

Politechnika Wrocławska
Wydział Elektroniki

Kierunek: Cyberbezpieczeństwo

Ochrona centrów danych

Keylime



Politechnika Wrocławska

Aneta Prządka
Anna Płęcha
Krzysztof Bocian

Wrocław, 2022

Spis treści

1. Wstęp	2
2. Etapy zadania	2
3. Podsumowanie	11

1.Wstęp

Celem tego laboratorium jest utworzenie weryfikacji zaufanego stanu zasobu chmurowego na podstawie rejestrów PCR. W ramach tych zajęć zainstalujemy serwisy Keylime, wygenerujemy certyfikaty EK, uruchomimy serwisy Keylime, dodamy zasoby certyfikowane oraz zweryfikujemy poprawność certyfikacji. Wymagane były działające dbus oraz jeden z zainstalowanych wcześniej symulatorów tpm.

2.Etapy zadania

2.1 Pierwszym krokiem projektu jest instalacja Keylime. Zrobiliśmy to przy pomocy następujących kroków:

- git clone <https://github.com/keylime/keylime.git>

```
root@a860e66386de:/# git clone https://github.com/keylime/keylime.git
Cloning into 'keylime'...
remote: Enumerating objects: 5179, done.
remote: Counting objects: 100% (118/118), done.
remote: Compressing objects: 100% (76/76), done.
remote: Total 5179 (delta 62), reused 62 (delta 40), pack-reused 5061
Receiving objects: 100% (5179/5179), 13.57 MiB | 2.27 MiB/s, done.
Resolving deltas: 100% (3665/3665), done.
root@a860e66386de:/# cd keylime
root@a860e66386de:/keylime#
```

Rys 1. Pobieranie repozytorium Keylime

- cd keylime
- git checkout v6.2.0
- python3 -m pip . -r requirements.txt

```
Successfully installed keylime-0.0.0
root@db36c1caa8f2:/keylime#
```

Rys 2. Wykonanie komendy python3 -m pip . -r requirements.txt - instalacja keylime.

Dodatkowo do poprawnej instalacji potrzebowaliśmy uprzednio następujących komend:

- apt-get install python3-pip
- apt-get install swig

2.2 Następnie należało wygenerować certyfikat EK. Do wygenerowania certyfikatu niezbędna była łątka, więc zainstalowano repozytorium keylime_EK.

```
root@900105369fc5:/# git clone https://github.com/CBE-OCD-2021-22/keylime_EK.git
Cloning into 'keylime_EK'...
Username for 'https://github.com': AniaPlecha
Password for 'https://AniaPlecha@github.com':
remote: Enumerating objects: 3, done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 3
Unpacking objects: 100% (3/3), 1.85 KiB | 1.85 MiB/s, done.
root@900105369fc5:/# cd keylime_EK
```

Rys 3. Pobieranie repozytorium keylime_EK.

Patchowanie nastąpiło z użyciem komendy:

```
patch -p1 -i /keylime_EK/tpm2_ek_cert_generator.patch -d tpm2_ek_cert_generator
```

(komenda podana w instrukcji zawierała błąd dotyczący lokalizacji)

Następnie wygenerowano certyfikat komendą make.

2.3 Uruchomienie serwisów Keylime

- keylime_verifier - stale weryfikuje stan integralności komputera, na którym działa agent.

```
root@900105369fc5:/# keylime_verifier
Using config file /etc/keylime.conf
2022-01-18 17:51:02.159 - keylime.keylime_db - INFO - database_url is not set,
using multi-parameter database configuration options
2022-01-18 17:51:02.270 - keylime.keylime_db - INFO - database_url is not set,
using multi-parameter database configuration options
2022-01-18 17:51:02.271 - alembic.env - INFO - Migrating database cloud_verifie
r
2022-01-18 17:51:02.272 - alembic.runtime.migration - INFO - Context impl SQLit
eImpl.
2022-01-18 17:51:02.272 - alembic.runtime.migration - INFO - Will assume non-tr
ansactional DDL.
2022-01-18 17:51:02.289 - keylime.cloudverifier - INFO - Starting Cloud Verifie
r (tornado) on port 8881, use <Ctrl-C> to stop
2022-01-18 17:51:02.289 - keylime.cloudverifier - INFO - Current API version 1.
0
2022-01-18 17:51:02.290 - keylime.cloudverifier_common - INFO - Setting up TLS.
..
2022-01-18 17:51:02.290 - keylime.cloudverifier_common - INFO - Generating a ne
w CA in /var/lib/keylime/cv_ca and a client certificate for connecting
2022-01-18 17:51:02.290 - keylime.cloudverifier_common - INFO - use keylime_ca
-d /var/lib/keylime/cv_ca to manage this CA
2022-01-18 17:51:02.291 - keylime.cloudverifier_common - WARNING - CAUTION: usi
ng default password for CA, please set private_key_pw to a strong password
2022-01-18 17:51:02.585 - keylime.ca_impl_openssl - WARNING - CRL creation with
openssl is not supported
2022-01-18 17:51:02.587 - keylime.ca-util - INFO - CA certificate created succe
ssfully in /var/lib/keylime/cv_ca
```

