Dlhodobé sledovanie parametrov QKD a export kľúčov

Subtitle

Ing. Adrián Tomašov

utko@vut

19.10.2021

Osnova

1. Dlhodobé sledovanie parametrov QKD
   - Poskytnuté riešenie – Cockpit
   - Návrh vlastného riešenia

2. Export kľúča a systém KEMS
   - Inštalácia a nasadenie
   - Nastavenie systému
   - Test – Export kľúča

Dlhodobé sledovanie parametrov QKD

Poskytnuté riešenie – Cockpit

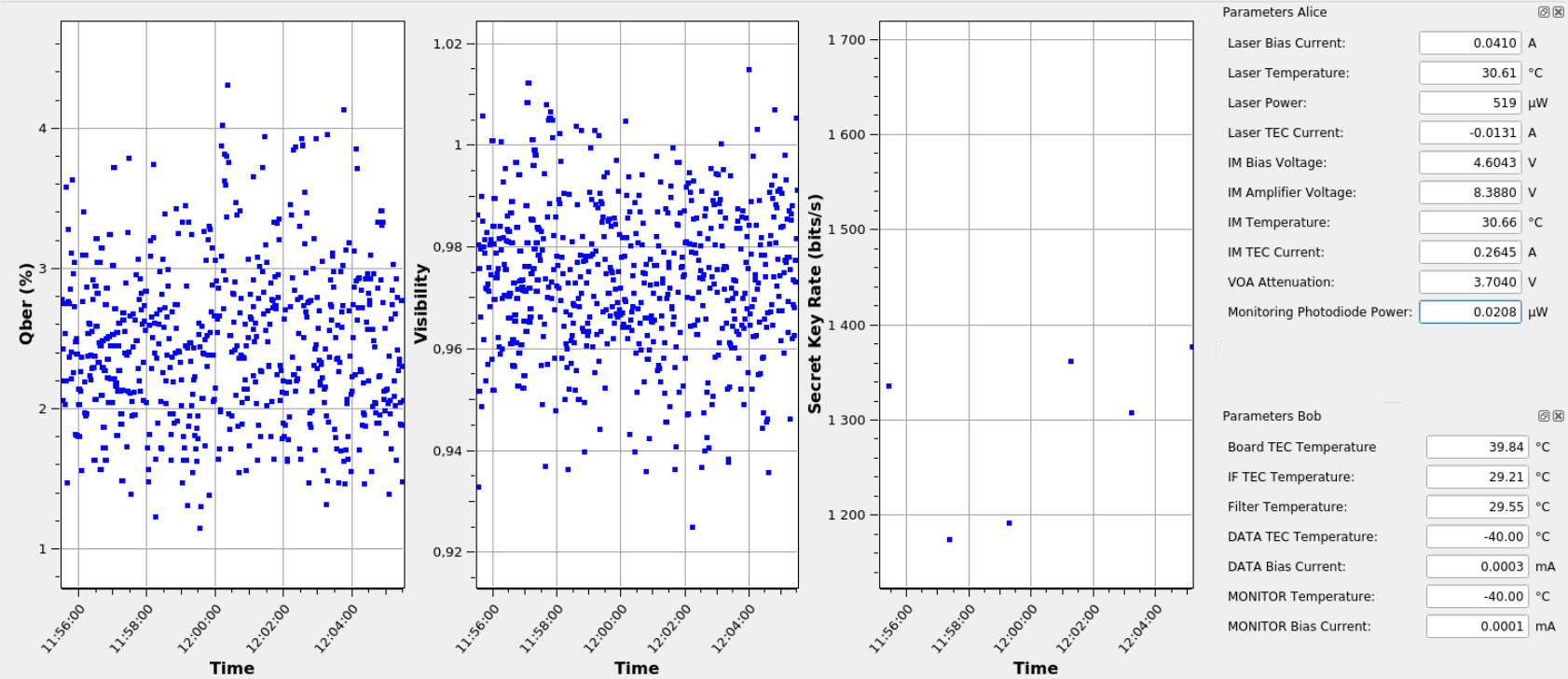
Použitie:

- Sledovanie parametrov QKD systému
- Aktuálne dáta zobrazí a uloží do CSV
- Sledovanie inicializačného procesu QKD

Nedostatky:

- Limitácia prostredia
- Chýba možnosť úpravy
- Chýba dlhodobé sledovanie a zobrazenie parametrov

IDQ Cockpit



Obr.: Sledovanie parametrov QKD systému pomocou program Cockpit od IDQ.

