ICT & Infra S2 M/S week 6: Secure network protocols, part B

**Class: 2**

**Student numbers: 4538528**

**Student names: Mihai Glodici**

Date: Feb 2022  
Version 1.0

# Introduction

In this practicum you will use a web server with a self-signed certificate. Although it is not recommended to use self-signed for environments that need to be safe, however configuring a self-signed certificate is useful for learning purposes.

How to deliver your assignments?

Fill in this document with required information about your group. Answer questions and upload the document to Canvas at most one week after the assignment is given.

## Assignment 1: Self-signed certificate webservers

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 120 minutes.

The following tutorial will guide you how to create a 4096-bit RSA key instead of a 2048-bit key. <https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-debian-8>

Make use of Linux VM at Fontys Seclab (see part A) or any other Linux VM deployed at your InfraLab environment.

Add some screenshots of the data from the self-signed certificate of your web server as evidence (you can do this via the web browser by looking at the certificate).

Graphical user interface, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Execute this command on your webserver:

*$ openssl s\_client -showcerts -host YOUR\_WEBSERVER\_IP -port 443*

What is the output of this command?

Text

Description automatically generated

Text

Description automatically generated

A digital certificate contains a lot of information, this can also be seen in the output of the above command. What information can you find in the digital certificate en make a comparison between a self-signed certificate and an extended Validation certificate (recognizable at the green area within the URL). Execute the same command, but now for a website with EV-certificate. Paste the output in the answer area hereunder.

What is the output of this command? (EV certificate)

Text

Description automatically generatedText

Description automatically generated

Describe the similarities and differences between the certificates

similarities:

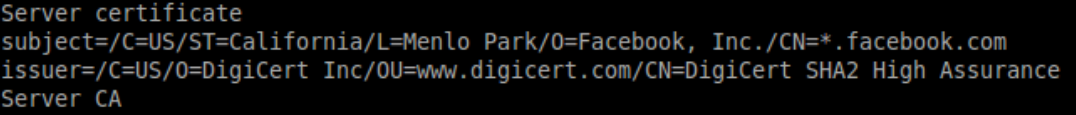
both use the same encryption method:

A computer screen capture

Description automatically generated with medium confidence

differences:

- last line shows that it’s a self signed certificate (code18) for mine, while facebook’s cert gives code 20

-facebook’s is a SHA2 High Assurance Server based in California from digicert.com

While mine is locally certified by me

Text

Description automatically generated

Same story with the certification chain.

Graphical user interface, text

Description automatically generated

## Bonus assignment 2: Client-Side certificate

Difficulty: C:\Users\874156\Desktop\flatastic-icons-part-1-by-custom-icon-design\png\16x16\star-3_5.png. Estimated time: 120 minutes.

What is a client-side certificate? Find out yourself what you can do with it.

Describe your scenario and steps.