Verifizierung digitaler Signaturen auf Kassenzetteln in Deutschland

Erik Prendke

Bachelorarbeit am Institut für Informatik der Freien Universität Berlin

Arbeitsgruppe Sichere Identität

09.02.2023

Motivation

- Manipulation von Registrierkassen war in der Vergangenheit sehr einfach
- Seit Januar 2020 Beginn der Umstellung auf eine TSE Pflicht [4]
- TSE soll jeden Vorgang sichern und digital signieren
- Ende der Übergangsfrist bis Ende 2022 [4]
- QR-Codes auf Bons sollen den Vorgang vereinfachen und Papier sparen

Problemstellung

- Ist es möglich ist, anhand eines Kassenzettel diesen auf seine Echtheit, bzw. Legitimität zu überprüfen, bzw. wie einfach ist dies möglich.

Grundlagen: Signatur

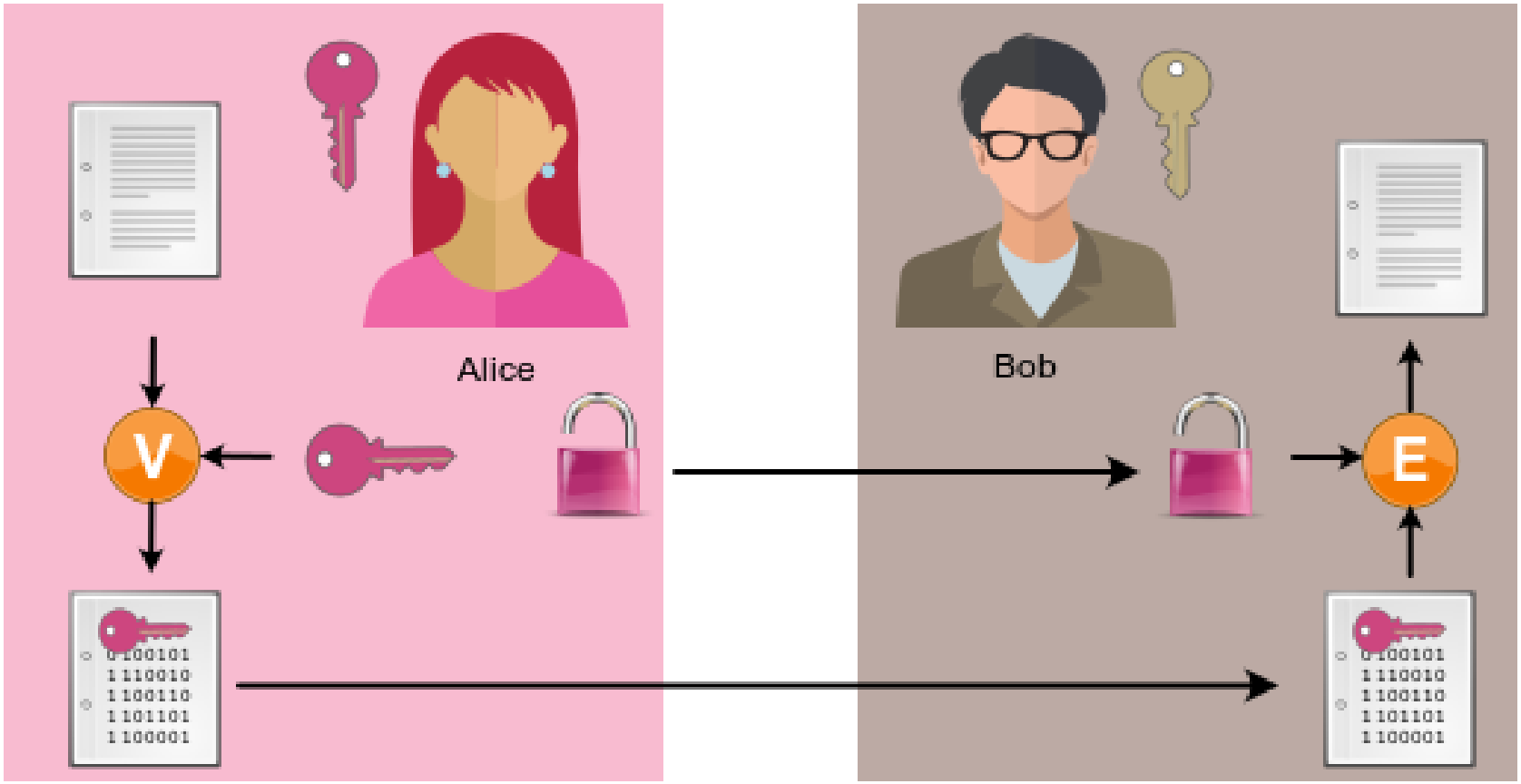

Abbildung: Alice und Bob Beispiel digitale Signaturen[1]

