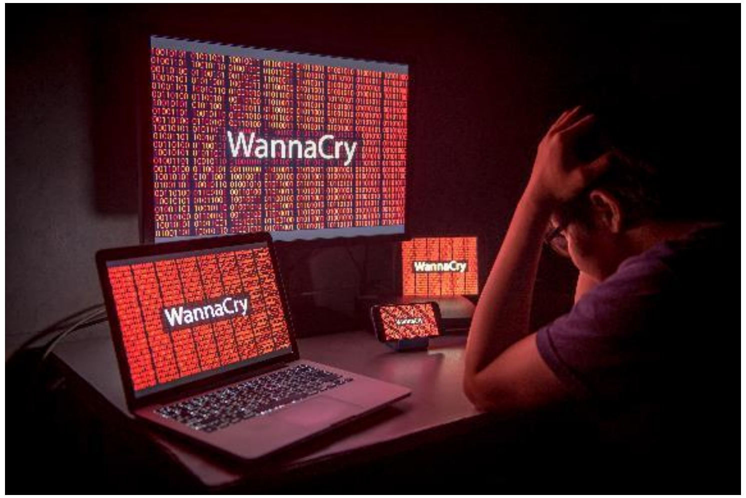
A part of this work was supported by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), ``Cyber Physical Security for IoT Society'' (funding agency: NEDO).

A new use case of attribute certificates: application to software supply chain

Yuto Nakano, Takao Kojima
KDDI Research, Inc

Threats in Supply Chain

- **Connected industries enable flexible supply chains and create additional value**
- **They can also cause new threats**
  - **Malicious chip embedded in hardware**
  - **Attacks against supply chain**



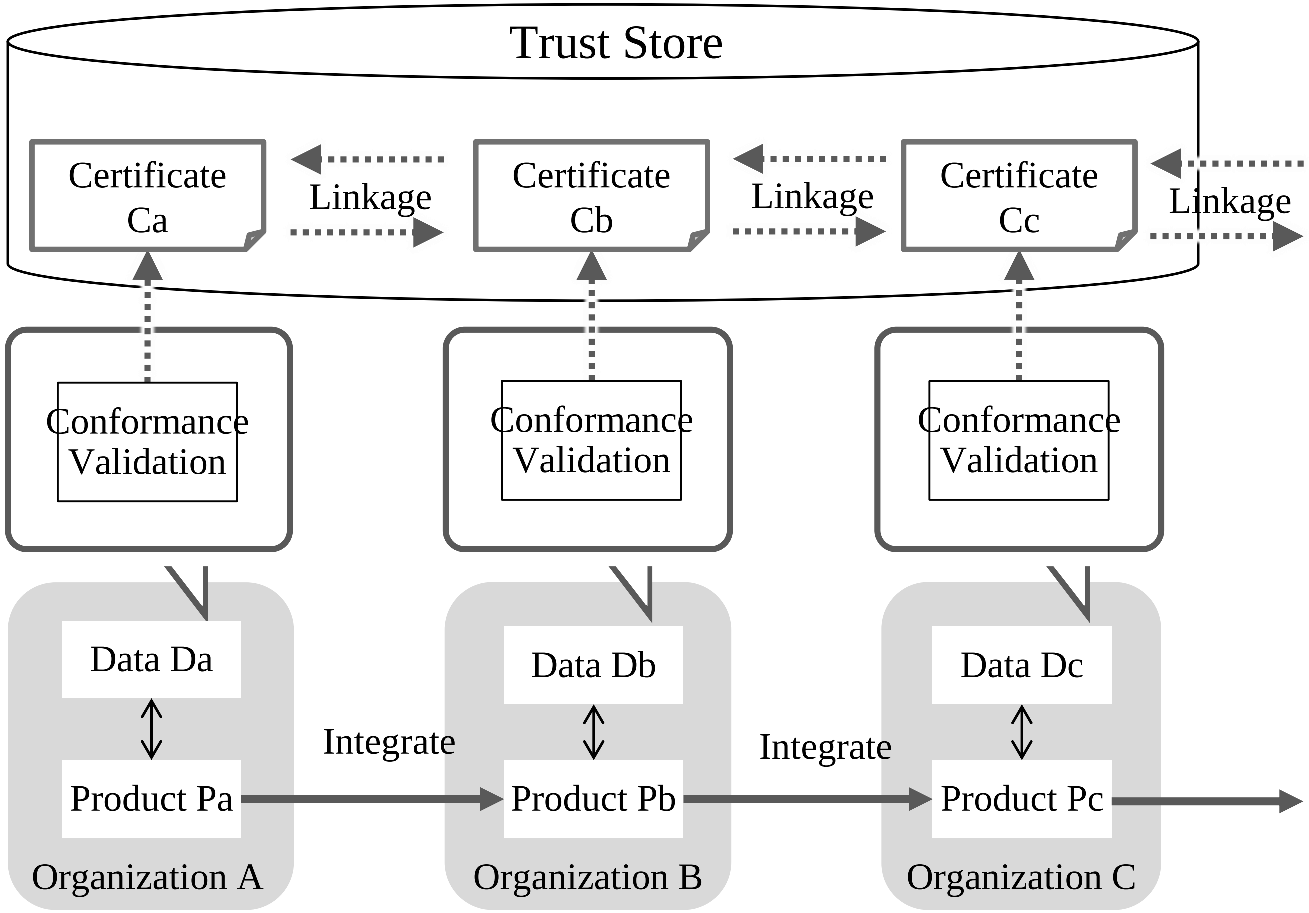
- **New framework that can realize trustworthy supply chains**
  - **Eliminate risks such as malicious chip or data**
  - **Ensure the security level of entire supply chain**

