A method of building global mutual trust infrastructure based on Blockchain

Leng Bing

June 2021

Southwest Communications Institute of China

CONTENTS

Part 1:

BACKGROUND

1. BACKGROUND

- With the evolution of digitalization and the expansion of stakeholders, civil aviation information system is facing more and more security threats.
- It is necessary to establish a global trust cyberspace of ICAO.
- In this cyberspace, every entity can be identified and every behavior can be expected.

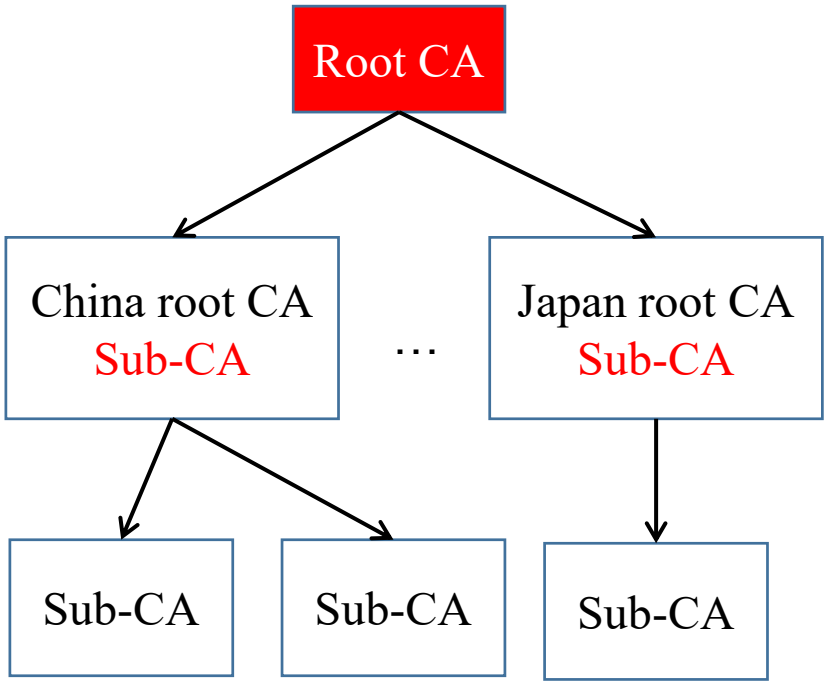
1. BACKGROUND

- The premise of CNS (Communications Navigation & Surveillance) is the identification and mutual trust between cyberspace entities.
- A Public Key Infrastructure (PKI) is a mature and reliable digital identity management system.
- With the help of PKI, every digital space entity, *including users, service providers, aircraft, terminals, servers, engines, software, and even data*, has a unique digital certificate, just like the passport in the physical world.

1. BACKGROUND

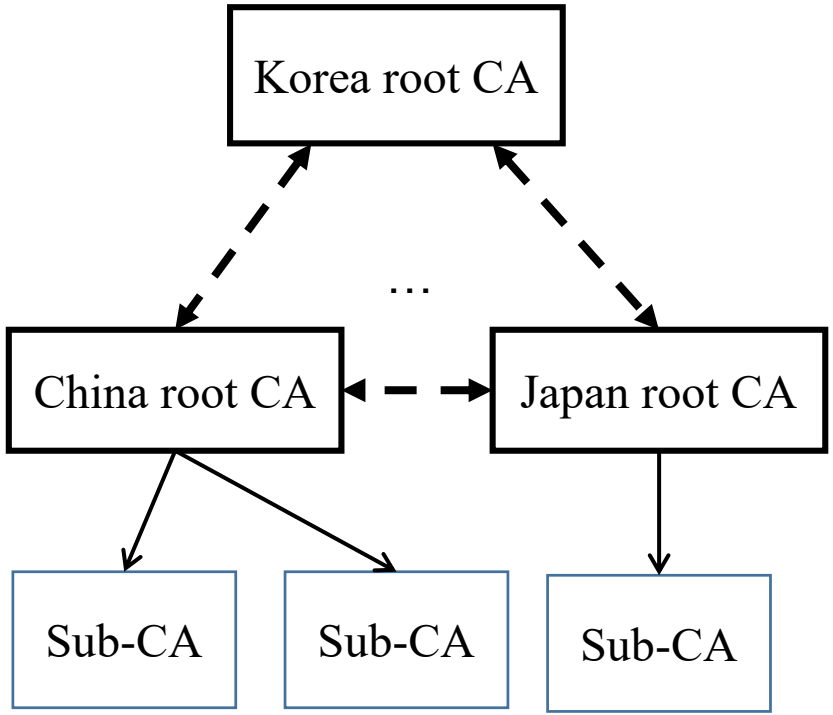
- It is easy to establish a PKI system within a state, the challenge is how to build mutual trust between state PKIs?
- According to the analysis of the ICAO publication *Global Resilient Aviation Network Concept of Operations*, there are three main architectural approaches to establishing the aviation PKI.

