# TSE-Signatur Verifier

Kevin App, Robin Kern, Torsten Kramer, Max Dümpelmann
Hochschule Furtwangen University
Fakultät Informatik
Deutschland, Furtwangen

Kevin.app@hs-furtwangen.de,
R.Kern@hs-furtwangen.de,
Torsten.Juergen,Kramer@hs-furtwangen.de,
max.duempelmann@hs-furtwangen.de

***Abstract***

**Introduction**

Since finances play a major role today, it is always important not to lose sight of the associated regulations. An example of this would be the Cash Register Security Ordinance, which is responsible for preventing manipulation of cash registers. This stipulates that every cash register in Germany must be equipped with a technical security device, also known as a TSE, if the year of manufacture permits this. This ensures that the transactions carried out by the respective cash register are stored on the internal memory and then supplies the code back to the cash register. The code received is then printed on the receipt. Since these cash register receipts are provided with a TSE signature and deposited with a QR code, it is also important to be able to verify this. To explain this in more detail to others, this topic will be used in a teacher training course about encryption and give the audience a more detailed insight and initial knowledge in the area of signing and verification.

## I. Objectives

The goal of this research project is to develop a verifier with the help of Prof. Dr. Neiße as well as the BSI and Swissbit, which offers the possibility to process cash receipts and signatures based on examples and to make it possible to verify them. In addition, training documents are to be provided, with which it is possible to use in the context of a teacher advanced training to the topic coding these and to bring the participants of this meeting this topic range more near.

## II. Tools/ programm

The training materials are extremely relevant for teacher training, and it was important to describe the individual paths and procedures in detail in the step-by-step instructions so that this could also be carried out using practical examples. The most important tools were documented in detail in the training documents to be created. These tools are crucial and to ensure learning success. They are as follows:

- beTSEy which is the self-developed app used to create and read QR codes.
- Cryptool 1 which is offered as a free program for cryptography and for cryptanalysis.
- Pari GP online calculator which is a computer algebra system created to facilitate calculations of number theories.
- Unixtime calculator which is used to convert time to a Unix time.
- Whitespace-Remover a program which is used to remove tabs, spaces, or line breaks.

With the above listed tools, it is possible to perform the present course and to build up the practical understanding.

## III. Results

At the beginning of the TSE Verifier project, the documents provided were first analyzed and an attempt was made to familiarize oneself with the BSI subject area. Based on the knowledge, the topics to be worked on were then discussed and classified. Accordingly, we developed an application as a frnt-end. At the same time, mathematical calculations in the area of elliptic curves were carried out for the back end, which were mandatory for the programming of the back end. In the same moment the training material for the course separate to the development was co-written, which documents the exact procedure and execution, so that it is clear and understandable for the reader. In the same period of the research, regular meetings with Prof. Dr. Neiße were held

in order to remain permanently up to date and also to always pick up feedback from the most current status in the project itself. This feedback was directly implemented, and the additions were implemented into the project. So that the source code can be used, the application was created and integrated on a cell phone. So that the TSE generator with its own created QR code can check, sign, and verify.

The achieved results are impressive, and the application can now be used productively. Since we did not get hold of the private key, we were only able to verify as well as sign a QR code, which however worked in the created application. The created training materials can now also be used in the expected teaching training.

## ACKNOWLEDGMENT

At this point we would like to thank the whole project team "TSE-Verifier" as well as Professor Neiße, who has been behind this project since day one and has always tried to help as much as possible. Also thanks to the team for the great cooperation and to the successfully completed project.

## REFERENCES

[1] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/TSE_Signature.pdfJ.

[2] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/TR-03151.pdfK.

[3] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/20190802_DSFinV_K_V_2_0.pdfY.

[4] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/ECDSA_e.pdf

[5] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/BSI-TR-03111_V-2-0_pdf.pdf

[6] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/sc27wg2-sd7-data.pdf

[7] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/Domain-parameters.pdf

[8] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/ecdsa_example_e.pdf

[9] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/BSI-TR-03116-5.pdf

[10] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/20220304_DSFinV_K_2_3.pdf

