

E-Voting-System Post R. 1.4.5.1: 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 4. Juni 2025, 11.59 Uhr, kompiliert und die Hashwerte der kompilierten Dateien gebildet. Der Voting-Card-Print-Service (VCPS) wurde gemäss https://gitlab.com/swisspost-evoting/e-voting/voting-card-print-service/-/tree/master/Build?ref_type=heads kompiliert.

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

crypto.ov-api.js	9aIQr57CZH3awteoDnjYkHFhdgE7OQlCh+RWiTSx39sM989KfglvMViaB/QEmQ8J
crypto.ov-worker.js	aH7DSWjF47y2wfmy6Z/oLhoKyf/XX1e3CARXKmpNzhjU8z0DLidxCqima+Ts92o9
main.js	9EB/F/VskZI7O/1BiJaB7Uo7he2SHJ2cRqMIF3QkBMcgH09hW8obgTclU3Y+ZCNO
polyfills.js	8ROFW0jLZoYdR6/AhAIGAAut9MMXLqXdRIB1vkE+Lsza7PPacvsxiaqA+vSgrWD7
runtime.js	YwZU+M0RWirxGUXpR82bV38PfKIXCa1y7ol8xk3Xo3l+rHG5znVHx9+02CX0YUS6

3. Hashwerte (SHA-256)

secure-data-manager-package-1.4.5.1.zip	9d1558db3d0cb529b0e1daad9df5c82d80652b678a490bc1d8fea3fc050bf756
direct-trust-tool-1.4.5.1.zip	1c43ced075304cba7b26fcf69aeb768b1a00b17b5e416e41231a7932904d5ec1
file-cryptor-1.4.5.1-runnable.jar	efbb08a08b17fb43fbe137d0174ed0b201375aeba7995bfa404a0289c11ee20e
xml-signature-1.4.5.1.jar	1fb8c8c13d3c84915ff56a6160f141e3d1a45d1094ae0984f338f877b1afeeb4
control-component-runnable.jar	c08779a7ac2ab5b553620ecb644c7f86786740cc7b54733dede8202f5a260a66
voter-portal-1.4.5.1.zip	4f7ee005b5da4c418dc1be6013d1b6f129b8a02e9fe7625c9cff86f764a126fb
voting-server-1.4.5.1-runnable.jar	be4950d5f0e13c9e0a5d6ac6e5be68c0d9403adc55c6f4ccffac15ea39a8d105
crypto.ov-api.js	bd32848a0e07e2dccef465d47d4e295ed079be1dbee43f652bec1294fadede48
crypto.ov-worker.js	56e824f518ca039e94601a971deb017c2e49712882ffc363218c58d65a06a0da
main.js	ae5e23190fa99c38553371e79812eaae0dec772222ba007b3a4cce297496a7f

2/4

polyfills.js	8c84c677de73f127cb5f86f608357cc659f58caaca556499d75e0a941cca87cb
runtime.js	ea965b429bb063139b86122fa981ec206efd2aa0834f13154580522967d0ecc5
verifier-assembly-1.5.5.1.zip	61772671aaebc4100b3339248bfce8ff84cdd40cf0de241e435e92f0b3d435db
data-integration-service-2.8.5.1.zip	c9f10688777928e99f92ae17ecb12ded6e6cd60a20711f861588db82196e125
index.html	45687bd20d523d4005f9da30dff69568fe78d01b912497c50ffb986395dcad17
VCPS 3.2.0 (VotingCardPrintService.exe)	c1c0ffdc7bcc37d65c1ff441d5770e640030fe68ec13d1d50bc0cb60650473f9

4. Skript

```
#!/bin/bash
#Vorbereitungsarbeiten
#1. Sicherstellen, dass kein Java installiert ist (java --version, whereis java, dpkg --get-selections | 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-21.0.7%2B6/OpenJDK21U-jdk_x64_linux_hotspot_21.0.7_6.tar.gz -O - | tar -xvz --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 -xvz --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 -xvz --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
```



3/4

```
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-1.4.5.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting.git
git clone -b e-voting-libraries-1.4.5.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/e-voting-libraries.git
git clone -b crypto-primitives-ts-1.4.5.0 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives-ts.git
git clone -b crypto-primitives-1.4.5.1 --single-branch git@gitlab.com:swisspost-evoting/crypto-primitives/crypto-primitives.git
git clone -b data-integration-service-2.8.5.1 --single-branch git@gitlab.com:swisspost-evoting/e-voting/data-integration-service.git
git clone -b verifier-1.5.5.1 --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
```



4/4

```
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 {} \;
```