① A single root CA



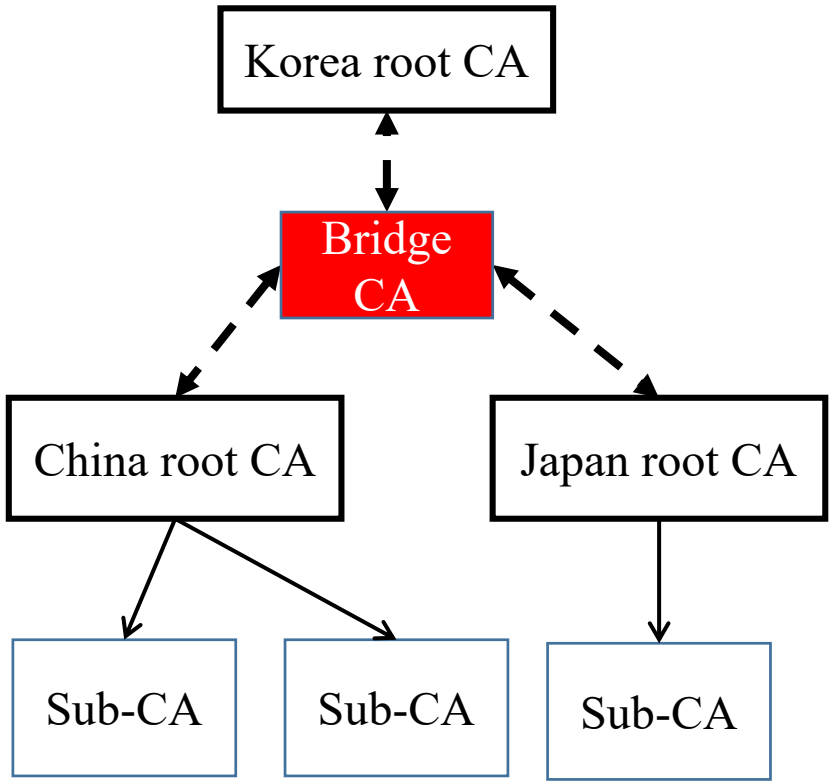
- Add a new root CA (Certificate Authority) beyond the existing root CAs.
- Disadvantage:
  - ① Put the liability of the PKI in the hands of one root CA;
  - ② Every system needs to be modified and reconfigured to adopt the new PKI hierarchy.

② Cross certification between each root CA



- A root CA per state with individual bi-lateral agreements.
- Disadvantage:
  - ① a root CA per state, region or organization requires the establishment and maintenance of N * (N-1) / 2 number of bi-lateral agreements between the root CAs.

③ A Bridge CA --*Recommended by ICAO publication*



- Use a Bridge CA providing bi-directional cross certification between each root CA and itself, which can reduce the bi-lateral agreements.
- Disadvantage:
  - ① the BCA is a third party service provider, the credibility of which determines the reliability of the mutual trust relationship.
  - ② There is no Trust Third Party government or organization beyond all member states under current ICAO framework. –*who operate it*?

