E-Voting-System Post R. 1.3.4.0: 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 27. Februar 2024, 16.26 Uhr, kompiliert und die Hashwerte der kompilierten Dateien gebildet.

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

crypto.ov-api.js	7G9+mPlpCYXzspoKVxrbB9gypA8LQN3AcdpKeGkl0JF/fMDXMpwPEuJuy43BX6Eb
crypto.ov-worker.js	QOSlTdVQ16wedQrA4QJYcUx3mK/UdyZ1yMF4IJW/XSDxero/1BqlvPky8RxA0GVY
main.js	4s2RRwKzdg4h375qYVuBDzlwTwV0CKWEEEbEZ3LUmzaZ6qGLz+3XiLumaK4bSPGk
polyfills.js	ADkau9TRfRJgjPSietYkJtX6HXQO0rHfv3Grxl4mrWOXJStCoIp3NYVehF+jV2tb
runtime.js	dl5N3uRQoV0Gvcn8R0Iwi5XWok4Hru2MaccA0GUVXpz+8KUybTBAJ88CJCSpQGiR

3. Hashwerte (SHA-256)

secure-data-manager-package-1.3.4.0.zip	6db07137ec01ce724d3c80109186e95bf472eabf4feb55647c097b6f462c899e
config-cryptographic-parameters-tool-1.3.4.0.jar	4ba919acebd943820c3de714de709b63d3d30475eb4ff62956bbfb7f94b2a116
xml-signature-1.3.4.0.jar	1006d8befb1545d48e7d349e01a463fb334b53e435a79f72aa31c24955b9a158
control-component-runnable.jar	470ea62f1db85f6cf1e7e992f6568b2de79a56bcf0f99bf738f06180c2a327f6
voter-portal-1.3.4.0.zip	a569742ecbc452411777d8541760be500f9d705c797ff64aa7ea36062e4547b0
voting-server-1.3.4.0-runnable.jar	f437c3dbd3dd69a3addd266297600603c37e70a06cc1c756984fdbed45578ae4
crypto.ov-api.js	2faf9fae8d6bf75cc1ca06aa9e4f5f2ae4f220420e9d047d884b3cac7bdb26a3
crypto.ov-worker.js	9003a5a2dff12259282d571fc17084fed8c16bab40490510a71bed9309ff7370
main.js	d7564715dac28ecf972c1bc81e5e8980c7e94945b935445433c003def4e5d0f6
polyfills.js	34dfb6e7c7123409169c1b505914dcf3a93b020cddf6d920af248aba9325b99a
runtime.js	12aabd163c442aae3e55119869e24e35654310fb3de1ced5aaf68f6400956ef1
verifier-assembly-1.4.4.0.zip	f1148eec1f63532079130515cf4cdcdd34b87f2887ac1733cf0b21c9777f8520
data-integration-service-2.7.3.0.jar	107f010f9acca2d5bd8642d898922bfee0bf90171a7e9fe9a30481f4f3cbbc56
index.html	f9b36103452e1035dedc667bbdccbeb1f1deb5e8bfecd261cf6d298370deb8ab

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/temurin17-binaries/releases/download/jdk-17.0.10%2B7/OpenJDK17U-jdk_x64_linux_hotspot_17.0.10_7.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/java
wget -c https://nodejs.org/dist/v16.20.2/node-v16.20.2-linux-x64.tar.gz -O - | tar -xzv --strip-components 1 -C ~/evoting/tools/node
wget -c https://archive.apache.org/dist/maven/maven-3/3.9.1/binaries/apache-maven-3.9.1-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-1.3.4.0 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting.git
git clone -b e-voting-libraries-1.3.5.0 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting-libraries.git
git clone -b crypto-primitives-ts-1.3.4.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives-ts.git
```

```
git clone -b crypto-primitives-domain-1.3.4.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives-domain.git
git clone -b crypto-primitives-1.3.4.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives.git
git clone -b data-integration-service-2.7.3.0 --single-branch git@gitlab.com:swisspost-evoting/e-voting/data-integration-service.git
git clone -b verifier-1.4.4.0 --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-domain -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}_${kanton}_ev_hashes.txt"
export dateiname
find ~/evoting/evsource -type f -name *secure-data-manager-* -exec sha256sum {} \; >>~/evoting/$dateiname
find ~/evoting/evsource/e-voting/tools/config-cryptographic-parameters-tool/target -type f -name "config-cryptographic-parameters-tool*.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/$dateiname
find ~/evoting/evsource/data-integration-service/target -type f -name "data-integration-service*.jar" -not -path "*archive-tmp*" -exec sha256sum {} \;
>>~/evoting/$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: 27.02.2024

Thurgau

lic. iur. Marius Kobi