

Worksheet 6 – Digital Signatures - EXTRA**Digital Signatures @.NET****Covered topics:**

- Concept of Digital Signatures
- Digital Signatures in .Net

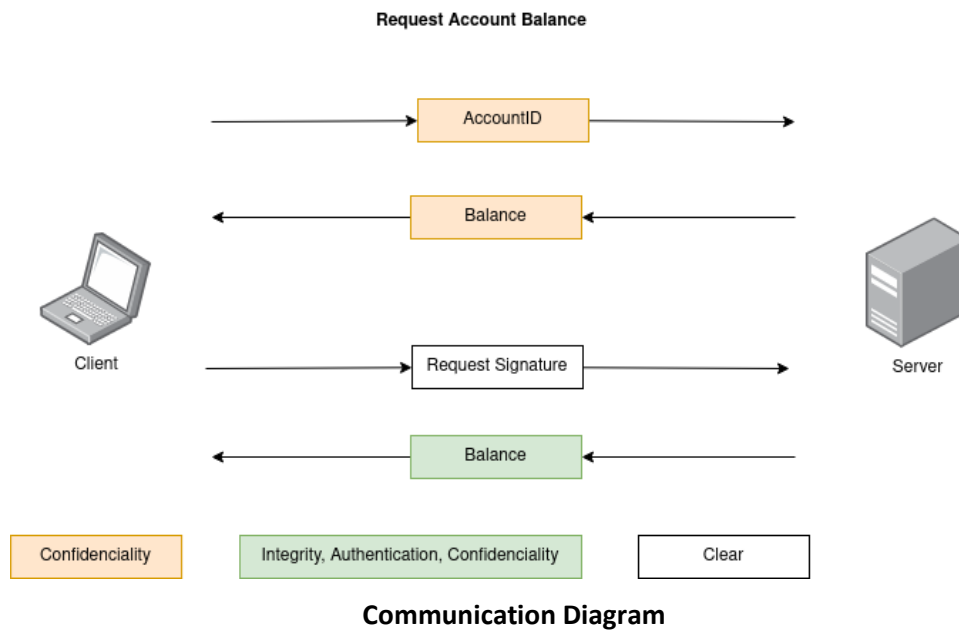
©2020:{ricardo.p.gomes, marisa.maximiano, alexandre.fernandes}@ipleiria.pt

Digital Signatures

The next exercise is intended to help you try out the concepts learned in the previous worksheets.

Exercise

1. Start with a blank solution or a copy for the solution you created for the exercise 1.2 of worksheet 6.
2. Implement the following scenario:
 - a) Share any necessary cryptographic components needed
 - b) Client sends an accountID (can be statically defined, see example bellow) and the server replies with the balance for that account
 - i. Both communications must be confidential
 - c) Client sends a request for a digital signature and the server replies by signing the previous account balance
 - i. The request can go in clear text, but the reply must guarantee confidentiality, integrity and authentication (assuming entities trust shared keys)



Example code for accounts on Server:

```
Dictionary<int, double> accounts = new Dictionary<int, double>();
accounts.Add(123,100.50);
accounts.Add(456,200.50);
accounts.Add(789,3000);
...
double balance = accounts[123]
```