Framework for Security Inspection for Supply Chain

Framework for ensuring the secure usage of data over the supply chain

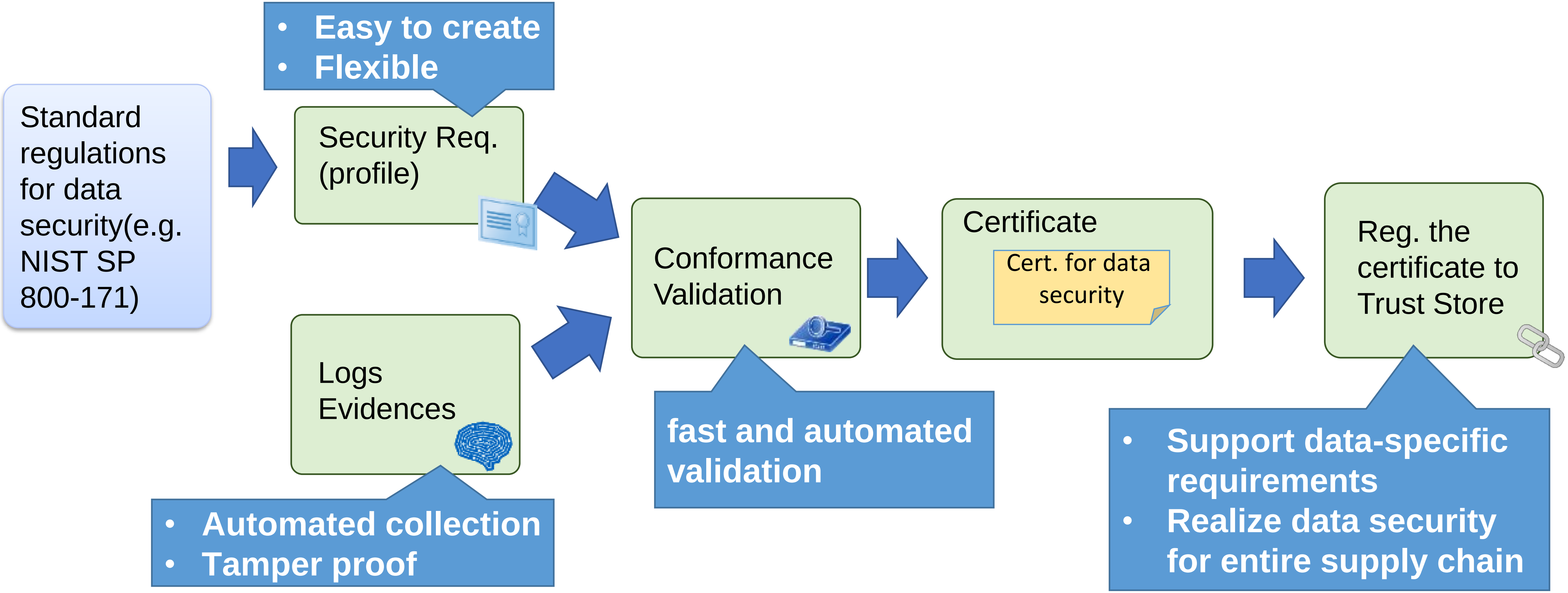
- Simple supply chain of org. A -> org. B -> org. C
- Each organisation produce a product
- Sensitive data (designs, instructions, testing results etc.) will be used in the production phase

