

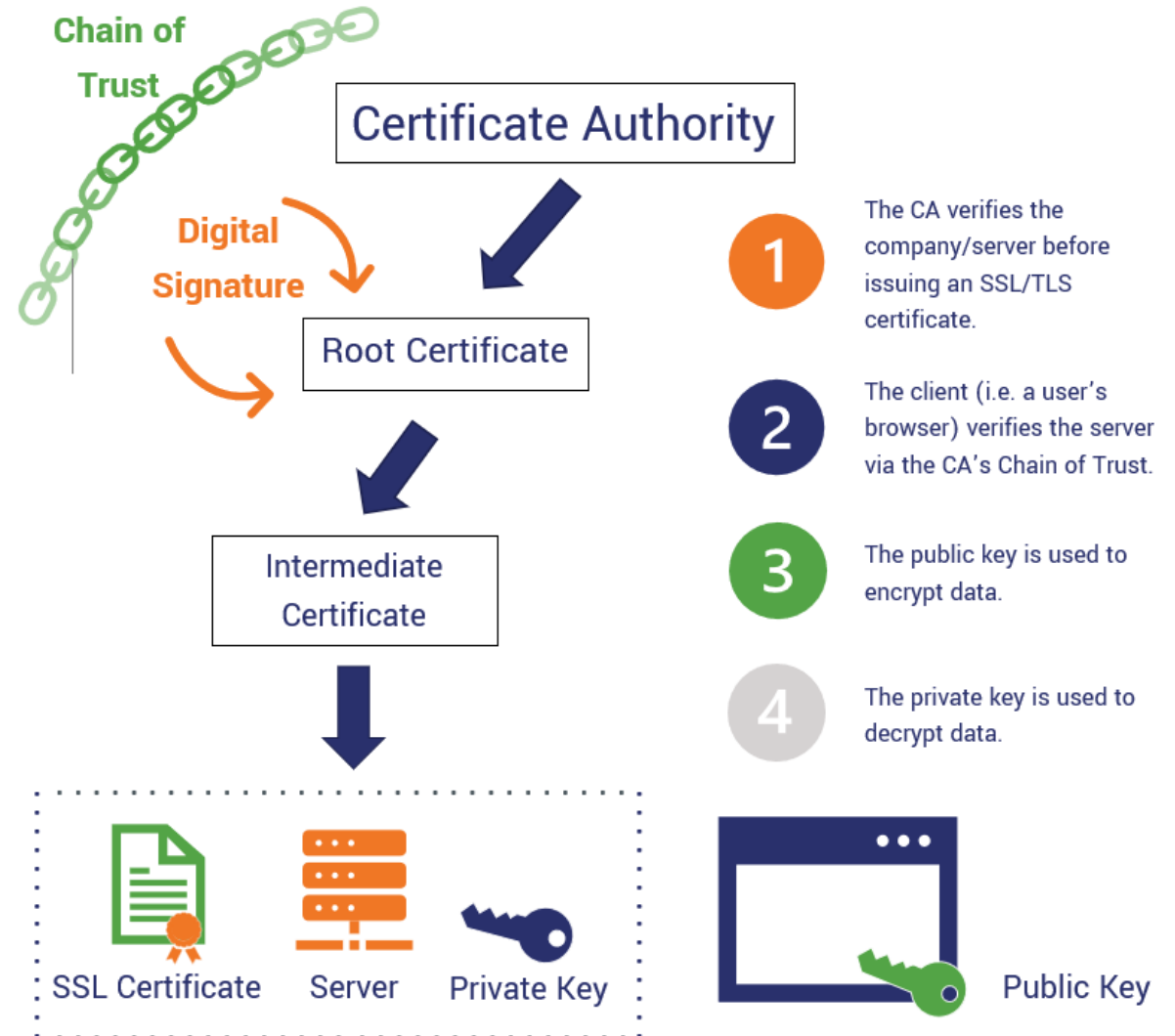
User Authentication based on DNSSEC and Blockchain

Hongtao Li
China Internet Network Information Center (CNNIC)
February, 2024



Background

- ❑ Current CA mainly implements the issuance of server certificates.
- ❑ The untrusted problem of CA will lead to the untrustworthiness of entity identity, and an attack on a CA or the issuance of a certificate by a malicious CA will bring major security risks to the information system.
- ❑ During the encrypted connection process, only the user can authenticate the server, but the server cannot authenticate the user.



