Handin ten: Exercise 15.2
Group: IT03

Kasper Iverslien Borgbjerg (201808262) – 201808262@post.au.dk
Oliver Christensen (201808502) – 201808502@post.au.dk
Frederik Bay (201800246) – 201800246@post.au.dk

December 1, 2020

Kasper Iverslien Borgbjerg – 201808262 Oliver Christensen – 201808502
Frederik Bay Nørgaard – 201800246

1 Exercise 15.2: Authenticated Key-Exchange

A browser starts an URL connection with a server by typing the URL which is desired to connect to. In this case there is no redirecting, and the URL typed is also the URL, which will connect to the server. The server will send its cerificate, and the browser will then verify it, and if the URL is still correct by the one typed, it can contact the server if the certificate does not verify.

1.1 Question 1:

By doing the check above, the browser can avoid malicious behaviour as it will have server send the certificate, and will only establish a secure connection if the URL is corresponding to the one typed, and that the certificate is correct. If this check were not performed, the client can not be certain that the server that it is connecting to, is corresponding to the server, which it wants to connect to. If the server does not send this, the client cannot be sure that this is right server. And by the server sending it URL in the certificate, the client can verify that the server corresponds to the URL, which is secure. An attack is layed out in figure 1, where n_3 acts maliciuos, and redirects the user to W_b

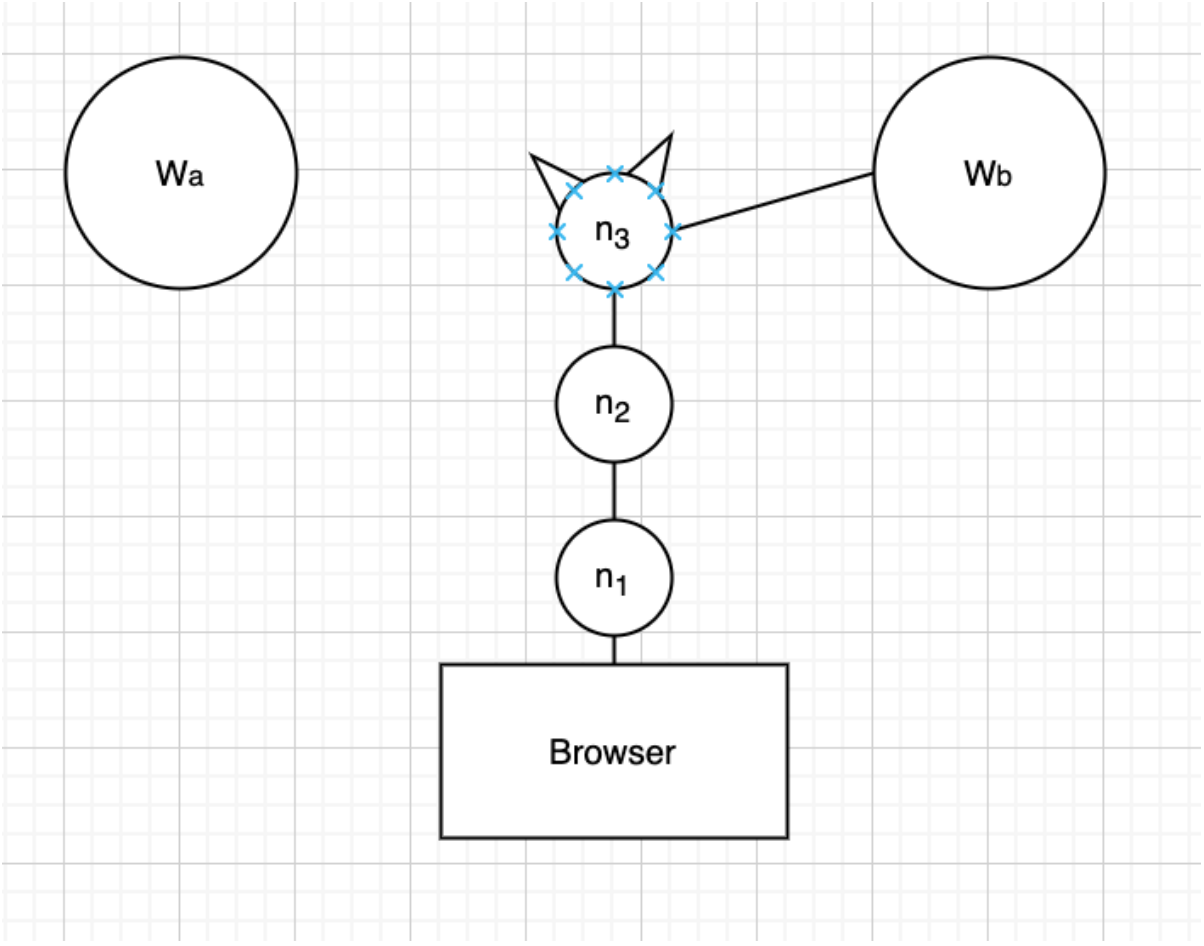

Figure 1: Website B

Now describe an attack where the user wants a secure connection to web site W_a, but instead gets a secure connection the adversary's website W_b without the browser showing any warnings to the user.

