𝔽oundations of Cybersecurity
Exercise Sheet 11
Singapore University of Technology and Design
November 22, 2017

- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Show the solutions of classwork (groups of max 3 persons) to an instructor before the end of the class.
- Submit your homework solutions (groups of max 2) to eDimension by the deadline below.

Classwork due on Wednesday November 22, 10:00 PM

Question 1

Design and implement a simple digital certificate framework. Your framework should allow to create a certificate chain and validate it.

Homework due on Wednesday November 29, 6:59 PM

Question 1

Incorporate your digital certificate framework to the key negotiation protocol from the previous week (week 10, classwork 1). Then incorporate both to the secure channel from the previous the previous classwork (week 8, classwork 1). More specifically, in the final system:

1. Alice and Bob trust a CA (i.e., Alice and Bob have the CA's certificate).
2. This CA issues certificates for Alice and Bob respectively.
3. Alice initiates a connection with Bob, starting an authenticated key negotiation (she needs to send her certificate which is then validated by Bob).
4. Bob authenticates the negotiation as well (he also needs to send his certificate to Alice).
5. After a shared key is established, the secure channel can be initiated.