Rys 4. Uruchomienie serwisu keylime_verifier.

- keylime_registrar - baza danych wszystkich agentów zarejestrowanych w Keylime i przechowująca klucze publiczne dostawców TPM.

```
root@900105369fc5:/# keylime_registrar
Using config file /etc/keylime.conf
2022-01-18 17:51:46.329 - keylime.keylime_db - INFO - database_url is not set,
using multi-parameter database configuration options
2022-01-18 17:51:46.442 - keylime.keylime_db - INFO - database_url is not set,
using multi-parameter database configuration options
2022-01-18 17:51:46.448 - alembic.env - INFO - Migrating database registrar
2022-01-18 17:51:46.449 - alembic.runtime.migration - INFO - Context impl SQLit
eImpl.
2022-01-18 17:51:46.449 - alembic.runtime.migration - INFO - Will assume non-tr
ansactional DDL.
2022-01-18 17:51:46.463 - keylime.cloudverifier_common - INFO - Setting up TLS.
..
2022-01-18 17:51:46.464 - keylime.registrar - INFO - Starting Cloud Registrar S
erver on ports 8890 and 8891 (TLS) use <Ctrl-C> to stop
2022-01-18 17:51:46.464 - keylime.registrar - INFO - Current API version 1.0
2022-01-18 17:52:27.289 - keylime.tpm - INFO - TPM2-TOOLS Version: 5.2
2022-01-18 17:52:27.289 - keylime.registrar - WARNING - Agent d432fbb3-d2f1-4a9
7-9ef7-75bd81c00000 did not submit an ekcert
2022-01-18 17:52:27.300 - keylime.tpm - INFO - Encrypting AIK for UUID d432fbb3
-d2f1-4a97-9ef7-75bd81c00000
2022-01-18 17:52:27.316 - keylime.registrar - INFO - POST returning key blob fo
r agent_id: d432fbb3-d2f1-4a97-9ef7-75bd81c00000
2022-01-18 17:52:27.514 - keylime.registrar - INFO - PUT activated: d432fbb3-d2
f1-4a97-9ef7-75bd81c00000
2022-01-18 18:01:12.734 - keylime.registrar - WARNING - GET returning 404 respo
nse agent_id d432fbb3-d2f1-4a97-9ef7-75bd81c00000 not found
```

Rys 5. Uruchomienie serwisu keylime_registrar.