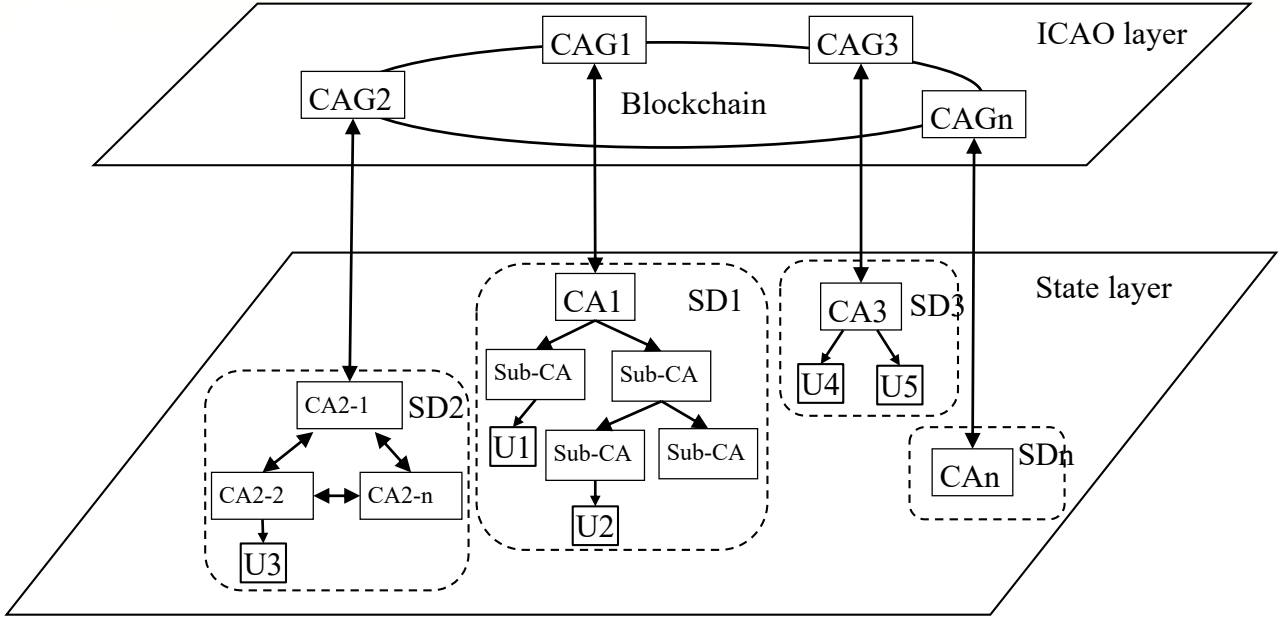
1. BACKGROUND

- Thanks to the latest technology, the Blockchain has the characteristics of natural decentralization and can be used for the construction of Mutual Trust Infrastructure among global states.
- At ICAO-UAE blockchain Summit and Exhibition, held on 3-4 April 2019 in Dubai, ICAO Council President Dr. Aliu underscores that:
  - Blockchain has the potential to enhancing both safety and security.
  - I am looking forward to some provocative ideas and insights from our key presenters.

Part 2:

MUTUAL TRUST ARCHITECTURE

Mutual trust architecture



- ICAO layer consists of CA Gateway(CAG) of each member state, which is a distributed and decentralized alliance blockchain. *--Simple deployment*
- Each state is an independent Security Domain and can adopt different PKI architectures. The existing PKI infrastructure does NOT need to be modified or reconfigured. *--Good compatibility*
- Each CAG node is managed by its own state, and a CAG provides bi-directional cross certification between a root CA and itself. *--Clear management*
- The digital certificates of all level CAs of each state and the Certificate Revocation List(CRL) should be stored in the blockchain. *--Clear function*

Part 3:

ADVANTAGES OF BLOCKCHAIN

3 ADVANTAGES OF BLOCKCHAIN

3.1 Transparent and trustworthy

- In the blockchain system, all nodes are peer-to-peer nodes. Everyone sends and receives messages equally in the network, so each node can observe all the behaviors of nodes in the system completely, and the whole system is transparent to each node.
- The final result is obtained by all nodes using a consensus algorithm.