Grundlagen: Signatur

- Signaturverfahren: ECDSA oder ECSDSA [5]
- Weitere Parameter, die bekannt sein müssen:
  - EC-Domain-Parameter
  - Hashfunktion
  - Public Key Format
  - Message

Grundlagen: QR-Code

<qr-code-version>;
<kassen-seriennummer>;
<processType>;<processData>;
<transaktions-nummer>;
<signatur-zaehler>;
<start-zeit>;<log-time>;
<sig-alg>;<log-time-format>;
<signatur>;<public-key>

Abbildung: QR-Code Beispiel mit Beispieldaten [6]

Grundlagen: Kassenzetteldaten

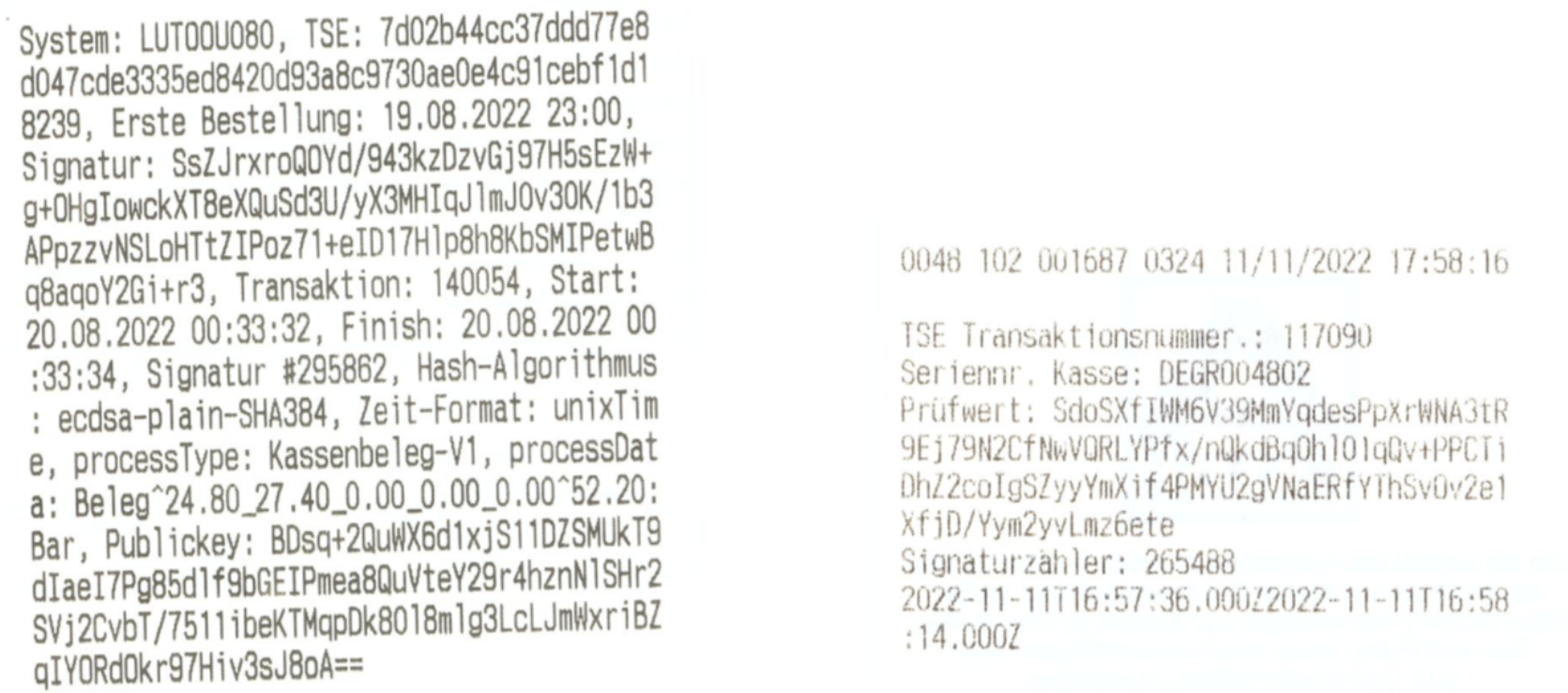

Abbildung: Beispiele für unterschiedliche Ausgaben von TSE-Daten auf Bons

Programm

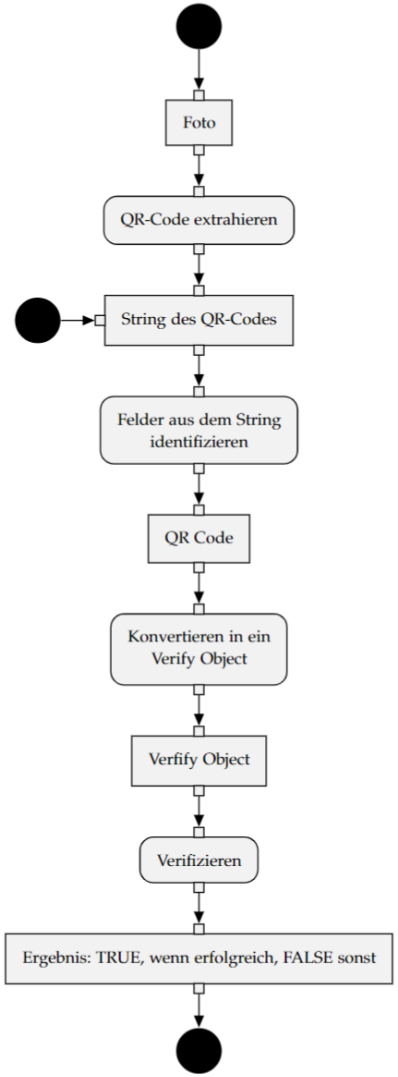
Foto
QR-Code extrahieren
String des QR-Codes
Felder aus dem String identifizieren
QR Code
Konvertieren in ein Verify Object
Verfify Object
Verifizieren
Ergebnis: TRUE, wenn erfolgreich, FALSE sonst

Programm: test.py

- Message Daten werden ausprobiert
- Zusammensetzung verschiedener Message Daten durch Schleifen
- Zusammensetzung von ASN1 codierter Message mit echter Log Message

Ergebnisse: Testdaten

- 43 gesammelte Bons fotografiert
- verschieden Farben, blau und weiß
- es gibt Empfehlungen zu der Größe der QR-Codes, die teils nicht eingehalten werden
- Fotos wurden mit rangezoomtem QR-Code und als ganzer Bon gemacht

Ergebnisse: QR- Code Extraktion

- Bilder werden für bessere Erkennung neu skaliert
- auf blau gedruckte QR-Codes sind schwer einlesbar
- QR-Codes ohne umgesetzte Empfehlung sind schwer einlesbar
- Ausgeblichene Bons sind ein Problem!

Ergebnisse: Verifikation

- Evaluierung konnte nicht durchgeführt werden
- Endgültige Message Zusammensetzung konnte nicht gefunden werden
- Probierte Methoden:
  - Konkatenierung der Felder mit Symbol
  - ASN1 DER Codierungen der Log Message

Diskussion: QR-Code

- Datenmenge nicht repräsentativ
