中国移动 China Mobile | 研究院 CMRI

DLT based PKI Certificate Management

Junzhi YAN
China Mobile
yanjunzhi@chinamobile.com

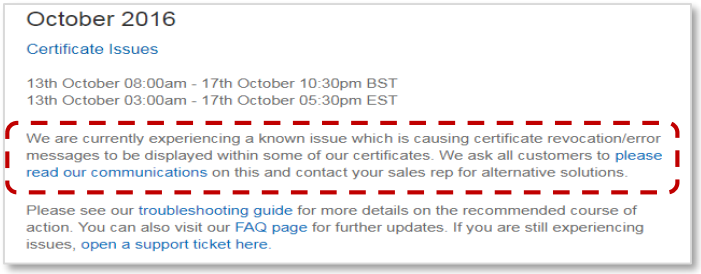
The content of this presentation is mainly from

- *Draft Recommendation ITU-T X.ss-dlt: Security services based on distributed ledger technology*
- *Blockchain based PKI and Certificates Management in Mobile Networks, IEEE TrustCom2020, pp.1764-1770, 2020 DOI:10.1109/TrustCom50675.2020.00242*

Issues of traditional PKI

- **Single point of failure**

Single point of failure of CA, may cause the issued certificates untrusted. (2011)



Single point of failure of CRL/OCSP service, may affect the related authentication progress.(2016)

- **No previsioned trust anchor (trust among multiple CA)**

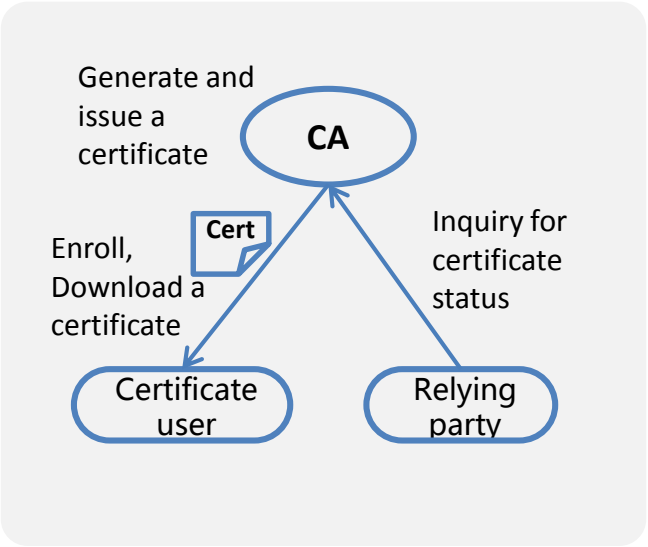
Due to geo-political situations, multiple CAs are required. Vendors have to use the designated CA trusted by the customer/operator.

- **CRL/OCSP is unavailable in intranet**

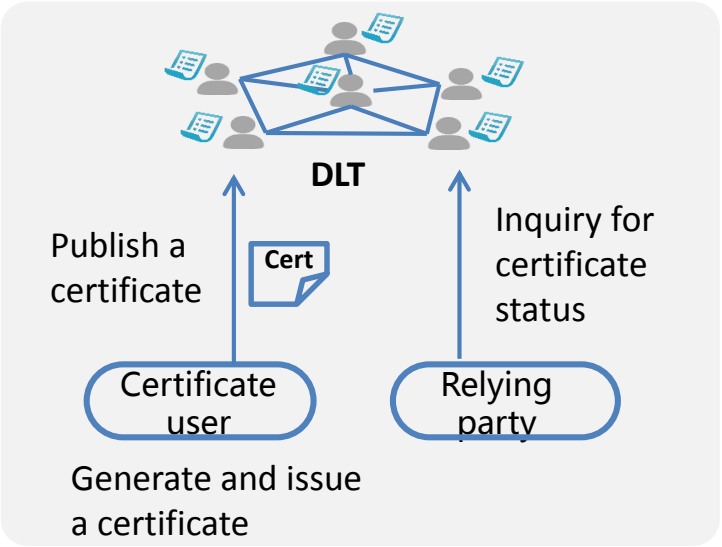
Some devices deployed in the core network cannot access the Internet, NFs(network functions) in 5G core network. The expected security cannot be reached.

