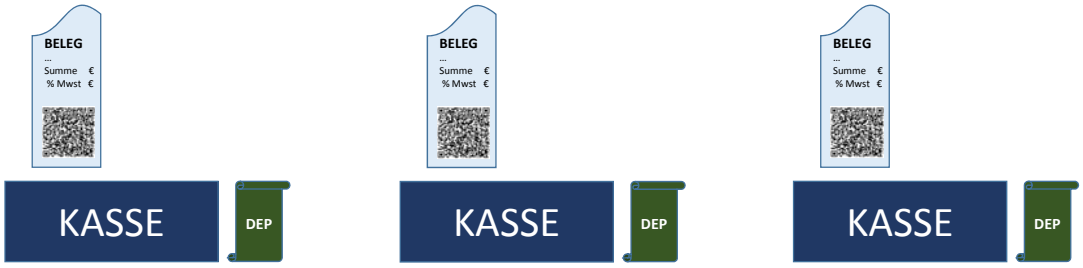
- https://github.com/a-sit-plus/at-registrierkassen-mustercode
  - Beispiele, technische Erläuterung der RKSV
  - Prüftools für Hersteller zum Verifizieren der Korrektheit der erstellen Belege
- Weitere Aktivitäten bis Version 1.0
  - Bereitstellen von Testfällen für unterschiedliche Abläufe
  - Wartung, QS
  - Beispiele für Kartenintegration (abhängig von Informationen der ZDAs)

Registrierkassenkonfigurationen



Registrierkassenkonfigurationen

Mehrere eigenständige Kassen mit einer Sicherheitseinrichtung verbunden



(Netz-) Verbindung

- Die Zahl der Kassen pro Sicherheitseinrichtung ist nur durch die Leistungsfähigkeit derselben limitiert
- Bei Netzausfall ist „**Sicherheitseinrichtung ausgefallen**“ am Beleg auszugeben

Sicherheits-Einrichtung

- Die Sicherheitseinrichtung kann eine Smartcard und ein Microrechner sein (z.B. Signaturkarte <10 €, PI-Zero inkl. WLAN < 25€) [bis ca 4 Signaturen(=Belegen] pro Sec.
- Die Sicherheitseinrichtung kann auch ein HSM sein [kann auch tausenden Belege pro Sec. Signieren]

Registrierkassenkonfigurationen

Mehrere Eingabestationen über das Netz mit einem DEP verbunden

(Netz-) Verbindung

Optional kann der Belegdrucker auch zentral aufgestellt sein

Sicherheits-Einrichtung

Bei Netzausfall ist in diesem Fall **die Kasse ausgefallen**! Es müssen die Belege entsprechend nacherfasst werden.

Geschlossene Gesamtsysteme Konfigurationen

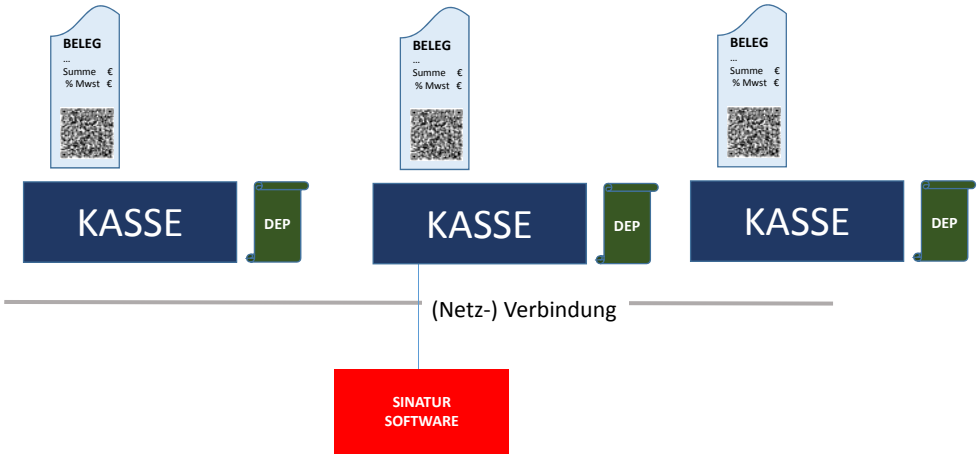
MINDESTENS 31 DEP!

