

Laboratorium 2, Sprawozdanie**Tworzenie podstawowych obiektów i konfiguracja FAPI****1. Tworzenie nowych obiektów.**

```
tpm2_createprimary -c primary.ctx
```

Tworzy klucz główny TPMi zapisuje jego kontekst do pliku primary.ctx

```
tpm2_create -C primary.ctx -G rsa2048 -u key.pub -r key.priv
```

Tworzy parę kluczy RSA 2048-bitowych, publiczny zostanie zapisany do pliku "key.pub", a prywatny do "key.priv", który zostanie przypisany do klucza głównego zapisanego w "primary.ctx"

```
tpm2_create -C primary.ctx -G rsa2048 -u key2.pub -r key2.priv -a
```

```
"restricted|decrypt|fixedtpm|fixedparent|sensitivedataorigin|userwithauth"
```

Tworzy klucz kryptograficzny RSA 2048-bitowy i zapisuje go do plików key2.pub i key2.priv, przy użyciu kontekstu primary.ctx, z zastrzeżeniem ograniczeń zdefiniowanych przez flagi restricted, decrypt, fixedtpm, fixedparent, sensitivedataorigin i userwit

```
tpm2_load -C primary.ctx -u key2.pub -r key2.priv -c key2.ctx
```

Ładuje klucz kryptograficzny do modułu TPM 2.0 i zapisuje go w kontekście key2.ctx, używając publicznego klucza key2.pub, prywatnego klucza key2.priv i kontekstu primary.ctx

```
tpm2_create -C key2.ctx -G Gaes -u key3.pub -r key3.priv echo "my sealed data" |
```

```
tpm2_create -C key2.ctx -i- -u key4.pub -r key4.priv
```

Tworzy dwie pary kluczy (publiczny i prywatny), z których jeden służy do wypełnienia danymi, a drugi do odczytu danych, następnie tworzy pliki .ctx, .pub i .priv dla każdej z par kluczy.

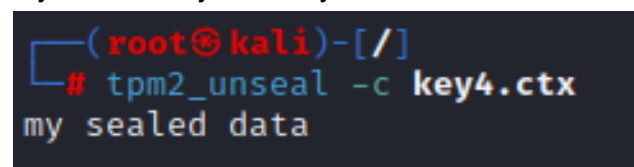
```
tpm2_load -C key2.ctx -u key4.pub -r key4.priv -c key4.ctx
```

Ładuje klucz prywatny, klucz publiczny i kontekst klucza do urządzenia TPM

```
tpm2_unseal -c key4.ctx
```

Odszyfrowuje dane z klucza kontekstowego key4.ctx przy użyciu modułu TPM 2.0

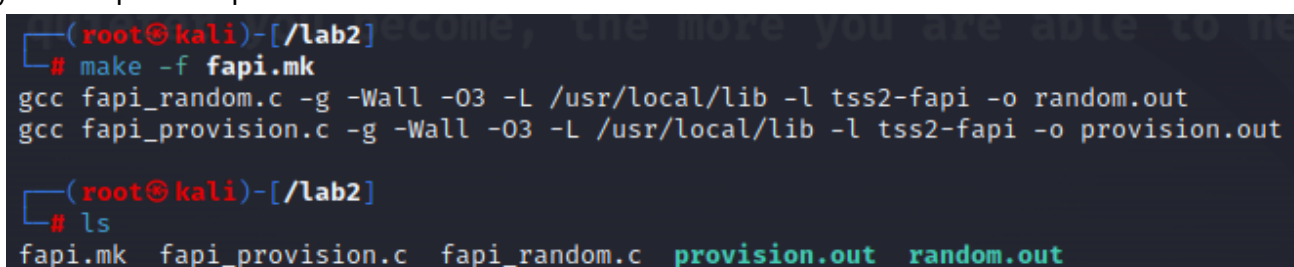
Wynik ostatniej komendy:



```
(root@kali)-[/]  
# tpm2_unseal -c key4.ctx  
my sealed data
```

2. Inicjalizacja FAPI.

Utworzono pliki fapi_provision.c, fapi_random.c oraz plik makefile fapi.mk. Następnie skompilowano pliki c i otrzymano 2 pliki out: provision.out i random.out.



```
(root@kali)-[/lab2]  
# make -f fapi.mk  
gcc fapi_random.c -g -Wall -O3 -L /usr/local/lib -l tss2-fapi -o random.out  
gcc fapi_provision.c -g -Wall -O3 -L /usr/local/lib -l tss2-fapi -o provision.out  
  
(root@kali)-[/lab2]  
# ls  
fapi.mk  fapi_provision.c  fapi_random.c  provision.out  random.out
```