- Conformance validation ensures the secure management of data in the organisation
- The result will be issued as a certificate
- Trust Store connects certificates to ensure the secure usage for entire supply chain



Security Inspection for each organization

✓ Automated inspection with conformance validation



Standard regulations for data security(e.g. NIST SP 800-171)

Security Req. (profile)

- Easy to create
- Flexible

Logs Evidences

- Automated collection
- Tamper proof

Conformance Validation

fast and automated validation

Certificate

Cert. for data security

Reg. the certificate to Trust Store

- Support data-specific requirements
- Realize data security for entire supply chain

The suggestion to ITU-T

The suggestion overview to ITU-T

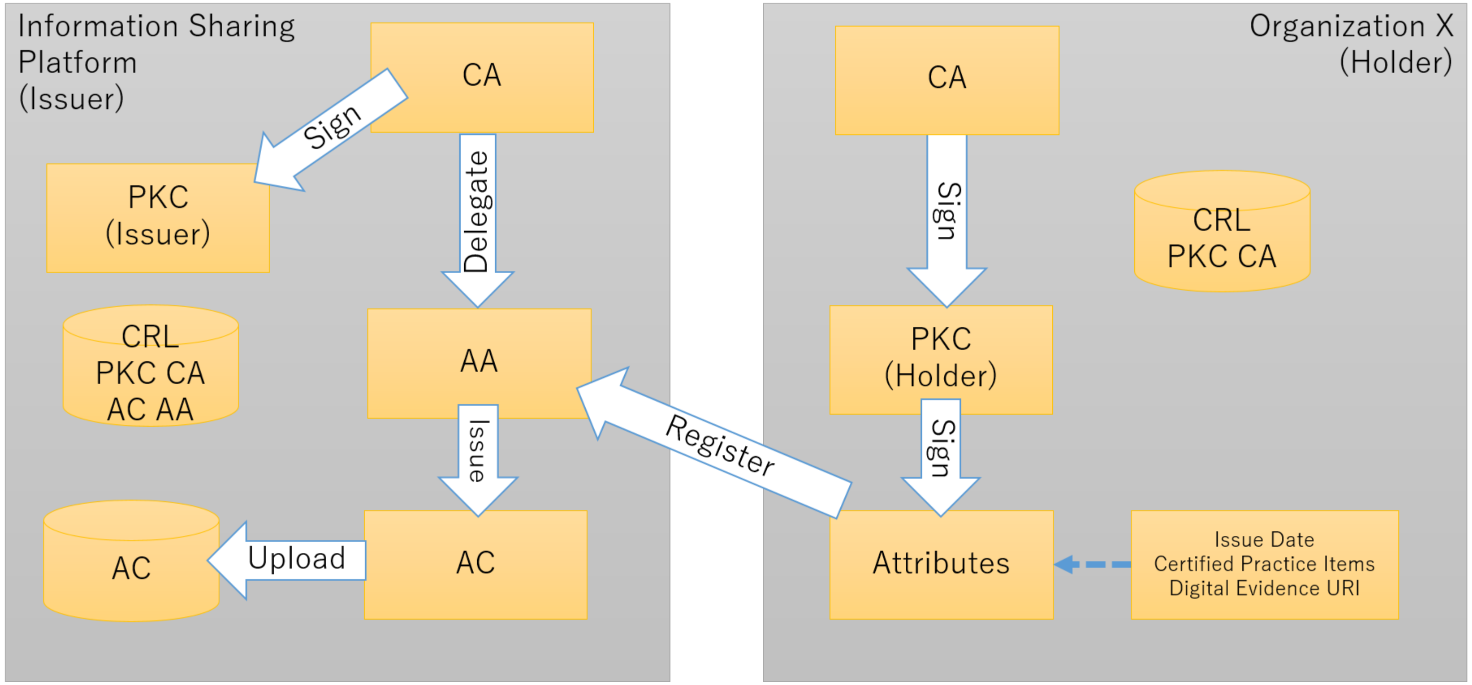
- **A new use case of X.509 Attribute Certificate for Supply Chain**

