Started on	Wednesday, 11 November 2020, 08:01
State	Finished
Completed on	Wednesday, 11 November 2020, 08:08
Time taken	6 mins 24 secs
Feedback	Your overall score for this part is 100%. Congratulations ! The exact grade as well as details for each question will be made available as soon as the submission period for the quiz closes.

Question 1

Complete

Marked out of 1.00

⚑ Flag question

How many packets are exchanged during the handshake phase with TLSv1.3?

Answer: 2

In the handshake phase, the client and the server must agree on the schemes to use for secure communication.

Question 2

Complete

Marked out of 1.00

⚑ Flag question

Drag the words from below and drop them at their right location in the following text:

In the handshake protocol of TLSv1.3, the first sent packet is a [_____], which consists of the [_____] initiating the communication with the [_____], this packet contains information on the [_____]. Then, the second packet is a [_____] in which the chosen cipher suite is specified. Finally a [_____] packet is sent by the client to confirm the chosen cipher suite, this packet also contains some [_____] and is not part of the [_____].

server

Now that the TLS communication is established, is the PMU authenticated to the PDC? Yes

And is the PDC authenticated to the PMU? No

Is it possible that the PMU agrees to send data to a fake PDC? Yes

Is it possible that the PDC receives data from a fake PMU? No

Recall that the PMU is the server and the PDC is the client.

Check again who provides a certificate and who checks it.

Question **4**

Complete

Marked out of 1.00

⚑ Flag question

For a secure two-way authentication, should the certificate of the PMU and the certificate of the PDC be signed by the same certificate authority?

Select one:

- ○ a. No
- ⊙ b. It doesn't matter
- ○ c. Yes

Finish
review

◀ [Graded] Lab3 - Part 4

Jump to...

[Bonus] Lab3 - Part 6 ▶

Quiz navigation

1 2 3 4

Show one page at a time

Finish review

EPFL