[11] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/Logmessage_Aufbau.pdf

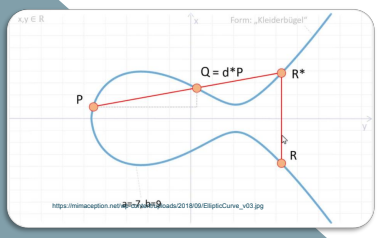
[12] https://felix.hs-furtwangen.de/auth/1%3A1%3A1446940485%3A3%3A0%3Aserv%3Ax%3A_csrf%3A4e352449-06d8-486b-a542-e46c3b3f7514/GS_TSE-Infozettel.pdf

2022

# TSE-Signatur Verifier

## Forschungsprojekt MOS:

Erstellung einer mobilen Applikation zur Verifizierung eines TSE QR-Codes




## Signierung

### Signieren:Der Teilnehmer T möchte die Nachricht m signieren

(1) Berechne Hash−Wert der Nachricht h:=H(m)

(2) Wähle zufällige Zahl 1<k<p

(3)Berechne K: [ k ]G, K = $(x_k,y_k)$

(4)Wenn r:= $x_k$ mod p = 0, beginne von (2)

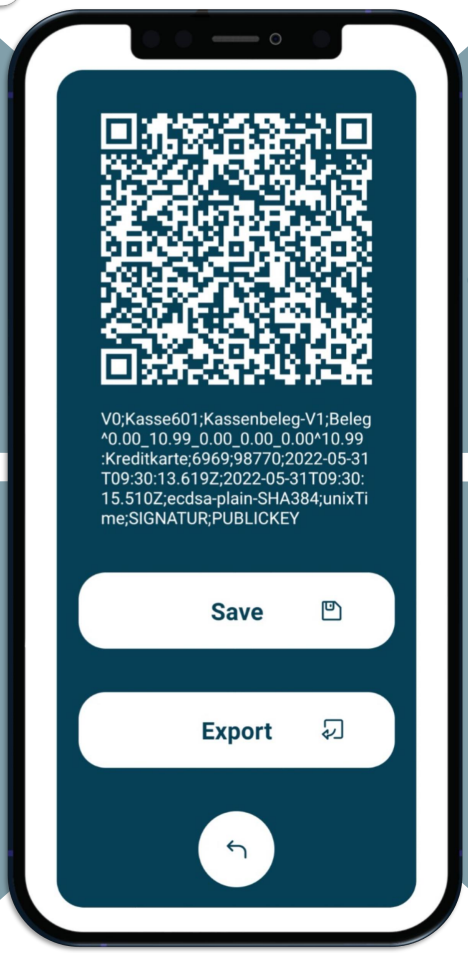
(5)Berechne in der Menge $\mathbb{F}_p$ das $k^*$ so dass $k \cdot k^*=1$ mod p

(6)Wenn s:=$k^* \cdot (h + r \cdot d_T)$ mod p Null ist, beginne von (2)

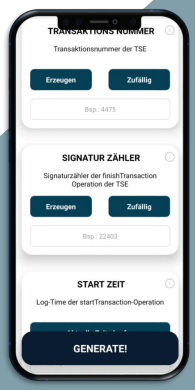
(7)Sende signierte Nachricht(m,(r,s))

### beTSEy

Multiplattform Applikation




### TSE Generator




### Erstellung eines eigenen TSE-QR Codes durch Eingabe eigener TSE-Daten

- Erstellung der Signatur und des öffentlichen Schlüssels
- Erstellung der Log Message

### Verifizieren: Jeder kann die Signatur T von der Nachricht m verifizieren

(1) Wenn r mod p=0 oder s mod p=0, dann Signatur ungültig

(2) Hash−Wert der Nachricht: h = H (m)

(3)Berechne in der Menge $\mathbb{F}_p$ das $s^*$ so dass $s \cdot s^*=1$ mod p

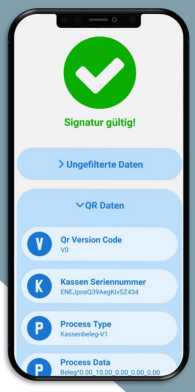
(4)Wenn L:=$[s^*]([h]G + [r]D_T) = (x_L,y_L)$ $\mathcal{O}$ entspricht → Signatur ungültig

(5)Wenn $x_L$ mod p gleich r, → Signatur gültig

## Verifizierung

### Verifizierung eines TSE QR-Codes

- Verifikation eines QR-Codes
- Ausgabe aller im QR-Code vorhandenen und ermittelten Daten




### TSE Verifier


von Kevin App, Robin Kern, Torsten Kramer, Max Dümpelmann