3 ADVANTAGES OF BLOCKCHAIN

3.2 Tamper proof and traceable

- In the blockchain, once the operation is written, it cannot be tampered.
- Any operation on the blockchain has a complete record and can be traced.

3 ADVANTAGES OF BLOCKCHAIN

3.3 High reliability

- Firstly, each node maintains an account book equally and participates in the consensus of the whole system. The failure or offline of one node will not affect the normal operation of the whole system.
- Secondly, the blockchain system supports Byzantine Fault Tolerance. Even if there are a certain number of malicious attack nodes in the system, the system can operate normally.

Part 4:

CAPABILITIES

4. CAPABILITIES

The system should:

(1) Support digital certificate storage, retrieval, verification, update, revocation and other operations.

(2) Provide web service interface;

(3) Blockchain building capacity of no less than 500 CAG nodes.

(4) The certificate query time on the Blockchain is less than 5 seconds.

(5) The certificate verification time is less than 1 second.

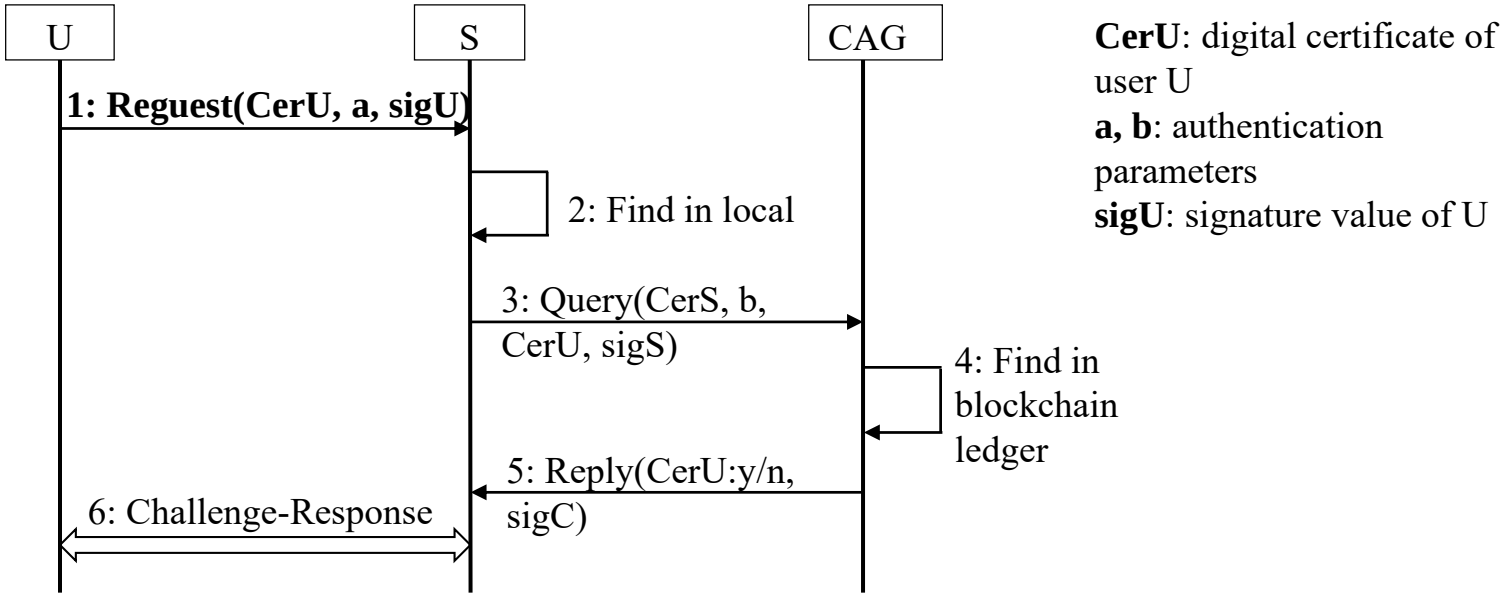
(6) The query time of certificate revocation list on the blockchain is less than 5 seconds.

