

Programming Project II
Due Date: April 26, 2007

A Secure Online Banking System

In this project, you will design and implement a highly simplified secure online banking system. The system will have three kinds of entities: users, one or more banks and a number of merchants. All of these entities run on machines in different locations that are connected by an open network. As a result, secure communication channels will be used to protect communication between two parties. You will explore a number of concepts in this project. These include (1) setting up a distributed systems security infrastructure, including a certificate authority (CA), certificates for users, banks and merchants, (2) secure communication channels, (3) delegation from users to merchants, and (4) multiple authentication credentials and authorization based on them. The following scenario illustrates typical operation of the system.

A user chooses a bank to open an online account. At this time, credentials are created that allow the user and the bank to authenticate each other and establish secure communication between their machines. Once an account is created, a user can “log into” the account to deposit or withdraw money. An access control policy may be defined that limits how much money can be withdrawn over a certain period. In addition, users can do online shopping at merchant sites and the merchants can be paid electronically by the bank on behalf of a user. This is done when a user completes a transaction with a merchant and authorizes the merchant to make withdrawal from the user account. You will use delegation of authority to implement this.

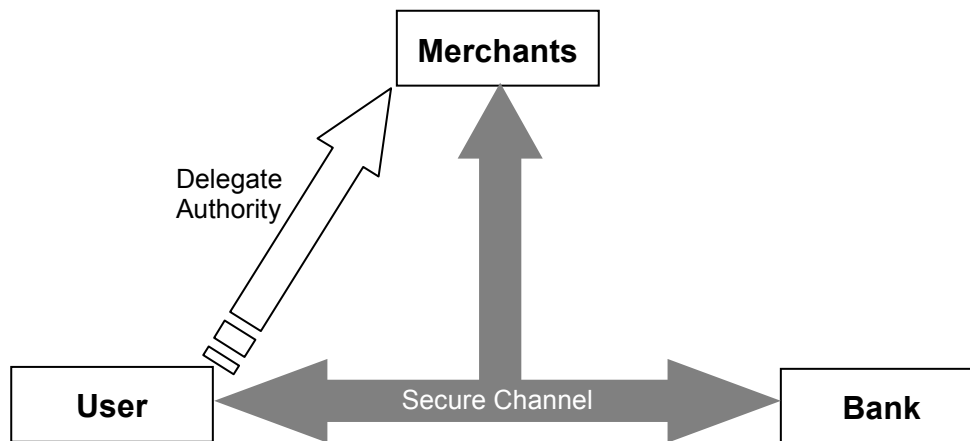


Fig. 1: System Diagram

Clearly, all this will require mutual authentication and establishment of secure communication channels, definition of credentials that are exchanged between various entities, processing of such credentials and decisions about when access to an account is granted. You will need to use a cryptographic library such as *OpenSSL*.

You first need to develop an API for interactions between the various entities in the system. Second, define the protocols that will be used to enable interactions between the entities. In particular, define the message formats that carry various credentials, how they are encrypted and decrypted, and their handling at their destination nodes. You clearly need to state the assumptions you make and explore why the protocols meet the security requirements defined in the system.