# E-Voting-System Post R. 1.4.4.4: Trusted-Build: Bericht

## 1. Vorgehen

Der Rechtsdienst der Staatskanzlei des Kantons Thurgau hat für die Kantone Thurgau, St. Gallen, Basel-Stadt und Graubünden das E-Voting-System der Post mit dem von der Post auf https://gitlab.com/swisspost-evoting/e-voting/e-voting veröffentlichten Quellcode mit einem vom Rechtsdienst selbst erstellten Skript am 17. November 2024, 23.08 Uhr, kompiliert und die Hashwerte der kompilierten Dateien gebildet.

## 2. Hashwerte JavaScript-Dateien Voter-Portal (SHA-384, base64)

| | |
|---|---|
| crypto.ov-api.js | 9alQr57CZH3awteoDnjYkHFhdgE7OQlCh+RWiTSx39sM989KfgIvmYiaB/QEmQ8J |
| crypto.ov-worker.js | AqfFbQGoWuNqQKdN5/yWUiSeBTcgTRKoFZjvGv6y54l2pb+goOGxKnqVrIlsCH11 |
| main.js | XytkG89QKqR/DN9HyXd0w0GX5JT+hMvuxQoqZIi4EjRyMg/eaXG8E4+z1QK6hHUY |
| polyfills.js | ZlVSoFeZ4Rl8BJTsjulnwRKxIPbb9acPMCKPB1hC9gPCGaFd7jusR1B90wXapEKz |
| runtime.js | YwZU+M0RWirxGUXpR82bV38PfKIXCa1y7oI8xk3Xo3I+rHG5znVHx9+02CX0YUS6 |

## 3. Hashwerte (SHA-256)

| | |
|---|---|
| secure-data-manager-package-1.4.4.4.zip | bb1ff024102c5564aef90386c0c01dc0ea67c8c19f193853aea5f3f923338d0e |
| direct-trust-tool-1.4.4.4.zip | b7c11631789dbb217d420b73c895f97834e157596d25015a38e0f453997d4f4d |
| file-cryptor-1.4.4.4-runnable.jar | cbfd46e1bcfb9f5a892bb6bc5cc28fb8dfabd9c9f57034f0d5391c372dcb2e66 |
| xml-signature-1.4.4.4.jar | 7983ed0f0e75536466cc6adcd5ffde630cffd6ab90016d1c810ba70fac81427d |
| control-component-runnable.jar | 910db2b50f058742a4a173b6e88efe2a773ec484e0f0d8a91dfcd421269061ec |
| voter-portal-1.4.4.4.zip | 923dfc84a9633fa6376bd8d1a8ea5c891311b001b9314f3b924e0ec42cd9afeb |
| voting-server-1.4.4.4-runnable.jar | c0a6300d343cedb38f10a418388b985dcf94627534292f46f7c74e72d4c03806 |
| crypto.ov-api.js | bd32848a0e07e2dccef465d47d4e295ed079be1dbee43f652bec1294fadede48 |
| crypto.ov-worker.js | 808104714101ddec957022f16c00f4aea7a5967f45da9d5512475db4c40fa5cc |
| main.js | 6f12c219ab543a03c73093a9b0c56ba14abe0cd83b7a5526b1b5c3e273f5c660 |
| polyfills.js | 4c6def3377663b9a437cb43a981b4c36edf5cbb78b956fd7ebbe1754d362860f |
| runtime.js | ea965b429bb063139b86122fa981ec206efd2aa0834f13154580522967d0ecc5 |

| | |
|---|---|
| verifier-assembly-1.5.4.3.zip | 6e5b770b4644a6deb81130f8f4803e9d2960ef8a60acc329225a3472967266a1 |
| data-integration-service-2.8.4.3.zip | d06b634d672f0f4960cd22831c57688217c3e794de79225259c80322b77fa9f9 |
| index.html | d96b7cdb46d3de04cca1257d151466df9d511cf78ad2abe250ff645acdc994cb |