When a user connects to a network with the typed URL, this person will connect to a note in the network at first. This note will connect to $note_n$, which eventually will connect the browser to a server, but if one

note in this is corrupt, this note can redirect the user to W_b, instead of W_a. And if there are no warning issued, the user does not know that it has connected to the wrong server.

1.2 Question 2:

If the URL is not present, the client C, can manually check the certificate of the browser of the website loaded. As seen below in the certificate for www.dr.dk, the user can validate the authenticity of the connection by looking at the different parameters of the certificate. These parameters could for example be Country of Region, Organization and Issuer Name.

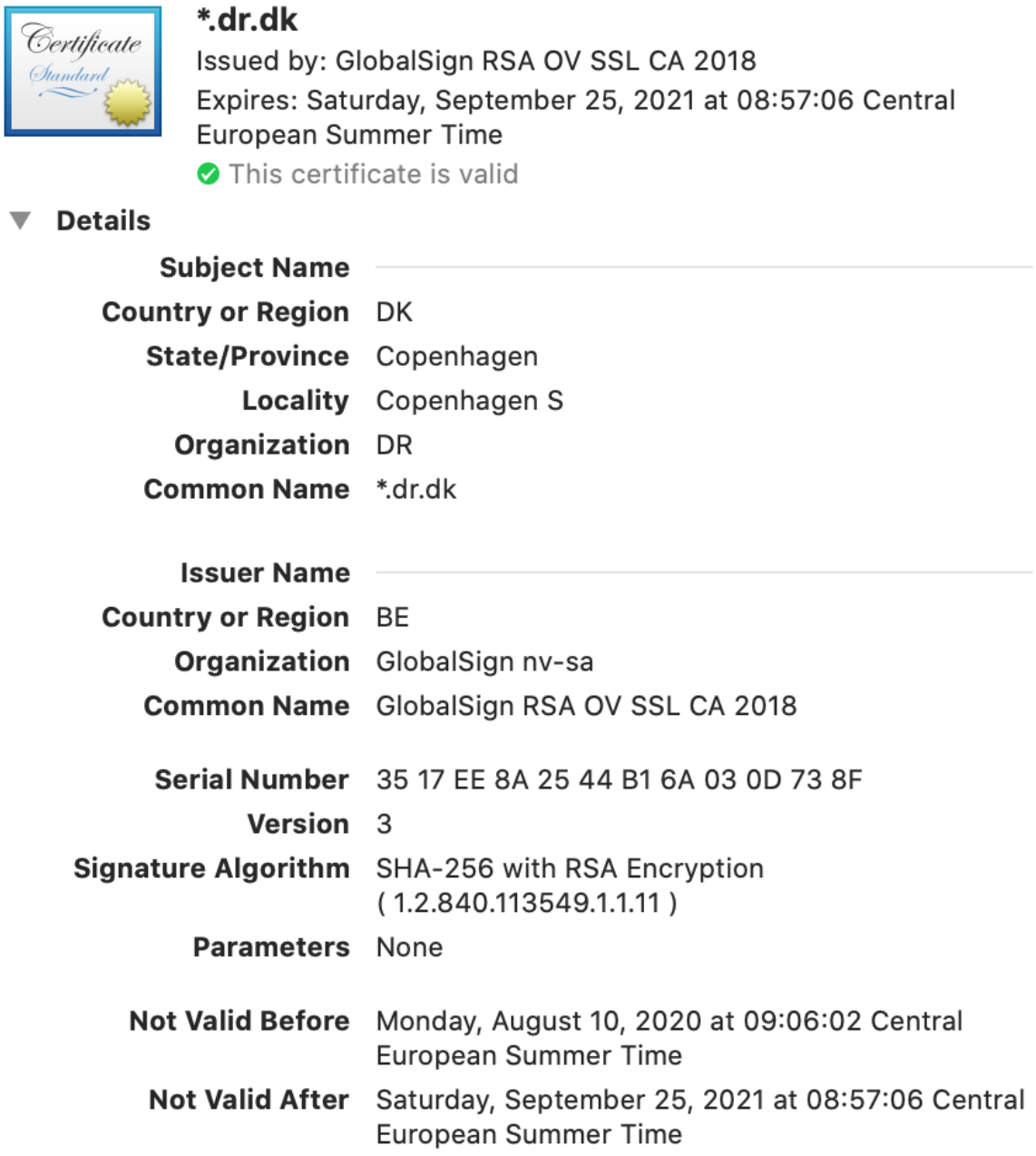

Figure 2: DR webiste Certificate

Kasper Iverslien Borgbjerg – 201808262 Oliver Christensen – 201808502
Frederik Bay Nørgaard – 201800246