VEREINFACHUNGEN BEI GESCHLOSSENEN GESAMTSYSTEMEN

- **Keine Zertifikate erforderlich** – Das Unternehmen erzeugt die Signaturschlüssel selber
- **Keine Sicherheitshardware notwendig** – Die Software zur Signatur wird vom Gutachter geprüft und zur Unveränderbarkeit im Einsatz signiert.
- **Einmelden von Kassengruppen** – Anstelle von Einzelkassen können Gruppen von Kassen eines Unternehmens mit gleichem Signaturschlüssel und gleichem AES-Schlüssel mit einer Meldemaske eingemeldet werden. **Diese Vereinfachung könnte bei entsprechendem Bedarf auch bei Kassen die eine Hardwaresicherheitseinrichtung gemeinsam nutzen verfügbar gemacht werden.**

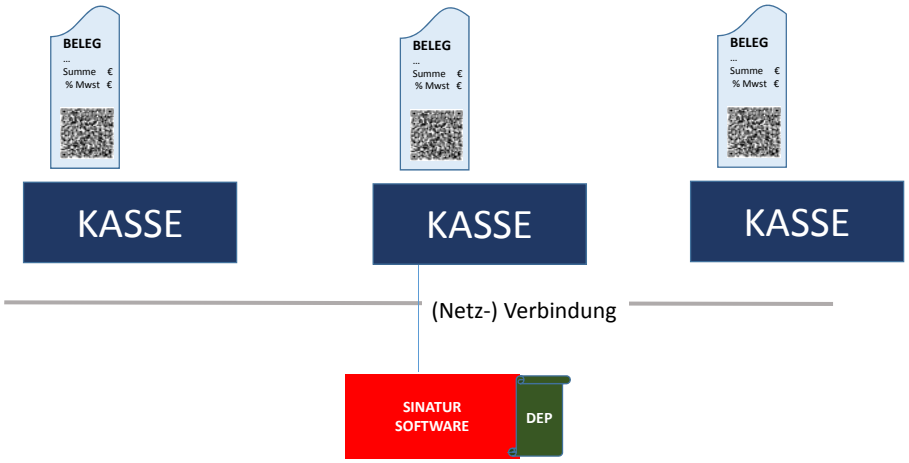
Geschlossene Gesamtsysteme Konfigurationen

MINDESTENS 31 DEP!



Geschlossene Gesamtsysteme Konfigurationen

MINDESTENS 31 DEP!



Registrierkassen Geschlossene Gesamtsysteme

- **ENTSCHEIDUNG** – Ob die Vereinfachungen für geschlossene Gesamtsysteme genutzt werden ist eine reine Unternehmensentscheidung. Auch eine große Handelskette könnte beispielsweise pro Filiale eine oder mehrere Karten bzw. einen HSM verwenden und nicht von der Vereinfachung gebrauch machen. Ein HSM für die gesamte Kette wäre gleichfalls vorstellbar.
- **NETZ UND SONSTIGE AUSFÄLLE** – Sofern der Zugang zur Signatur von der Kasse aus gestört ist, trifft der Fall „Sicherheitseinrichtung ausgefallen“ zu – Dies gilt sowohl für zentrale Serverlösungen in GG als auch bei HW-Signatureinrichtungen.
- **MINDESTENS 31 DEP** – Diese Voraussetzung ist bei GG zu beachten. Sofern diese nicht gegeben ist liegt keine Verwendung einer Registrierkasse im Sinne des Gesetzes vor. Eine reine Definition von 31 Kassen, die in der Praxis nicht verwendet werden, wird nicht als zulässig anzusehen sein.


Signatur – Sicherstellen der Unveränderthеit nach dem Stand der Technik
Verkettung über Hashwerte – Sicherstellen, dass kein Beleg mitten aus der Kette entnommen werden kann
Flexible Anordnung von Kasse (Gerät) Datenerfassungsprotokoll und Sicherheitseinrichtung
Keine Onlinefunktion der Kasse erforderlich – Belegprüfung via APP
Technische Erleichterungen bei geschlossenen Gesamtsystemen – gleiche Verfahren
DANKE FÜR DIE AUFMERKSAMKEIT
REINHARD.POSCH@A-SIT.AT
A-SIT