Part 5:

TYPICAL CROSS SECURITY DOMAIN AUTHENTICATION PROCESS

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.

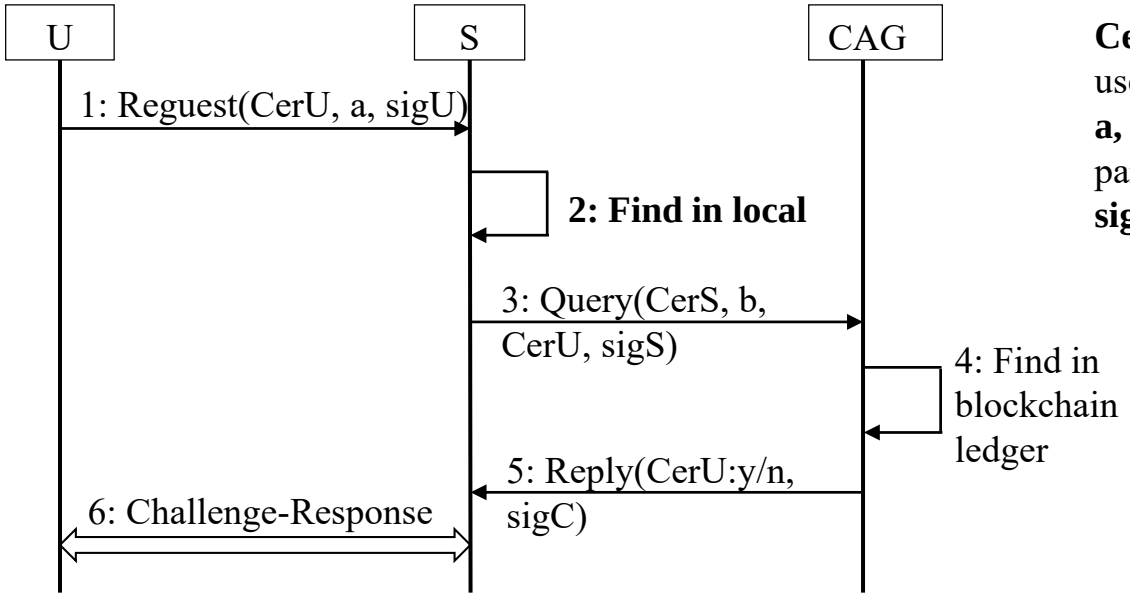


CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step1: User U send access request to Server S. The digital certificate of U is contained in the request package.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.