- Kontraste sind wichtig bei der Erkennung
- Qualität des Drucks ist entscheidend
- Einhaltung der Empfehlungen hilft

Diskussion: Verifikation

- Message wird unzureichend beschrieben
- Missverständliche Beschreibungen durch verschiedene Behörden
- Umsetzungen teils fehlerhaft
- Public Key kann nicht auf Echtheit überprüft werden
- QR-Code oder Bon reichen nicht für eine echte Überprüfung der Legitimität aus!

Ausblick

- Auslagerung der QR-Code Erkennung evt. sinnvoll
- Programm kann erweitert werden, wenn die Message Zusammensetzung bekannt ist.
- Es gibt bereits ein teilweise funktionierendes Programm eines Kassenherstellers [3]
- Anfrage an das BSI
- TSE-Simulator analysieren und Verifikation als Gegenstück bauen [2]

[1] *Asymmetrie umkehren*. 16. März 2021. URL: https://informatik.mygymer.ch/g23c/013.kryptologie-sicherheit/05.signature.html#asymmetrie-umkehren (besucht am 05. 02. 2023).

[2] Userpseudonym: DeJuPo. *TSE-Simulator*. 21. Apr. 2021. URL: https://github.com/DeJuPo/TSE-Simulator (besucht am 29. 12. 2022).

[3] ERGO SOFT Softwareentwicklung GmbH. *kassen-qr-code-test.de*. URL: https://kassen-qr-code-test.de/ (besucht am 29. 12. 2022).

[4] OktoPOS Solutions GmbH. *Kassensicherungsverordnung*. 28. März 2022. URL: https://kassensichv.com/ (besucht am 21. 12. 2022).

[5] *Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API*. Technische Richtlinie

BSI TR-03116 Stand 2022. Bonn, Deutschland: Bundesamt für Sicherheit in der Informationstechnik, 22. Feb. 2022.

[6] *Zusammenstellung der Beschlüsse und Bundeskonventionen zu den Standardtabellen im Bereich der Kassenbuchhaltung - Digitale Schnittstelle der Finanzverwaltung für Kassensysteme (DSFinV-K) -*. Dateiensammlung DSFinV-K Version 2.3. Bonn, Deutschland: Bundeszentralamt für Steuern, März 2022.