User Registration & Enrollment

Digital identities should be issued by certificate authorities (CAs) trusted by network participants. Hyperledger Fabric provides a built-in implementation of a CA component, Hyperledger Fabric CA, also known as Fabric CA. This component is a private root CA provider capable of managing the digital identities of Hyperledger Fabric network participants.

Fabric CA server is usually deployed in a Docker container along with other network components (such as peers, orderers, etc.). The server process can host multiple certificate authorities uniquely identified by name. Therefore, this single server process receives and routes the requests for each certificate authority it hosts.

The Fabric CA server has a database for keeping track of identities and certificates. In order to execute operations in the blockchain network, a user should obtain a certificate signed by a trusted authority. A trusted CA, in our case, is Hyperledger Fabric CA. However, the request for obtaining a signed certificate from Fabric CA requires proper credentials (i.e., a signed certificate and a corresponding key) for it to be fulfilled.

To solve this issue, Hyperledger Fabric CA can bootstrap one or more identities during the server initialization phase. At least one bootstrap identity is required to start the Fabric CA server - the CA server administrator. To bootstrap an identity, you should specify an enrollment ID and an enrollment secret. For example, **test-network's** CA server creates an administrator with the **admin** ID and **adminpw** secret.

Bootstrapping does not generate a certificate for the server administrator or any other user. It only registers the bootstrapped identities and stores their enrollment credentials in the Fabric CA database, granting the possibility to obtain an enrollment certificate right after the Fabric CA server starts.