

## Exercises “Anonymous Credentials III”

### Exercise 1. E-cash with Different Denominations

The ecash solutions we considered in the lectures only had one denomination. So, if a users wanted to buy goods for, say 84 Swiss Francs, she would need to spend 84 ecoins with the merchant. That would of course not be efficient. How can we do better?

1. How can we realize coins with different denominations?
2. How could we get exchange money without loosing anonymity?
3. In any case we probably need to download a number of coins. This of ways to make it more efficient to download and spend several coins at the same time.

### Exercise 2. Revocation of Credentials

1. Think about why credentials need to be revoked and why it could be important that a credential was recently issued.
2. Sometimes one is not aware that a credential has been lost and thus it gets misused before it can be revoked. Think about how to detect such misuse while still protecting privacy. Think about whether one could use some third party with the third party only learning minimal information.
3. Think about how short-lived certificates and the revocation mechanisms discussed in the lectures could be combined.