*Foundation of Cybersecurity - Project A.A. 2022-23*

# A Secure Bank Application

A Secure Bank Application (SBA) is a client-server application that allows users to issue operations on their own bank accounts.

Each user is modeled by *username* and a *password* whereas each bank account by an *accountID* and a *balance*. For simplicity we assume that a user owns a single account and that an account is owned by a single owner.

A user may issue the following operations on its own bank account:

- (accountId, balance) ← Balance() which returns the user's bank account's *accountId* and *balance*.
- Bool ← Transfer(UserName other, uint amount) which takes both the username of another user (other) and an amount of money as input parameters and transfers such an amount from the user's bank account to the other user's bank account. The operation returns false if the value of balance is smaller than the value of amount; it returns true otherwise.
- ListofTranfers ← History() which returns the last T transfers performed by the user, where T is a system configuration parameter. Each transfer is a triple (user, amount, timestamp).

The SBA application is hosted by a server which maintains users and accounts. Users interact with the SBA server through a secure channel that must be established before issuing operations.

Requirements

1. Each principal owns a pair of private and public keys.
2. The SBA server maintains the public key of every user.
3. Each user maintains the public key of the server.
4. Users are initialized at registration time which is off-line.
5. OpenSSL API TLS cannot be used.
6. The authentication protocol must fulfill Perfect Forward Secrecy (PFS).
7. Client-serve communication must fulfill confidentiality, integrity, no-replay and non-malleability.
8. Password and history of transfers of any given user cannot be stored in the clear.

**General Guidelines**

- Use C or C++ programming language and OpenSSL library.
- Key establishment protocol must establish one (or more) symmetric session key(s) with public-key crypto. Then, the session protocol must use session key(s) to communicate.
- Communication must be confidential, authenticated, and protected against replay.
- No coding vulnerabilities.
- Project report must contain:
    - Specifications and design choices
    - Format of all the exchanged messages
    - Sequence Diagrams of every used communication protocol (Application Level).