- Technical Report in ITU-T SG17 TR.x590ac4sc has been working.

- Overview
  - Information Sharing Platform using X.509 Attribute Certificate(AC)
  - Issuing AC with attributes that show a certain requirement is satisfied.
  - Ensuring a certain requirement is satisfied among the supply chain with sharing AC.

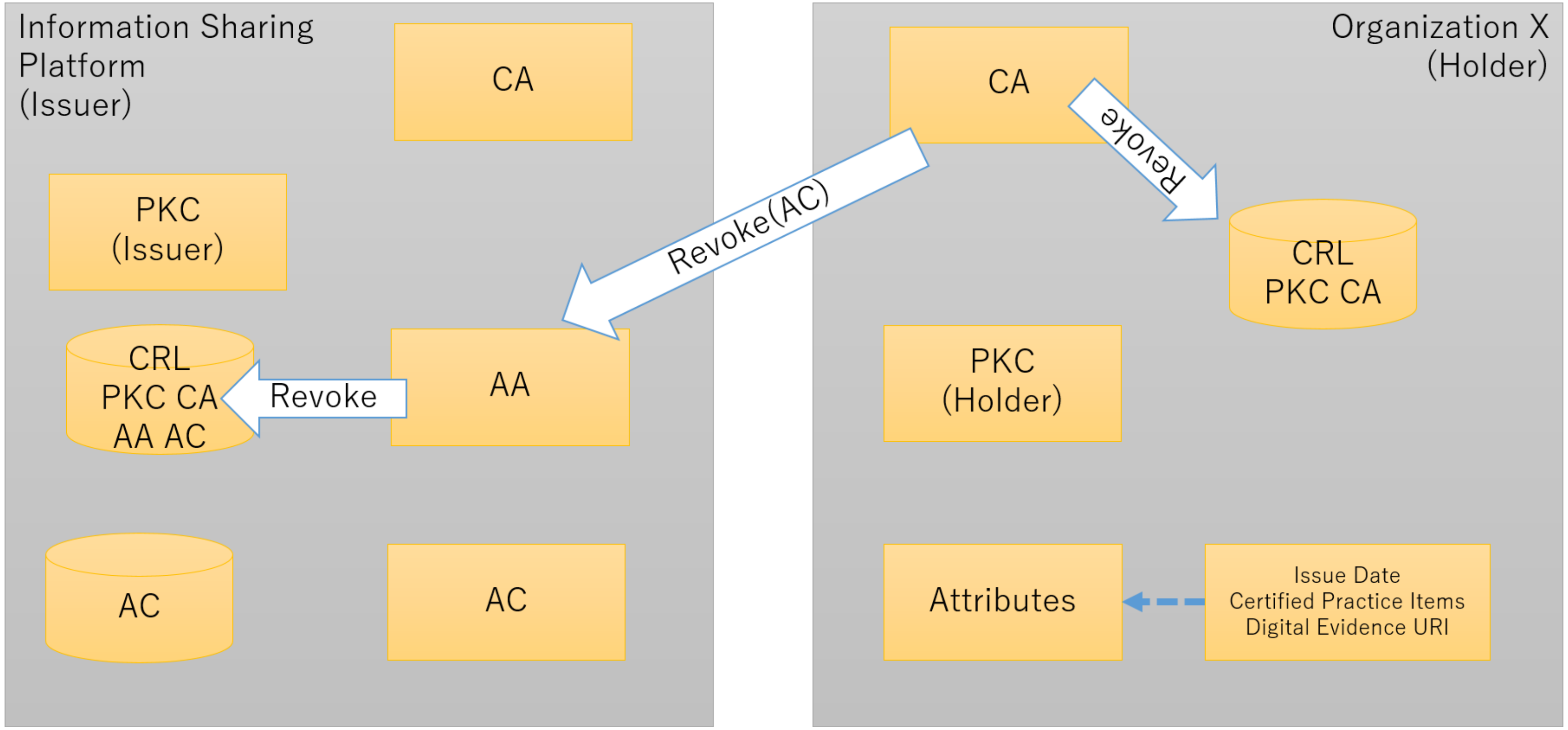
Issuing Certificate

- Trusted entity manages CA(Certificate Authority) and AA(Attribute Certificate Authority)
  - Organizations perform conformance validation.
    They send a request to AA to issue AC with attributes regarding conformance validation results.
  - AA checks identity of the organization and its PKC(Public Key Certificate).
    AA publishes AC with attributes itself.