Main idea of DLT based PKI certificate management system

Traditional PKI System



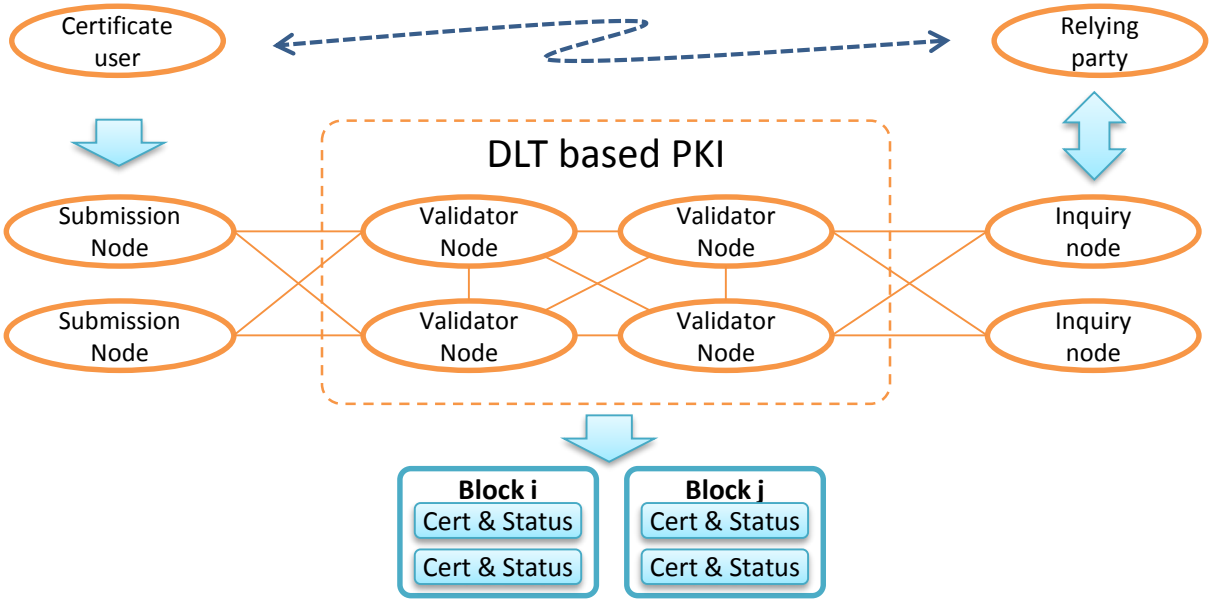
DLT based PKI System



Certificate user is the owner of the certificate. Relying party is an entity that relies on the data in a public-key certificate in making decisions.

- The trustworthiness of certificates relies on they are recorded in the ledger.
- Certificates could be recorded into the ledger after verification and consensus.

Framework of DLT based PKI certificate management system



- **Certificate user**: the owner of the certificate. It could be a device or software client in mobile networks.
- **Relying party:** an entity that relies on the data in a public key certificate in making decisions. The relying party is responsible to check the validity of the certificate by checking the certificate status.
- **Validator node:** the node to verify the received requests and generate new ledgers. The submitted certificates will be verified, only the verified certificates could be recorded into the ledger. They could be held by vendors, operators and service providers, and CAs. Users submit or renew certificates to a validator node. The validator node endorse the certificates recorded into the ledger.
- **Inquiry node:** provides certificate inquiry services. The service includes the certificate inquiry and certificate status inquiry.

Certificate profile

X.509 certificate profile is recommended.

- **Serial Number**

  Serial number is a positive number assigned by the CA in the traditional PKI system. The serial number is unique for each certificate issued by a given CA, and it is used in CRL to identify the revoked certificate. It will not be used in this solution.

- **Subject**

  The subject field identifies the entity associated with the public key stored in the subject public key field, and should contain a distinguished name. *The organization information in the subject filed of the self-signed certificate should be in accordance with the organization information of the submission node.*

  → **Ensure identity endorsement**

- **Key usage extension**

  The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. *If the subject field shows no information about the user's identity and its organization, the key usage extension could be keyAgreement, keyEncipherment, dataEncipherment, but not digitalSignature*.