- keylime_agent

```

root@900105369fc5:/# keylime_agent
Using config file /etc/keylime.conf
2022-01-18 17:52:26.533 - keylime.tpm - INFO - TPM2-TOOLS Version: 5.2
2022-01-18 17:52:26.580 - keylime.cloudagent - WARNING - Measurement list path
/sys/kernel/security/tpm0/binary_bios_measurements not accessible by agent. Any
attempt to instruct it to access this path - via "keylime_tenant" CLI - will r
esult in agent process dying
2022-01-18 17:52:26.580 - keylime.cloudagent - WARNING - Measurement list path
/sys/kernel/security/ima/ascii_runtime_measurements not accessible by agent. An
y attempt to instruct it to access this path - via "keylime_tenant" CLI - will
result in agent process dying
2022-01-18 17:52:26.591 - keylime.tpm - INFO - TPM2-TOOLS Version: 5.2
2022-01-18 17:52:26.661 - keylime.tpm - INFO - Taking ownership with config pro
vided TPM owner password
2022-01-18 17:52:26.831 - keylime.tpm - INFO - TPM Owner password confirmed: ke
ylime
2022-01-18 17:52:27.061 - keylime.tpm - WARNING - No EK certificate found in TP
M NVRAM
2022-01-18 17:52:27.272 - keylime.cloudagent - INFO - Agent UUID: d432fbb3-d2f1
-4a97-9ef7-75bd81c00000
2022-01-18 17:52:27.317 - keylime.registrar_client - INFO - Agent registration
requested for d432fbb3-d2f1-4a97-9ef7-75bd81c00000
2022-01-18 17:52:27.500 - keylime.tpm - INFO - AIK activated.
2022-01-18 17:52:27.514 - keylime.registrar_client - INFO - Registration activa
ted for agent d432fbb3-d2f1-4a97-9ef7-75bd81c00000.
2022-01-18 17:52:27.675 - keylime.cloudagent - INFO - Starting Cloud Agent on 1
27.0.0.1:9002 with API version 1.0. Use <Ctrl-C> to stop
2022-01-18 17:52:27.676 - keylime.revocation_notifier - INFO - Waiting for revo

```

Rys 6. Uruchomienie serwisu keylime_agent.

2.4 Dodanie zasobu certyfikowanego (wymagało utworzenia pliku filetosend z dowolną zawartością tekstową)

```

root@900105369fc5:/# keylime_tenant -c add -t 127.0.0.1 -v 127.0.0.1 -u d432fbb
3-d2f1-4a97-9ef7-75bd81c00000 -f filetosend
Using config file /etc/keylime.conf
2022-01-23 05:48:42.115 - keylime.tpm - INFO - TPM2-TOOLS Version: 5.2
2022-01-23 05:48:42.119 - keylime.tenant - INFO - Setting up client TLS in /var
/lib/keylime/cv_ca
2022-01-23 05:48:42.119 - keylime.registrar_client - WARNING - TLS is enabled.
2022-01-23 05:48:42.119 - keylime.registrar_client - INFO - Setting up client T
LS...
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWa
rning: Unverified HTTPS request is being made to host '127.0.0.1'. Adding certi
ficate verification is strongly advised. See: https://urllib3.readthedocs.io/en
/latest/advanced-usage.html#ssl-warnings
warnings.warn(
2022-01-23 05:48:42.132 - keylime.tenant - INFO - TPM PCR Mask from policy is 0
x408000
2022-01-23 05:48:42.132 - keylime.tenant - INFO - TPM PCR Mask from policy is 0
x808000
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWa
rning: Unverified HTTPS request is being made to host '127.0.0.1'. Adding certi
ficate verification is strongly advised. See: https://urllib3.readthedocs.io/en
/latest/advanced-usage.html#ssl-warnings
warnings.warn(
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:999: InsecureRequestWa
rning: Unverified HTTPS request is being made to host '127.0.0.1'. Adding certi
ficate verification is strongly advised. See: https://urllib3.readthedocs.io/en
/latest/advanced-usage.html#ssl-warnings
warnings.warn(

```

Rys 7. Dodanie zasobu certyfikowanego.

2.5 Weryfikacja poprawności certyfikacji - serwisy działające poprawnie.

```
root@900105369fc5:/# tpm2_pcrread sha256
sha256:
 0 : 0x0000000000000000000000000000000000000000000000000000000000000000
 1 : 0x0000000000000000000000000000000000000000000000000000000000000000
 2 : 0x0000000000000000000000000000000000000000000000000000000000000000
 3 : 0x0000000000000000000000000000000000000000000000000000000000000000
 4 : 0x0000000000000000000000000000000000000000000000000000000000000000
 5 : 0x0000000000000000000000000000000000000000000000000000000000000000
 6 : 0x0000000000000000000000000000000000000000000000000000000000000000
 7 : 0x0000000000000000000000000000000000000000000000000000000000000000
 8 : 0x0000000000000000000000000000000000000000000000000000000000000000
 9 : 0x0000000000000000000000000000000000000000000000000000000000000000
10 : 0x0000000000000000000000000000000000000000000000000000000000000000
11 : 0x0000000000000000000000000000000000000000000000000000000000000000
12 : 0x0000000000000000000000000000000000000000000000000000000000000000
13 : 0x0000000000000000000000000000000000000000000000000000000000000000
14 : 0x0000000000000000000000000000000000000000000000000000000000000000
15 : 0x0000000000000000000000000000000000000000000000000000000000000000
16 : 0xAD8506E332E7699D2243E76610676C3CF4036B1AE50309EB18F39E9FB11D4BEA
17 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
19 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
20 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
21 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
22 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
23 : 0x0000000000000000000000000000000000000000000000000000000000000000
```

Rys 7. Odczytanie rejestrów PCR przed zmianami.