Návrh vlastného riešenia

Dátový server

Vytvorenie a inštalácia sady programov na náš dátový server.

Zámer na odstránenie limitácií:

- Závislosť OS
- Ukladanie dát
- Dostupnosť

Použité technológie:

- Python3
- SystemD
- SNMPv3
- InfluxDB
- Grafana

Náhľad na graf z Grafany

Obr.: Graf kvantovej bitovej chybovosti v Grafane.

Sledované metriky

Sledované:

- Prenosová rýchlosť kľúča
- Kvantová chybovosť
- Viditeľnosť

Možno rozšíriť o:

- Stav QKD
- Kompresný pomer
- Výkon lasera
- Počet detekcií

Grafana

Obr.: Zobrazenie celého Grafana dashboard

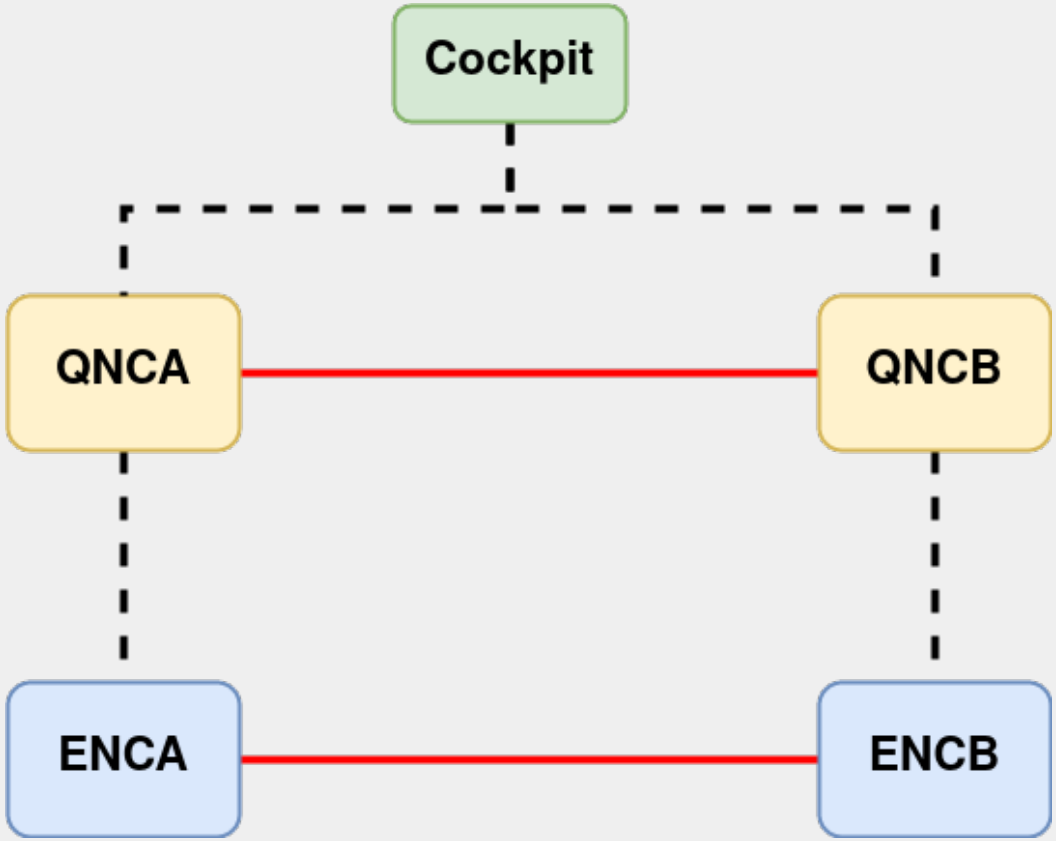
Export kľúča a systém KEMS

Inštalácia

Inštalácia:

