Protokollssicherheit

Workshop – Design and Implementation of Protocols
E-Shop Scenario

Consider the scenario where a **Customer** wants to buy some product from some **E-Shop**. The **E-Shop**, on the other hand, interacts with the customer’s **Payment Service** (PS) in order to carry out the transaction.

However, in order for the PS to validate the transaction, it asks the customer to validate the transaction once again, but this time with the PS. (Here for simplicity, we can assume that the customer has enough credit to buy the intended item.)

Once the customer validates (or not) the transaction, the **e-shop** is informed whether the transaction was completed or not.

Now, imagine that you are working for **PayMal™** and your goal is to allow web-sites, such as E-Shop, to handle their payment transaction using your services.
(You can imagine yourself as a competitor of PayPal.)
E-Shop Scenario

Some Expected Properties

- The customer’s data should only be known to the E-Shop.
- The E-Shop should know whether the transaction was carried out by the PS with the correct amount and the correct customer.
- Of course, the transaction should only be carried out whenever there was the intention of the customer to buy some item from the E-Shop.
- The Credit Card information of the user should remain secret.
- The PS and the E-Shop have published their public keys.
- Does the customer need to know the public keys of the PS and/or the E-Shop?
- Think of any other reasonable property that should be satisfied in this scenario.