2.6 Negatywna weryfikacja (zmiana oczekiwanych rejestrów => odwołanie poświadczenia)

```
root@900105369fc5:/# cat skrypt.sh
#!/bin/bash
for ((c=1; c<=16; c++))
do
tpm2_pcrextend $c:sha1=`tpm2_getrandom 20 |xxd -ps`
tpm2_pcrextend $c:sha256=e6baf5b7c5523230e03d1d00983b7286a82646840d3dd68292edf9
e721a61234
done
```

Rys 8. Utworzenie skryptu zmieniającego rejestry PCR.


```

root@900105369fc5:/# tpm2_pcrread sha256
sha256:
 0 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 1 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 2 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 3 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 4 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 5 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 6 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 7 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 8 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 9 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
10 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
11 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
12 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
13 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
14 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
15 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
16 : 0xAD8506E332E7699D2243E76610676C3CF4036B1AE50309EB18F39E9FB11D4BEA
17 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
19 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
20 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
21 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
22 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
23 : 0x0000000000000000000000000000000000000000000000000000000000000000

```

Rys 9. Nadpisane rejestry PCR sha256, Anna.

```

root@683ebde1f28a:/# tpm2_pcrread sha256
sha256:
 0 : 0x0000000000000000000000000000000000000000000000000000000000000000
 1 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 2 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 3 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 4 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 5 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 6 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 7 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 8 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
 9 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
10 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
11 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
12 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
13 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
14 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
15 : 0xFA5E3714A460081A95FB59F639C4F0A0672A91BB6D30A0756030495EC51ABE24
16 : 0x9D9874EE1F8AE346E224D604978178F5BA70DACF89B51834A6A706F9A22C0B70
17 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18 : 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

"683ebde1f28a" 19:26 26-Jan-22

Rys 10. Nadpisane rejestry PCR sha256, Aneta.


```

root@ba9e2699020d:/# tpm2_pcrread sha256
sha256:
 0 : 0x0000000000000000000000000000000000000000000000000000000000000000
 1 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 2 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 3 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 4 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 5 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 6 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 7 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 8 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
 9 : 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
10: 0xD3EE936003B71FF85FDAE6027267409226F97C48B528FA774F5E4AE0AB90E134
11: 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
12: 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
13: 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
14: 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
15: 0x70BC134F86F2D694CE338D7660199EBB8CE263683713FE4A39952CAB09F01CE7
16: 0xD0BD695D2FCB1B3208B180B159605A5F769781853300AFFA911622D79BCECF863
17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

Rys.11 Nadpisane rejestry PCR sha256, Krzysztof.

```

23: 0x0000000000000000000000000000000000000000000000000000000000000000
root@900105369fc5:/# tpm2_pcrread sha1
sha1:
 0 : 0x0000000000000000000000000000000000000000000000000000000000000000
 1 : 0x481E051ED2F42BF4F73C0B9141C6DB5E3AE20257
 2 : 0xE152C0D63C936BE1E3BD41158810CD4C6868BE29
 3 : 0xB3FBE89D0A0152C396FC6DAD324DCAF3CE87280C
 4 : 0x8EADD0DE6720135C162AB3674943A12978DFF2F8
 5 : 0xCAC17614C2A276471E643CC2ACFEC8B62B7A2AA6
 6 : 0x2C625A3A7F209B2133DD4071E6FA8D9CA0B69E4F
 7 : 0x7AB5136A95AE41DCE427287C9DB119D6D82E3D64
 8 : 0xB4F44048175D85379A9AF968D1FFA01D27ED29CF
 9 : 0xCC6AC1E6622258275C0BF878B8B06D532FACB32
10: 0xF492E2EEF0547DB68B156C0B57B884FC534BE524
11: 0x0991CA430CFCD0D6592D6D4D9C80E3602E880063
12: 0x2CCEC1347AEA16E99A85298CEF302F671405A539
13: 0x1B21CBE0429840382F468F9E0D103AEE688DF2E2
14: 0x53A59ABC595F595A5C3E352A2BF4586F683C6820
15: 0xBB8F30EDD694E2DF7118F405A72721C2D617BFD8
16: 0x0000000000000000000000000000000000000000000000000000000000000000
17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
19: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
20: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
21: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
22: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
23: 0x0000000000000000000000000000000000000000000000000000000000000000