- Trusted entity manages and issues AC.



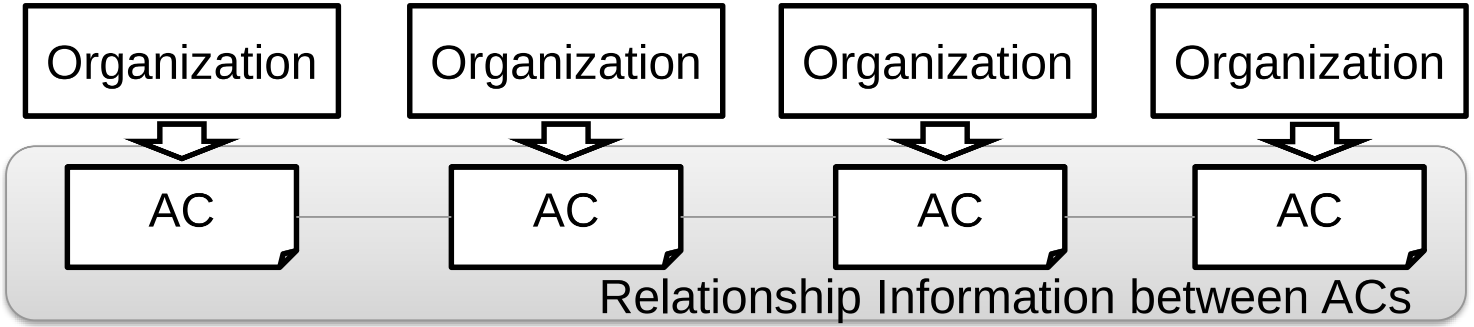
Revoking Certificate

- Organizations sends a request to CA.
  CA revokes PKC and updates PKC CRL(Certificate Revocation List).
- Organizations sends a request to AA. AA revokes AC and updates AC CRL.
- CRL for organizations are referred via OCSP(Online Certificate Status Protocol).



Relationship Management between ACs

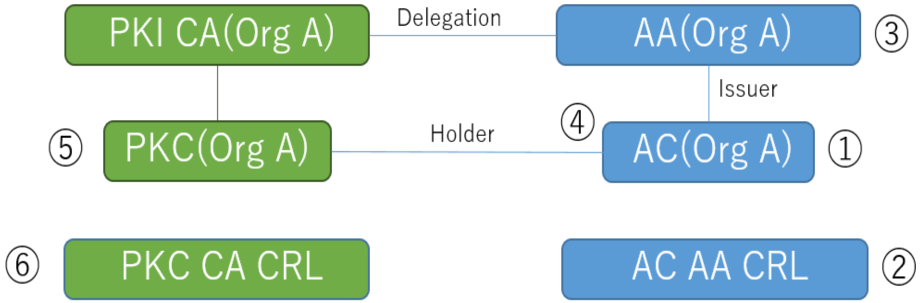
- Manage ACs published by organizations on repository.
- Manage Relationship Information between ACs
  as relationship between organizations in the supply chain.
  - Use case: verifying the entire supply chain. Information sharing in incident response.