Background

In summary, the current user authentication mainly has the following 3 problems:

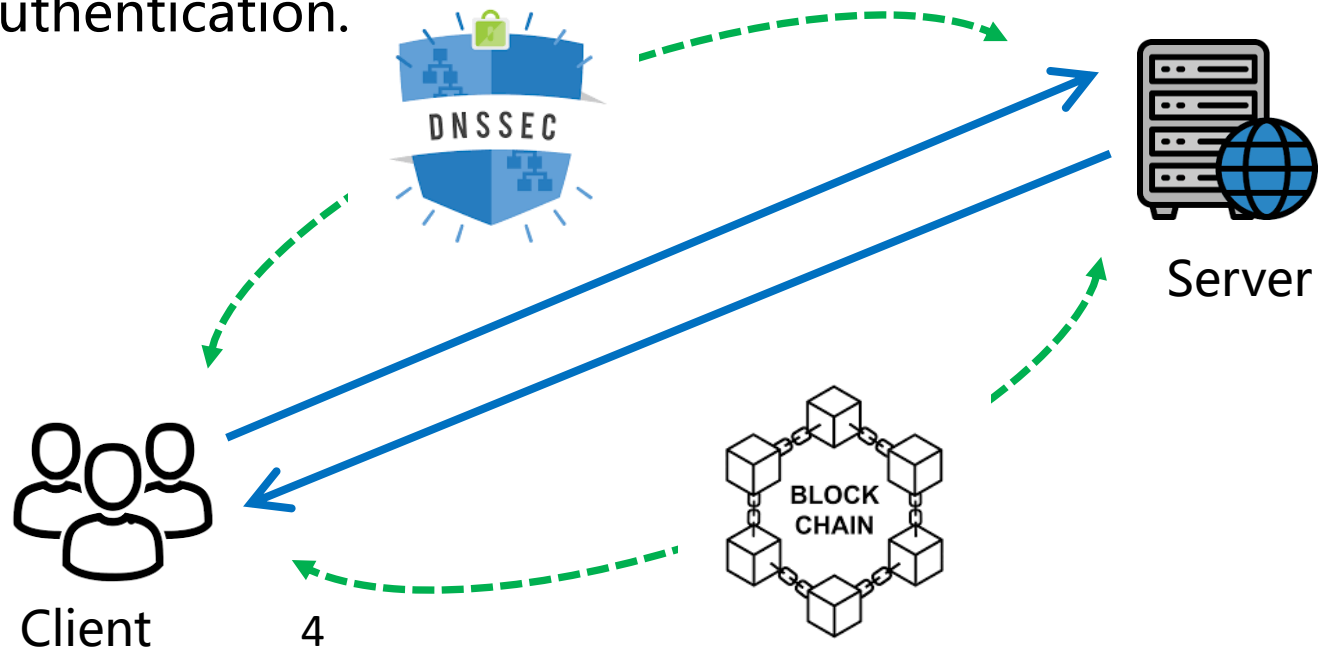
- ❑ It is difficult to provide two-way authentication; X
- ❑ It has a great dependence on CA, with the problems of CA single point of failure and multi-CA mutual trust risk; X
- ❑ It has a high implementation cost. X

Method

When an encrypted connection over Internet need to be performed between a server and a client:

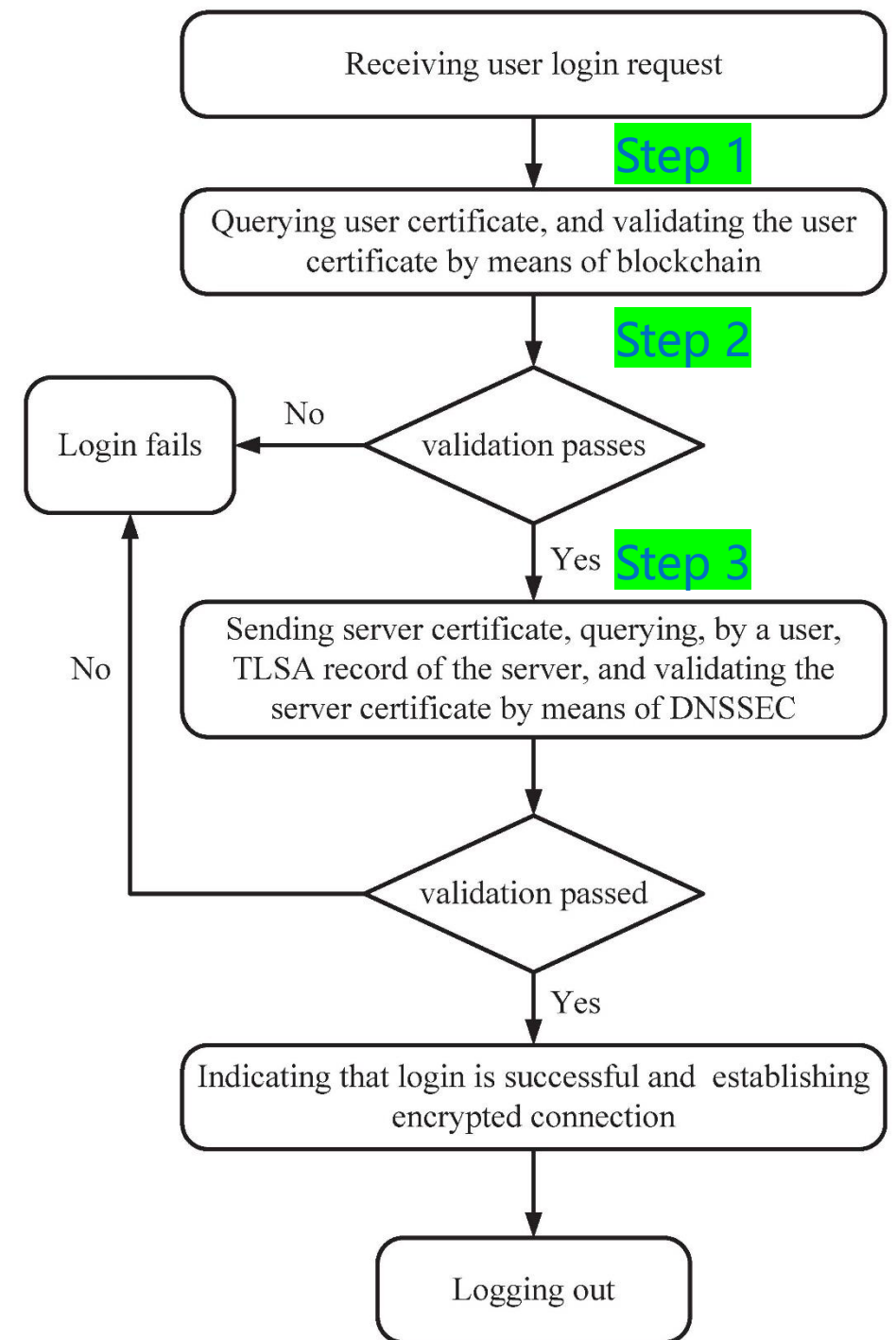
- ❑ authenticating, by the server, the identity of the client by means of a blockchain-based authentication mechanism;
- ❑ authenticating, by the client, the identity of the server by means of a DNSSEC-based mechanism.

Therefore, mutual authentication for an encrypted connection process over Internet is achieved without relying on CA authentication.