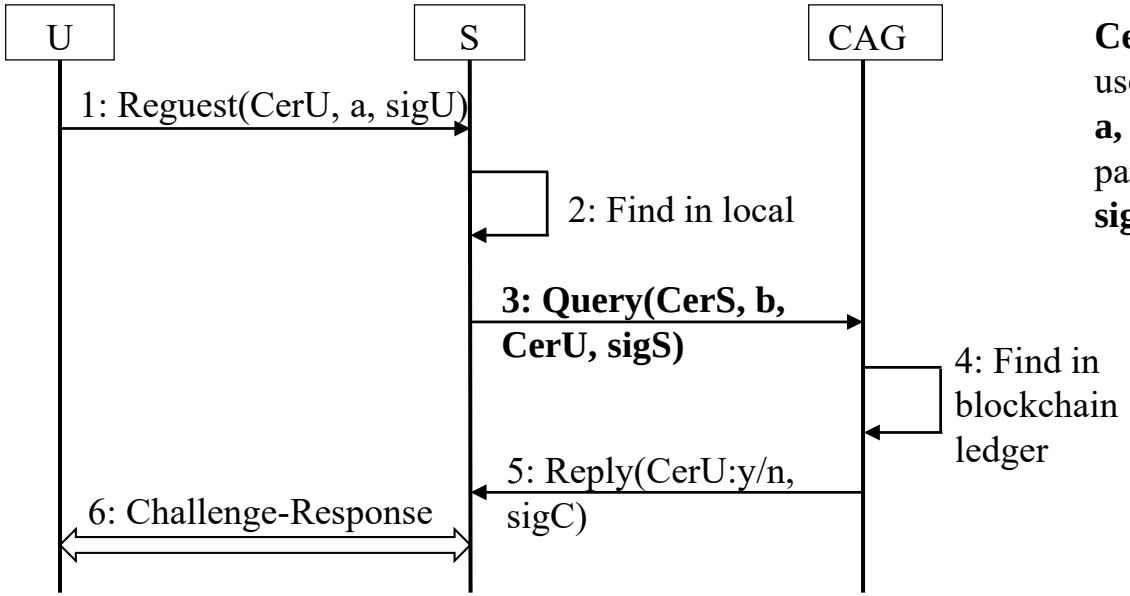


CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step2: Server S tries to find the public key of the CA who issued the digital certificate of U in its local cache.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.

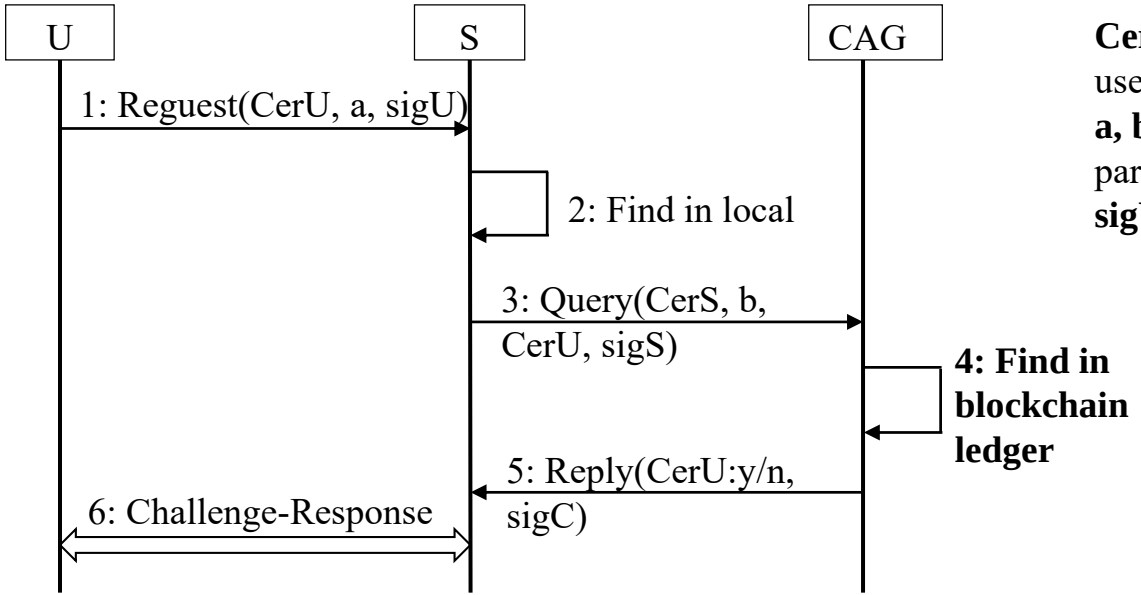


CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step3: If S has not found the right public key, it can not validate the truth of digital certificate U, so S refers to CAG of China for help.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.