```

Rys 12. Nadpisane rejestry PCR sha1, Anna.

```
root@683ebde1f28a:/# tpm2_pcrread sha1
sha1:
0 : 0x0000000000000000000000000000000000000000000000000000000000000000
1 : 0xC7AD11557327EC68870EB1144A12F8955E2BC38E
2 : 0xA7999E264E29302CBEE48CD645AFC0D897E46E65
3 : 0xFE6281DFEB2CE72C12BD40F2E5C26751A913DB68
4 : 0x2770D588B646FC2957ECBA1820D6984B2C760C88
5 : 0xD5CE6FD96A1397DD7374E4EF058CB26C85AC2E90
6 : 0xECEC8AE9F71E6C68A120F2EF08F185939981B775
7 : 0x4D00AE942B081A61BBB8B9B96041FAD5395FF287
8 : 0xFFFFF28E177FF9D9AE7EC98E072C40A3498BD663C
9 : 0xC5F5CEBA770B0FCF9ACF6AA8BBE1717F08BBA7BC
10: 0x33DBA2E8B825AC1809F75B6B2D60C24E6CFEC840
11: 0xC70C30EAC45F9E34116B7DB0F6BC50DF05BE2F5B
12: 0xE35F3C335DFE24EB148F19279F9F2A647B14344F
13: 0xC3E73B81BFCA7C1DFA7F74B518F39CF450BAC8CB
14: 0x2A9BDBE09D2010386AF1DC46ACEC98424766CE29
15: 0x584927D97FBBBC39597DBF73F2DBEA79B4CB58CB7
16: 0x0000000000000000000000000000000000000000000000000000000000000000
17: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
18: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Rys 13. Nadpisane rejestry PCR sha1, Aneta.

```
root@ba9e2699020d:/# tpm2_pcrread sha1
sha1:
0 : 0x0000000000000000000000000000000000000000000000000000000000000000
1 : 0x23C8720B1FF384C9BF8F3BB4BDBC7A78B0BFD849
2 : 0x337EE920AACFA986CB30C51462BFAB48CB7D6E20
3 : 0x4D129D770439CA506B0D78405D3DAA22B604468C
4 : 0xDA5861F7B8E65A3D292576795474D50617109809
5 : 0x2568D46F6154F8835B65F1F00CDD11126021CE60
6 : 0xDF7886CF170FDA6E5E92EDF0D6E825EBDDF160BD
7 : 0x3066CF812644499EBCAA3D813E04FC950924CCBD
8 : 0xB1A56D42ECA885C135F907E008B2BE32C831E6B5
9 : 0x25C5D89D2D5E900B24D49A6F18BB07B3F986213E
10: 0xD9BA4D884843127CC7F520DD86C0D5050A4185D1
11: 0xE171F06BFEB0E5CCBD238923B3EA934246578893
12: 0x569B012A5B73F477E665461D7B66E03CB606C0FB
13: 0x979179D12FDE3F82BF91521B3F345FB2FE7AF5E6
14: 0xF53CD258B516BE42E35DB4029D538ECC4DC20BAA
15: 0xCAE3DB146496A14751EC0988C69913E49D9C21EB
16: 0x5CA1570AFD069834ECB1F5B501D716EBA8F1588A
```

Rys. 14 Nadpisane rejestry PCR sha1, Krzysztof.

- Zmiana poświadczeń względem oczekiwanych spowodowało zatrzymanie działania serwisów z komunikatem zaprezentowanym poniżej (na przykładzie keylime_verifier):