## 4. Skript

```
#!/bin/bash
#Vorbereitungsarbeiten
#1. Sicherstellen, dass kein Java installiert ist (java --version, whereis java, dpkg --list | grep jdk)
#2. Docker installieren
#3. Wine installieren

#Erstellen der Verzeichnisse
mkdir -p ~/evoting
mkdir -p ~/evoting/evsource
mkdir -p ~/evoting/tools/java
mkdir -p ~/evoting/tools/maven
mkdir -p ~/evoting/tools/node

#Herunterladen und Entpacken der Tools
wget -c https://github.com/adoptium/temurin21-binaries/releases/download/jdk-21.0.4%2B7/OpenJDK21U-jdk_x64_linux_hotspot_21.0.4_7.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/java
wget -c https://nodejs.org/dist/v23.1.0/node-v23.1.0-linux-x64.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/node
wget -c https://archive.apache.org/dist/maven/maven-3/3.9.9/binaries/apache-maven-3.9.9-bin.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/maven

#Setzen der Umgebungsvariablen
export JAVA_HOME=~/evoting/tools/java
export NODE_HOME=~/evoting/tools/node
export MAVEN_HOME=~/evoting/tools/maven
export EVOTING_HOME="~/evoting/evsource"
export DOCKER_REGISTRY=registry.gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev
export PATH=$PATH:$JAVA_HOME/bin:$MAVEN_HOME/bin:$NODE_HOME:$NODE_HOME/bin
```

```
#Respositories klonen
cd ~/evoting/evsource
git config --global core.longpaths true
git clone -b e-voting-1.4.4.4 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting.git
git clone -b e-voting-libraries-1.4.4.3 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting-libraries.git
git clone -b crypto-primitives-ts-1.4.4.3 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives-ts.git
git clone -b crypto-primitives-1.4.4.3 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives.git
git clone -b data-integration-service-2.8.4.3 --single-branch git@gitlab.com:swisspost-evoting/e-voting/data-integration-service.git
git clone -b verifier-1.5.4.3 --single-branch git@gitlab.com:swisspost-evoting/verifier/verifier.git

#Kompilieren
cd ~/evoting/evsource
mvn clean install -f crypto-primitives -DskipTests -T 1.5C --no-transfer-progress
mvn clean install -f crypto-primitives-ts -DskipTests -T 1.5C --no-transfer-progress
mvn clean install -f e-voting-libraries -DskipTests -T 1.5C --no-transfer-progress
mvn clean install -f e-voting -DskipTests -T 1.5C --no-transfer-progress
mvn clean install -f data-integration-service -DskipTests -T 1.5C --no-transfer-progress
mvn clean install -f verifier -DskipTests -T 1.5C --no-transfer-progress

#Generieren der Haswerte
datum=$(date '+%Y%m%d_%H%M')
kanton=TG
dateiname="${datum}_${kanton}_ev_hashes.txt"
export dateiname
find ~/evoting/evsource -type f -name *secure-data-manager-*.zip -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource -type f -name direct-trust-tool-*.zip -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource -type f -name file-cryptor-*runnable.jar -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource -type f -name "xml-signature-*.jar"  -not -path "*archive-tmp*" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource -type f -name "control-component-runnable.jar" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target -type f -name voter-portal-*.zip -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voting-server/target -type f -name "voting-server*runnable.jar" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "crypto.ov-api.js" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "crypto.ov-worker.js" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "main.js" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "polyfills.js" -exec sha256sum {} \; >>~/evoting/$dateiname
```

```
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "runtime.js" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource -type f -name "verifier-assembly*.zip" -not -path "*archive-tmp*" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/data-integration-service/target -type f -name "data-integration-service*.zip" -not -path "*archive-tmp*" -exec sha256sum {} \;
>>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "index.html" -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "crypto.ov-api.js" -exec sh -c 'HASH=$(openssl dgst -sha384 -binary "$1" | openssl enc -base64); echo
"$HASH  $1" >> ~/evoting/"$dateiname" sh {} \;
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "crypto.ov-worker.js" -exec sh -c 'HASH=$(openssl dgst -sha384 -binary "$1" | openssl enc -base64);
echo "$HASH  $1" >> ~/evoting/"$dateiname" sh {} \;
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "main.js" -exec sh -c 'HASH=$(openssl dgst -sha384 -binary "$1" | openssl enc -base64); echo "$HASH
$1" >> ~/evoting/"$dateiname" sh {} \;
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "polyfills.js" -exec sh -c 'HASH=$(openssl dgst -sha384 -binary "$1" | openssl enc -base64); echo
"$HASH  $1" >> ~/evoting/"$dateiname" sh {} \;
find ~/evoting/evsource/e-voting/voter-portal/target/dist -name "runtime.js" -exec sh -c 'HASH=$(openssl dgst -sha384 -binary "$1" | openssl enc -base64); echo
"$HASH  $1" >> ~/evoting/"$dateiname" sh {} \;
```

Digital signiert Marius Kobi

SK RD

Datum: 17.11.2024

Thurgau