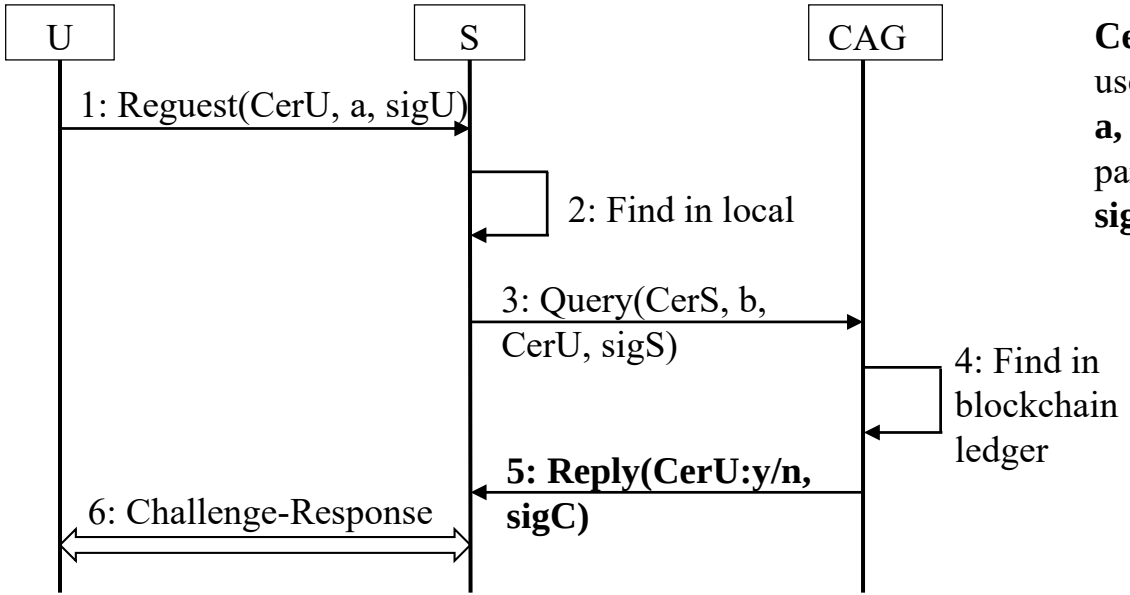


CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step 4: When receiving the query from S, the CAG of China will search for the public key of the CA who issued the digital certificate of U in the blockchain ledger according to the IssuerUniqueID. With the help of the public key of CA, CAG can validate the truth of digital certificate U. At the same time the certificate revocation list is queried to ensure that digital certificate U has not been revoked.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.

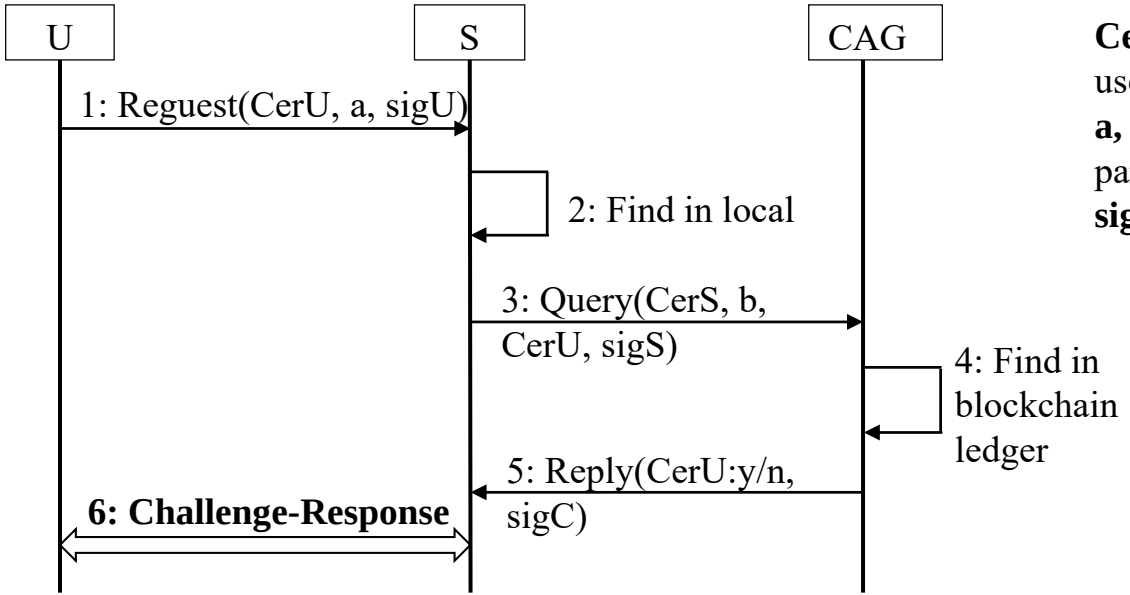


CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step5: The CAG reply S the validity of the digital certificate U.

