IVXV miksimisadapteri kasutusjuhend

Juhend

Versioon 1.0

20. september 2017

6 lk

Dok IVXV-JVA-1.0

Sisukord

PEATÜKK 1

Juhend miksneti ettevalmistamiseks ning kasutamiseks

1.1 Eeldused

Juhend on kirjeldatud kasutamiseks Ubuntu 16.04.1 LTS (Xenial Xerus) distributsiooniga. Me eeldame, et käske käivitatakse tavakasutaja õigustest, kellel on õigus käivitada *sudo* käsku. Lisaks eeldame järgmiste failide olemasolu kodukaustas:

Github repositooriumist (https://github.com/vvk-ehk/intcheck): * intcheck.py - tööriist kataloogide täielikkuse kontrolliks

IVXV tarnefailist:

- gmpmee.dirsha256sum - gmpmee kataloogi räsi
- vmgj.dirsha256sum - vmgj kataloogi räsi
- vcr.dirsha256sum - vcr kataloogi räsi
- vmn.dirsha256sum - vmn kataloogi räsi
- ivxv-verificatum-1.0-runner.zip - IVXV adapter Verificatumi kasutamiseks

Valimise korraldaja käest:

- data/bb-4.json - anonümiseeritud e-urn
- data/pub.pem - häälte krüpteerimiseks kasutatud võti

Kataloogis *data/* ei tohi olla ühtegi teist faili.

Pärast protsessi lõppu on kataloogis *data/* vajalikud järgnevad failid:

- shuffled.json - miksitud e-urn
- proof.zip - korrektse miksimise tõend

1.2 Verificatumi ehitamine

Kõigepealt tuleb paigaldada ehitamiseks vajalikud pakid:

```
sudo apt-get install --no-install-recommends -y autoconf autoconf␣
↪automake \
build-essential libgmp-dev libtool mercurial openjdk-8-jdk-headless␣
↪\
python2.7 unzip wget
```

Seejärel tuleb alla laadida Verificatumi lähtekood:

```
hg clone https://bitbucket.org/verificatum/gmpmee -r 875677a1961f
hg clone https://bitbucket.org/verificatum/vmgj -r f82d277ea43c
hg clone https://bitbucket.org/verificatum/vcr -r 0b64f5bf2747
hg clone https://bitbucket.org/verificatum/vmn -r f55a5b78b52b
```

Tekitame lähtekoodist puhtad arhiivid täielikkuse kontrolliks:

```
cd gmpmee
hg archive ../gmpmee-clean
cd ../vmgj
hg archive ../vmgj-clean
cd ../vcr
hg archive ../vcr-clean
cd ../vmn
hg archive ../vmn-clean
cd ..
```

Kontrollime Verificatumi lähtekoodi täielikkus:

```
chmod +x ./intcheck.py
./intcheck.py verify gmpmee-clean gmpmee.dirsha256sum
./intcheck.py verify vmgj-clean vmgj.dirsha256sum
./intcheck.py verify vcr-clean vcr.dirsha256sum
./intcheck.py verify vmn-clean vmn.dirsha256sum
```

Ehitame *gmpmee*:

```
cd gmpmee-clean/
make -f Makefile.build
./configure
make
sudo make install
```

Ehitame *vmgj*:

```
cd ../vmgj-clean/
make -f Makefile.build
./configure
```

```
make
sudo make install
```

Ehitame *vcr*:

```
cd ../vcr-clean/
make -f Makefile.build
./configure --enable-vmgj
make
sudo make install
```

Ehitame *vmn*:

```
cd ../vmn-clean/
make -f Makefile.build
./configure
make
sudo make install
```

1.3 Adapteri ettevalmistamine ja käivitamine

Pakime lahti IVXV Verificatumi adapteri ja käivitusskripti:

```
cd ..
unzip ivxv-verificatum-1.0-runner.zip
```

Kopeerime Verificatumi teegid adapteri väliste teekide kataloogi:

```
cp /usr/local/share/java/verificatum-vmgj-1.2.0.jar mixer/lib/
 ↪verificatum-vmgj.jar
cp /usr/local/share/java/verificatum-vcr-vmgj-3.0.2.jar mixer/lib/
 ↪verificatum-vcr-vmgj.jar
cp /usr/local/share/java/verificatum-vmn-3.0.2.jar mixer/lib/
 ↪verificatum-vmn.jar
cp /usr/local/lib/libgmpmee.so.0.0.0 mixer/lib/libgmpmee.so.0
cp /usr/local/lib/libvmgj-1.2.0.so mixer/lib/libvmgj-1.2.0.so
```

Käivitame Verificatumi miksneti:

```
cd data
../mixer/bin/mix.py --pubkey pub.pem --ballotbox bb-4.json \
--shuffled shuffled.json --proof-zipfile proof.zip shuffle
```

1.4 Miksimistõendi verifitseerimine

Verificatumi adapteri abil saab miskimistõendit ka verifitseerida:

```
cd ..
mkdir verify
cp data/proof.zip verify
cd verify
../mixer/bin/mix.py verify --proof-zipfile proof.zip
```