Verifying Certificate

- Verification phases can be selected depending on the use-case or circumstance.
  - Verifying all phase each time costs high. Select phases as needed.

Phase	Description
①	Validity verification for AC. Signature is verified.
②	Certificate Status verification for AC and AA via CRL and OCSP.
③	Validity verification for certificate of AA. Signature is verified.
④	Identity verification for PKC associated with AC.
⑤	Validity verification of PKC. Signature and Path are verified.
⑥	Certificate status verification for PKC and CA via CRL and OCSP.



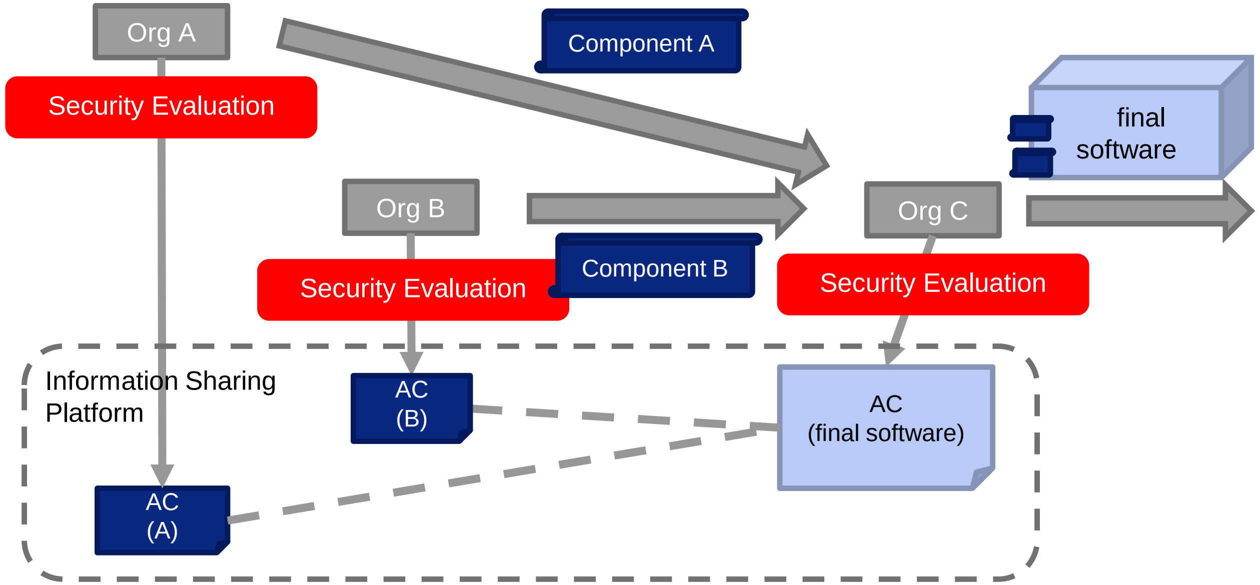
Use case: SBOM (Software Bill Of Materials)

- Vulnerability:
  Malicious or vulnerable functions can be installed into software.

- Goal:
  Preventing from installing of vulnerabilities
  with sharing security evaluation results in the whole supply chain.

- Solution Steps:
  - Perform security evaluation for each developing components in the software.
  - Issue AC that attribute show "This component doesn't include vulnerabilities."
  - Verify the entire supply chain with ACs

- What attributes may be included in X.509 AC:
  Security Evaluation Results



Takeaway

KDDI Research

■ **Framework for Security Inspection for Supply Chain**

- Eliminates risk such as malicious hardware and software
- Ensures the security level of the entire supply chain
- Automates inspection with conformance validation

■ **ITU-T SG 17 Technical Report .x590ac4sc**
A new use case of X.509 Attribute Certificates (AC)

- Issues AC with attribute that shows a certain requirement is satisfied.
- Ensures a certain requirement is satisfied
  among the supply chain with sharing ACs.
- Information Sharing Platform
- SBOM is one of usecases

KDDI

KDDI Research