

# Wallets and Identities

In this lesson, we will see how wallets and identities are used in client applications through a sequence diagram.

## WE'LL COVER THE FOLLOWING

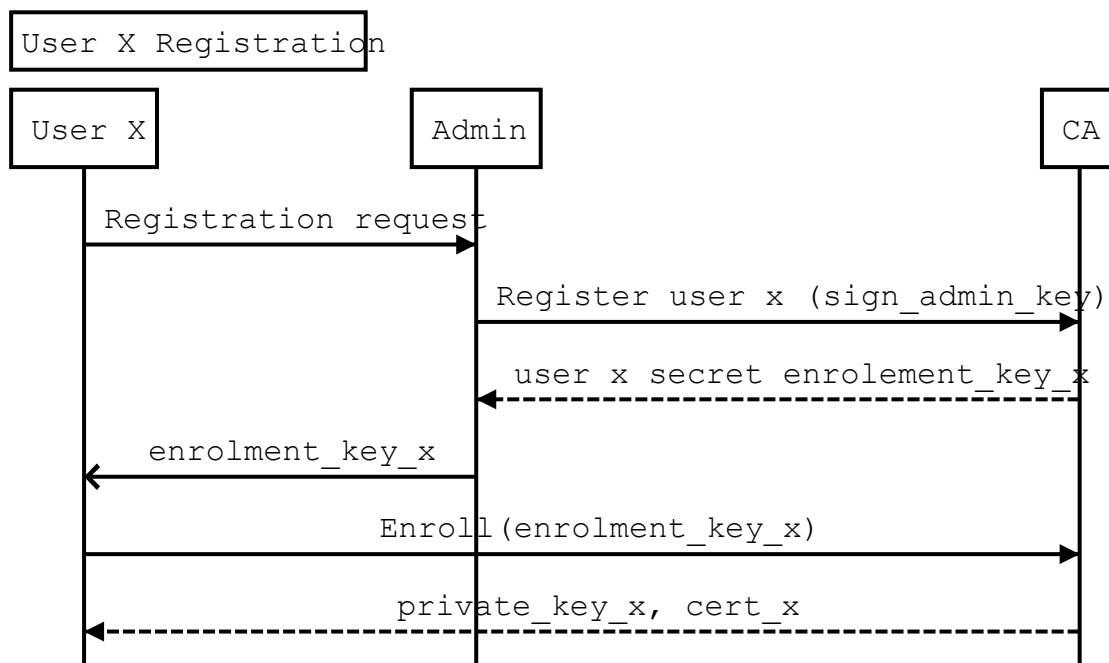
- Wallets and Identities in Client Application
- First User (Admin)

## Wallets and Identities in Client Application #

Now lets see how the wallet and user identities work.

We can issue a new user's key and get CA signed cert by contacting the CA.  
Here are the needed steps:

1. A valid existing user A **registers** a new user X to CA. The CA returns the **enrollment key**.
2. The user A shares that **enrollment key** with X
3. User X/A contacts the CA to **enroll** user X and passes in the **enrollment key**. CA returns valid key and signed certificate for user X.



User X

Admin

CA

## First User (Admin) #

When deploying the CA we need to bootstrap it with one initial admin user that can further register new users. The `enrollment key` for this admin user is pre-set in our initial configuration and the admin user is hence already registered when CA starts. Hence, all we need to do is to `enroll` the admin user with right `enrollment key` on application first launch.

In the next lesson, we will deploy our client application.