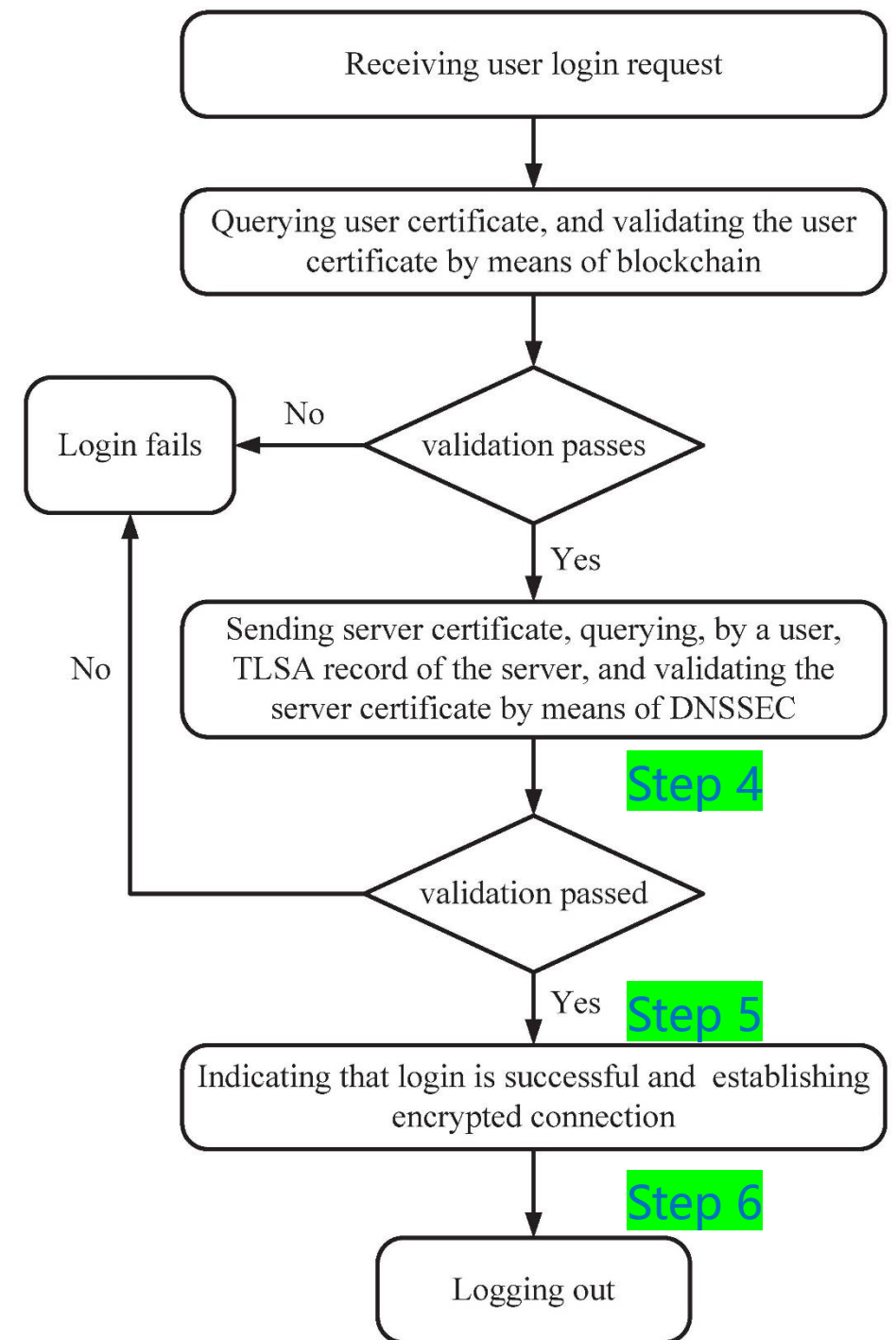
Details

- ❑ **Step 1:** accepting a user' s login request;
- ❑ **Step 2:** searching for, by a server, a corresponding personal certificate in the blockchain-based certificate system according to the user information, and validating; indicating that the user certificate is invalid and the login fails when the validation fails;
- ❑ **Step 3:** sending, by the server, the certificate to the client;



Details

- ❑ **Step 4:** searching for, by the client, a TLSA record corresponding to the management system of the server, and performing DNSSEC validation, indicating the server certificate is invalid and the login fails when the DNSSEC validation fails or the TLSA comparison is inconsistent;
- ❑ **Step 5:** establishing an encrypted transmission connection when the certificates of both parties are successfully validated;
- ❑ **Step 6:** logging out after the transaction is completed.



Outcomes

According to the above blockchain and DNSSEC-based user authentication method:

- ❑ Two-way authentication; ✓
- ❑ No problems of CA single point of failure / multi-CA mutual trust risk; ✓
- ❑ Relatively convenient to be implemented. ✓

We hope our work could promote the application of DNSSEC, not only in the DNS itself, but also in some wider areas, to make the DNSSEC more valuable and prospectively.

Thank you!