1. Inštalácia potrebných aplikácií
2. Import docker imagov
3. Úprava deployment scriptu pre automatické zapnutie po reboote
4. `docker compose up`
5. Povoliť porty vo firewall

Diagram systému



Obr.: Logické zapojenie systému

Nastavenie systému

Nastavenie systému KEMS

1. Vytvorenie skupiny v KEMS
2. Pridanie Clavis3 zariadení (sériové čísla, IP adresy)
3. Vytvoriť kvantový kanál
4. Pridanie informácií o šifrátoroch + použité ETSI REST
5. Pridanie certifikátov (verejných kľúčov)
6. Nastavenie zabezpečenej cesty

Nastavenie systému

Nastavenie systému KEMS

1. Vytvorenie skupiny v KEMS
2. Pridanie Clavis3 zariadení (sériové čísla, IP adresy)
3. Vytvoriť kvantový kanál
4. Pridanie informácií o šifrátoroch + použité ETSI REST
5. Pridanie certifikátov (verejných kľúčov)
6. Nastavenie zabezpečenej cesty

Použitie

KEMS je potrebný len pre konfiguráciu a nastavenie. Na beh kvantového systému nie je potrebný.

Test – Export kľúča

```
NewKey=$(curl --cert /root/qkd_certs/ENCB-cert.pem  --key /root/qkd_certs/ENCB-key.pem
    --cacert /root/qkd_certs/ca-cert.pem -k https://$KMSM_IP/api/v1/keys/ENCA/enc_keys)
KeyID=$(echo $NewKey | jq '.keys[0].key_ID' | cut -d '"' -f 2)
echo "        Found ID: $KeyID"
```

Test – Export kľúča

```
NewKey=$(curl --cert /root/qkd_certs/ENCB-cert.pem  --key /root/qkd_certs/ENCB-key.pem
    --cacert /root/qkd_certs/ca-cert.pem -k https://$KMSM_IP/api/v1/keys/ENCA/enc_keys)
KeyID=$(echo $NewKey | jq '.keys[0].key_ID' | cut -d '"' -f 2)
echo "        Found ID: $KeyID"


echo "    Get Key with ID from slave"
Rep=$(curl --cert /root/qkd_certs/ENCA-cert.pem  --key /root/qkd_certs/ENCA-key.pem
    --cacert /root/qkd_certs/ca-cert.pem -X POST -H 'Content-Type:application/json'
    -d "{\"key_IDs\":[{\"key_ID\":\"$KeyID\"}]}"
    -k https://$KMSS_IP/api/v1/keys/ENCB/dec_keys)
Key=$(echo $Rep | jq '.keys[0].key' | cut -d '"' -f 2)
KeyIDSlave=$(echo $Rep | jq '.keys[0].key_ID' | cut -d '"' -f 2)
echo "        Found Key: $Key"
echo "        Found ID: $KeyIDSlave"
```

Test – Výstup

```
Get key round
    Get New Key from master
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   145  100   145    0     0   1559      0 --:--:-- --:--:-- --:--:--  1559
        Found ID: 7122cbb0-d2ae-4d02-be58-ce82bab321d6
```

Test – Výstup

```
Get key round
    Get New Key from master
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   145  100   145    0     0   1559      0 --:--:-- --:--:-- --:--:--  1559
       Found ID: 7122cbb0-d2ae-4d02-be58-ce82bab321d6


    Get Key with ID from slave
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   208  100   145  100    63   1907    828 --:--:-- --:--:-- --:--:--  2736
       Found Key: /dg734O+WCmGKfchJJ2SkWQxcEzP4Wv4I8JGiGY+sUY=
       Found ID: 7122cbb0-d2ae-4d02-be58-ce82bab321d6
```

Ďakujem za pozornosť!
Q&A