LABB 3

VINCENT PALMA
IOT20

CA

CERTIFICATION AUTHORITY

UPPGIFT

Labben går ut på att skapa ett certifikat som kan användas för en website. Certifikatet ska sedan signeras med hjälp av en CA som tillhandahålls. För certifikathanteringen använder vi OpenSSL som är ett standardverktyg.

Certifikatet används sedan för att besöka en website. Om allt gjorts rätt kommer besöketa att synas från serverns sida.

Labben görs i Ubuntu VM i VirtualBox.

Deluppgift 2

3. Delfråga: Vad är "2048" i kommandot ovan?

2048 i kommandot "openssl genrsa -out key.pem 2048" betyder att det certifikatnyckel som genereras till key.pem ska genereras med bitantalet/bitstorlek 2048 .

5. Fråga: Vilken hashfunktion har den använt för signaturalgoritmen (inte namnet på signaturalgoritmen)?

Den kryptografiska Hashfunktionen som användes i detta sammanhang heter SHA256(Secure Hash Algorithm) som ger en output på 256bitar. Detta är en hashfunktion som vart standard år 2012.

7.

(a) Vad har certifikatet för serienummer?

```
Certificate Details:
        Serial Number: 4389 (0x1125)
```

(b) Hur länge är certifikatet giltigt?

```
        Validity
            Not Before: Aug 31 13:47:39 2021 GMT
            Not After : Aug 31 13:47:39 2022 GMT
```

(c) Hur stor (hur många bits) nyckel har certifikatet signerat?

```
            RSA Public-Key: (2048 bit)
```

(d) Vad heter den Certificate Authority som signerat ditt certifikat?

```
        Subject: C = SE, ST = Stockholm, O = Nackademin, OU = IoT20, CN = Vincent,
```

Deluppgift 3

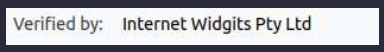
10. Översätt

Score! VG-poäng. Konvertera [förnamn, efternamn] till base64-kod och skriv det i labbrapporten :-)
Detta var översättningen och nedan är svaret på uppmaningen.

VmluY2VudCwgUGFsbWE=

12. Fråga: Vad är Common Name för serverns certifikat?

13. Vilken Certificate Authority har signerat serverns certifikat?



14. Vi har pratat om skillnaden mellan att göra en egen Certificate Authority och att köpa signering från ett företag/organisation som är en Certificate Authority.

Vilket av detta använder sig servern av? Resonera kring varför vi valt att göra på det sättet. Vad hade hänt om vi gjort på det andra sättet?

Det vi ser på server är att den har en self signed certifikat och anledningen till varför det är gjort så är dels för att det går att göra själv och det blir då gratis.
Hos ssl dragon verkar ett certifikat kosta 8usd per år. Ett självsignerat certifikat är ett som inte är signerat av en känd CA . I det här fallet är certifikatet signerat med sin egen genererade privata nyckel. Självsignerade certifikat erbjuder vissa fördelar när de används i interna nätverk och utvecklingsfaser, men de kan också skapa flera risker utan korrekt synlighet och kontroll speciellt hos publika sidor.