Typical cross Security Domain authentication process

Use Case: a user U in Korea wants to access a server S in China.



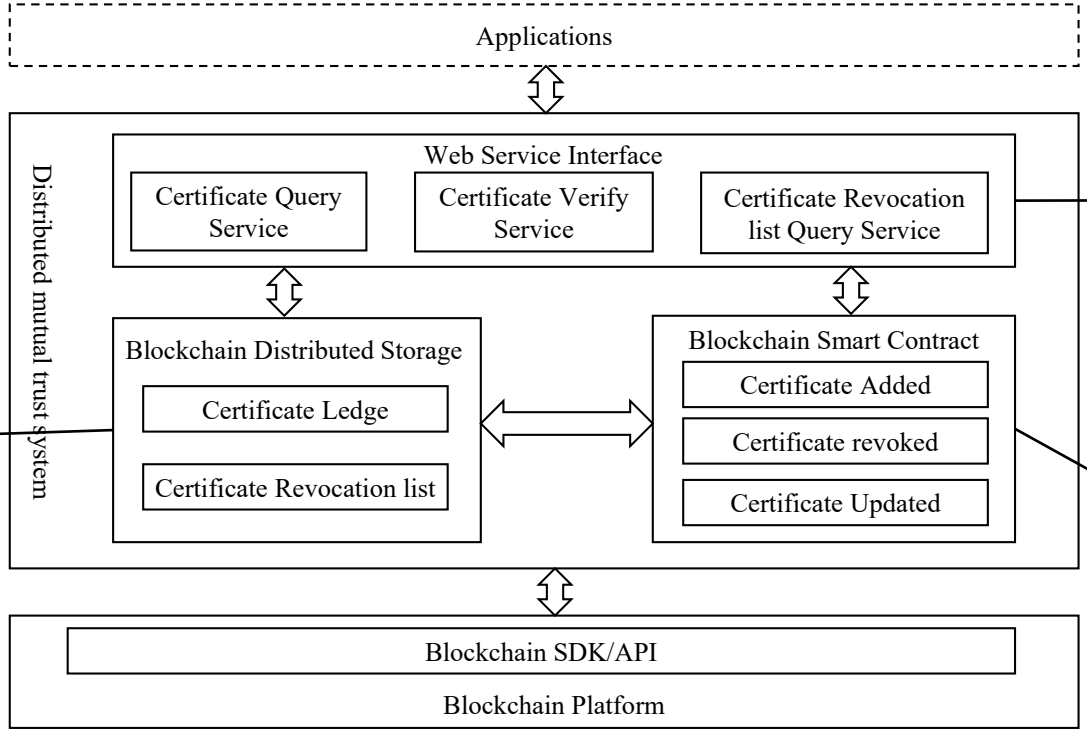
CerU: digital certificate of user U
a, b: authentication parameters
sigU: signature value of U

Step6: After S knows the digital certificate U is valid, it can initiate the subsequent challenge-response authentication process.

Part 6:

SOFTWARE FUNCTIONAL ARCHITECTURE

Software Functional Architecture



provides external standard interface, such as certificate query, certificate verify and so on.

storages the Certificates and the Certificate Revocation lists.

implements the Certificate adding, revoking and updating.

- The bottom layer provides basic functions of blockchain, which exposes the blockchain APIs.
- The middle layer is a distributed mutual trust system, which is composed of three parts.
- The upper layer uses the distributed mutual trust system for security protection, such as Flight Plan Filling.

THANK YOU

Contact information:

Leng Bing,
Southwest Communications Institute of China
Address: Chengdu, Sichuan, China
Tel: +86-13980086683
Email: lengbing@tom.com