1.3 Question 3:

Show how to construct from π' a new AKE protocol π that satisfies definition D. You are looking for a very simple solution in which your protocol may fail even if π' succeeds.

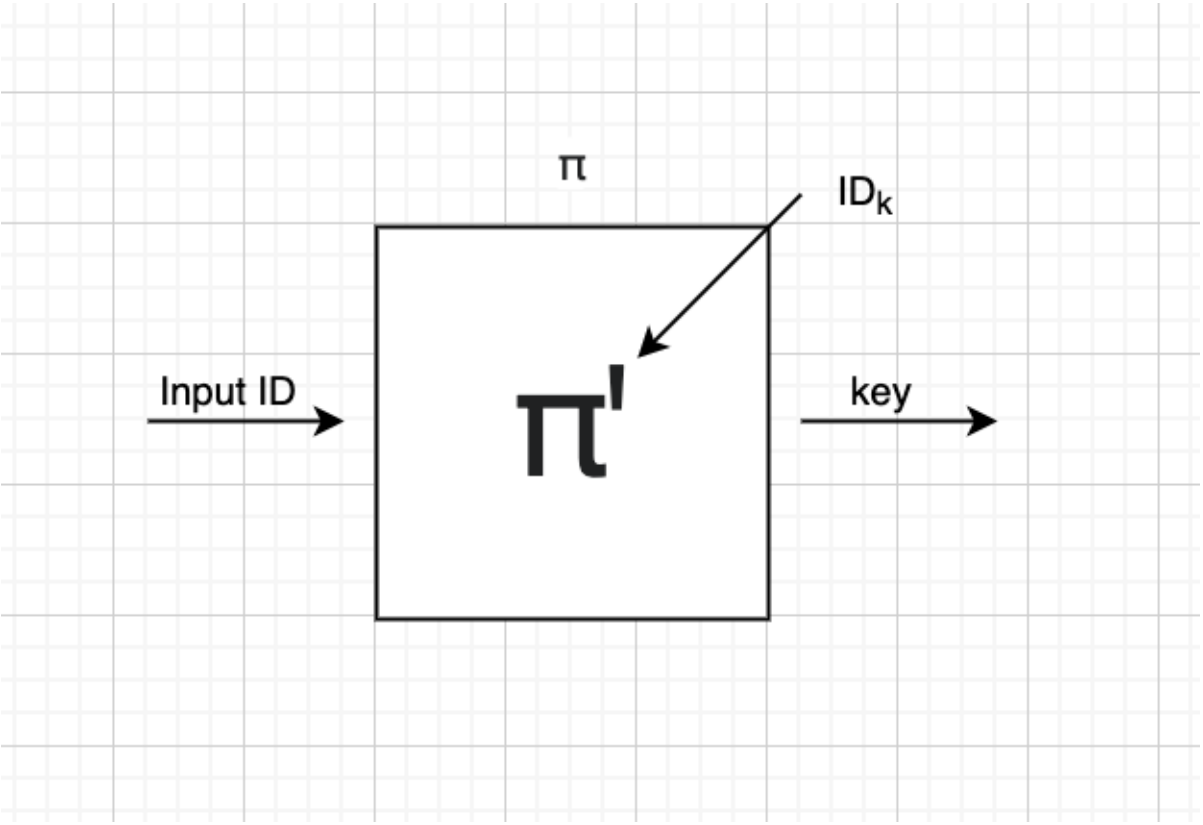

Figure 3

The figure 3 above, show how the new AKE protocol, π, could look like. The input of the AKE is the ID of the reciever. The output is the key_A, ID_B, if the input is ID_A. By doing this, the protocol π', does not require an input, and will satify D'. By incupsulating π', this can succeed given that it does require an input, though π would not succeed if no input is given.

Consider the SSL AKE without the URL check. Which of the two definitions D, D' does it satisfy?

The one that satisfies, is D' because it requires no input. Therefore the key exchange will only happen, if the validation is completed, and you will receive the identity and a key of the party, that has exchanged a key with.