E-Voting-System Post R. 1.4.3.1: 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 2. Juli 2024, 09.41 Uhr, kompiliert und die Hashwerte der kompilierten Dateien gebildet.

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

crypto.ov-api.js	9alQr57CZH3awteoDnjYkHFhdgE7OQlCh+RWiTSx39sM989KfglvmYiaB/QEmQ8J
crypto.ov-worker.js	4v/AWGLOeuiktB5MpfVLlvJ+mWTSYH+UutYcS2GRm6UvyPtxeuf1vuYmqvraLblL
main.js	ZdZYowJf6LskiFMxr/vVvPN2WokgMlMvoNOGlOd+Q8iQzBPBo3/5p5VgDNy4M7in
polyfills.js	5FgKmq12RDumrub2BWyG7nG16Uhr3/uq/g58n/as3ABNJ449XfcgJAPk5bALy6r6
runtime.js	YwZU+M0RWirxGUXpR82bV38PfKIXCa1y7oI8xk3Xo3I+rHG5znVHx9+02CX0YUS6

3. Hashwerte (SHA-256)

secure-data-manager-package-1.4.3.1.zip	49ecc43612dd970c6c9e9ca23265752e04a4dc254a636ebdb1c7380a2b52fe8e
direct-trust-tool-1.4.3.1.zip	a280a22188febedd2ac0f669f8618d259235550c8c01e3bdd6a39cc06f47fcb2
file-cryptor-1.4.3.1-runnable.jar	a769c3cfc0eff4cbdd54858eb1035dd5b8d20bdb24808c3b9548505c48c7b512
xml-signature-1.4.3.1.jar	702f34b9aacaf4be3efbf246c5562742b2c456833dfd510a72c931e1863c7244
control-component-runnable.jar	29dcee5b8ddc161ada15b7c178a902d0b2089056758ca3caf6d426f3c6aad2ad
voter-portal-1.4.3.1.zip	84e4a35adf5642d74a4a5777295889d6ea06546b79bc9aec875baa2a9080e118
voting-server-1.4.3.1-runnable.jar	710d3684a872f5d42b40cde956beac6de52311eecea90708b79141453f36ad07
crypto.ov-api.js	bd32848a0e07e2dccef465d47d4e295ed079be1dbee43f652bec1294fadede48
crypto.ov-worker.js	02afbdd5beecdc2e5329c1df72443fa69f443fb8eda2762fa2e67dceb3633c2d
main.js	7b1baa8d37d560371a35b9ea41adeaab1a7ee78dff0db283930f257af7451111
polyfills.js	cc870ae271d9fc412e1ca30b5dd14926bbc4012150cf2989b334df7c02556ed6
runtime.js	ea965b429bb063139b86122fa981ec206efd2aa0834f13154580522967d0ecc5

verifier-assembly-1.5.3.1.zip	dc0289532cd7b2626742629553332 5afbd9742a02b2c5efeff9c1bf930406fae
data-integration-service-2.8.3.1.zip	d8c29ec1ea6fa0fb8ca029a6388d7c620c9bc731ee809ca714cd4737bb9e37d7
index.html	8c0e04bbd05f4dacd2e7c33bb3530648309a7b2120f9af81d68b799e47c48c38

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-21.0.3%2B9/OpenJDK21U-jdk_x64_linux_hotspot_21.0.3_9.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/java
wget -c https://nodejs.org/dist/v18.20.3/node-v18.20.3-linux-x64.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/node
wget -c https://archive.apache.org/dist/maven/maven-3/3.9.7/binaries/apache-maven-3.9.7-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-1.4.3.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting.git
git clone -b e-voting-libraries-1.4.3.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting-libraries.git
git clone -b crypto-primitives-ts-1.4.3.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives-ts.git
git clone -b crypto-primitives-1.4.3.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives.git
git clone -b data-integration-service-2.8.3.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/data-integration-service.git
git clone -b verifier-1.5.3.1 --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 {} \;
```

Staatskanzlei des Kantons Thurgau
Leiter Rechtsdienst

Digital signiert Marius Kobi

SK RD

Datum: 02.07.2024 **Thurgau**

lic. iur. Marius Kobi