Assignment 12

Opdracht 1

a
Let's encrypt authority X3

b
DST ROOT CA X3
Let's encrypt authority X3

c
06.03.2017

d
SA: SHA256 RSA
HA: SHA256

e
De domeinnaam van het certificaat komt niet overeen met de domeinnaam van de website.

f
Dit certificaat is niet ondertekend door een goede Certificaat authoriteit.

g
1. Alice vertrouwd alleen Bob (Manual)
2. Ze vertrouwen hun vrienden (Web of trust)
3. Trust on first use (TOFU)

h
1. Usability: De key moet ofwel met een telefoon, ofwel face-to-face gecheckt worden.
   Security: Als Bob en Alice nog nooit hebben ontmoet kunnen ze elkaars authentiteit niet controleren.
2. Security: De vrienden kunnen met elkaar samenspannen en zo de sleutel achterhalen.
3. Security: De eerste keer dat de key wordt verzonden kan Eve de key achterhalen en/of veranderen.

i
De site heeft elementen die via http geladen worden in plaats van https.