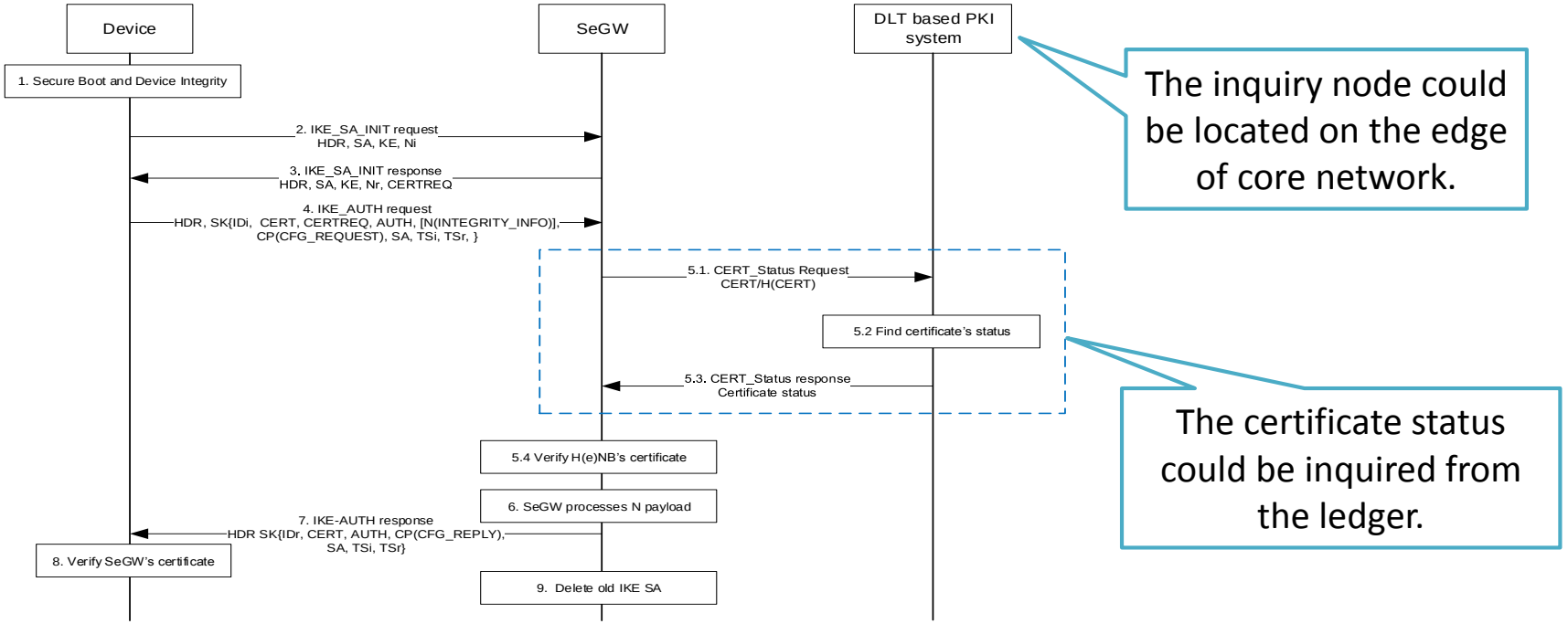
  → **Ensure certificate cannot be wrongly used**

Scenarios——Device certificate provision and authentication

- **Certificate Provision**

1. The vendor generates and provisions private keys and certificates for each device.
2. The vendor submit the certificates into the blockchain PKI system via a submission node. The submission node will endorse the validity of the certificate. ***The organization information in the subject filed of the self-signed certificate should be in accordance with the organization information of the submission node***.
3. The validator nodes verify the certificates and record them into the ledger.

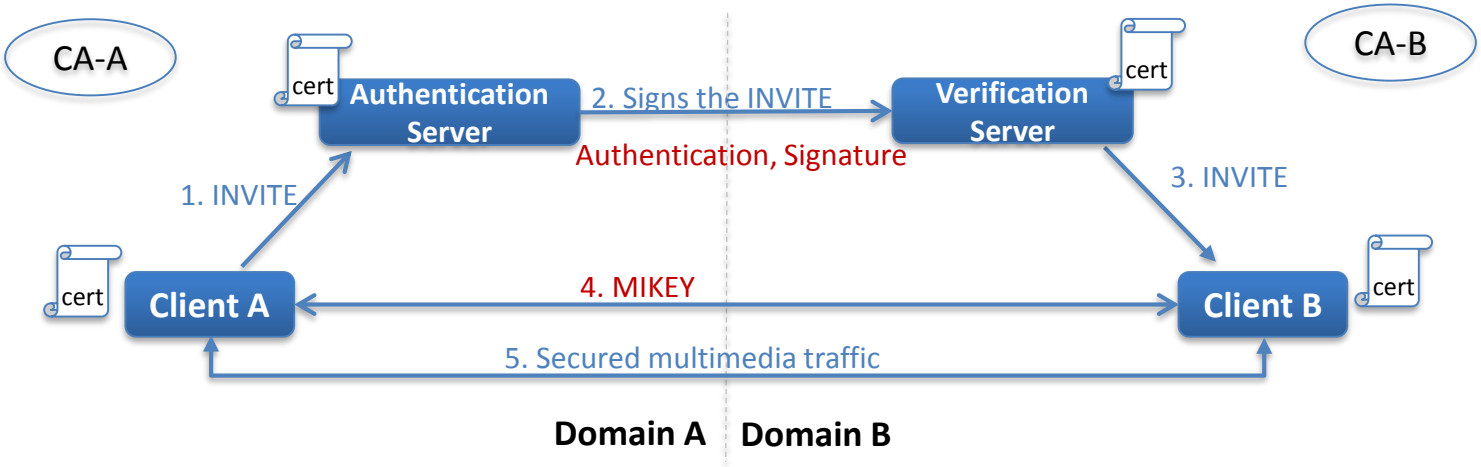
- **Device Authentication**



Next steps

New work item proposal in SG17: *Guidelines for secure voice communications based on DPKI*

- **Key requirements to secure voice telecommunication and issues related with PKI**
  - Authentication of the calling identifier
  - Confidentiality and integrity of voice traffic
  - Each operator has its own CA to manage the certificates. It is difficult for one operator to trust another operator's CA.
- **Proposal**
  - Use DPKI to assure the authenticity of the calling identity
  - Develop the key management schemes based on DPKI for secure voice telecommunication



中国移动
China Mobile

Thank you!