```

AWARNING: TypeDecorator JSONPickleType() will not produce a cache key because t
he ``cache_ok`` attribute is not set to True. This can have significant perfor
mance implications including some performance degradations in comparison to pri
or SQLAlchemy versions. Set this attribute to True if this type object's state
is safe to use in a cache key, or False to disable this warning. (Background o
n this error at: https://sqlalche.me/e/14/cprf)
    session.query(VerfierMain).filter_by(
2022-01-23 06:20:04.350 - keylime.tpm - ERROR - PCR #15: fa5e3714a460081a95fb59
f639c4f0a0672a91bb6d30a0756030495ec51abe24 from quote does not match expected v
alue ['0000000000000000000000000000000000000000000000000000000000000000', '0000000000000000000000000000000000000000000000000000000000000000', '0000000000000000000000000000000000000000000000000000000000000000', '0000000000000000000000000000000000000000000000000000000000000000']
/usr/local/lib/python3.8/dist-packages/keylime/cloud_verifier_tornado.py:823: S
AWARNING: TypeDecorator JSONPickleType() will not produce a cache key because t
he ``cache_ok`` attribute is not set to True. This can have significant perfor
mance implications including some performance degradations in comparison to pri
or SQLAlchemy versions. Set this attribute to True if this type object's state
is safe to use in a cache key, or False to disable this warning. (Background o
n this error at: https://sqlalche.me/e/14/cprf)
    session.query(VerfierMain).filter_by(
2022-01-23 06:20:04.373 - keylime.cloudverifier - WARNING - Agent d432fbb3-d2f1
-4a97-9ef7-75bd81c00000 failed, stopping polling
2022-01-23 06:20:04.559 - keylime.revocation_notifier - INFO - Sending revocati
on event to listening nodes...

```

Rys 15. Błąd działania serwisu keylime verifier wywołany zmianą rejestrów, Anna.

[illegible]

Rys 16. Błąd działania serwisu keylime verifier wywołany zmianą rejestrów, Aneta.

[illegible]

Rys.17 Błąd działania serwisu *keylime verifier* wywołany zmianą rejestrów,

Krzysztof.

3.Podsumowanie

Keylime to skalowalny system zaufania typu open source wykorzystujący technologię TPM. Zapewnia elastyczne ramy do zdalnej atestacji dowolnego danego PCR (Rejestr Konfiguracji Platformy). Użytkownicy mogą tworzyć własne, dostosowane akcje, które zostaną uruchomione, gdy maszyna nie przejdzie oczekiwanych pomiarów.

Celem tego laboratorium było utworzenie weryfikacji zaufanego stanu zasobu chmurowego na podstawie rejestrów PCR. W ramach tych zajęć zainstalowano oraz uruchomiono serwis Keylime, wygenerowano certyfikat EK, dodano zasoby certyfikowane oraz zweryfikowano poprawność certyfikacji metodą pozytywną oraz negatywną.

W trakcie instalacji napotkano kilka problemów, które udało się ostatecznie rozwiązać. Pierwszym problemem była zła komenda patch, która zawierała złą ścieżkę, następnie należało uruchomić ponownie kontener z parametrem `--tmpfs /var/lib/keylime/secure` (wykorzystano do tego obraz utworzony na bazie kontenera używanego do tej pory komendą `commit` (brak `dockerfile`)). Na nowo utworzonym kontenerze udało się stworzyć certyfikat, uruchomić `dbus`, symulator `tpm` oraz serwis `keylime`. Po dodaniu zasobu certyfikowanego (wymagało utworzenia pliku `filetosend` z dowolną zawartością tekstową) nastąpiła weryfikacja pozytywna - sprawdzenie rejestrów PCR oraz stanu uruchomionych serwisów. Następnie nadpisano rejestry poprzez utworzenie skryptu (Rys 8.). - problem z brakiem edytora tekstowego rozwiązano komendą `echo`. Ponownie sprawdzono rejestry PCR, czy zostały prawidłowo nadpisane. Ostatnim krokiem było sprawdzenie działania serwisów `keylime` - po zmianie rejestrów prawidłowo zareagowały w sposób oczekiwany.

W ostatnim etapie raportu umieszczono screeny potwierdzające wykonanie ćwiczenia u każdej z osób z grupy - napisane rejestry oraz reakcję `keylime` na zmiany.