# Simple Localized management of trusted Web PKI certificate supporting fine-grained configuration for Internet browser

draft-liu-lamps-browser-webpki-cert-preservation

**Yu Fu (China Unicom)**
**Penghui Liu (PCNL)**

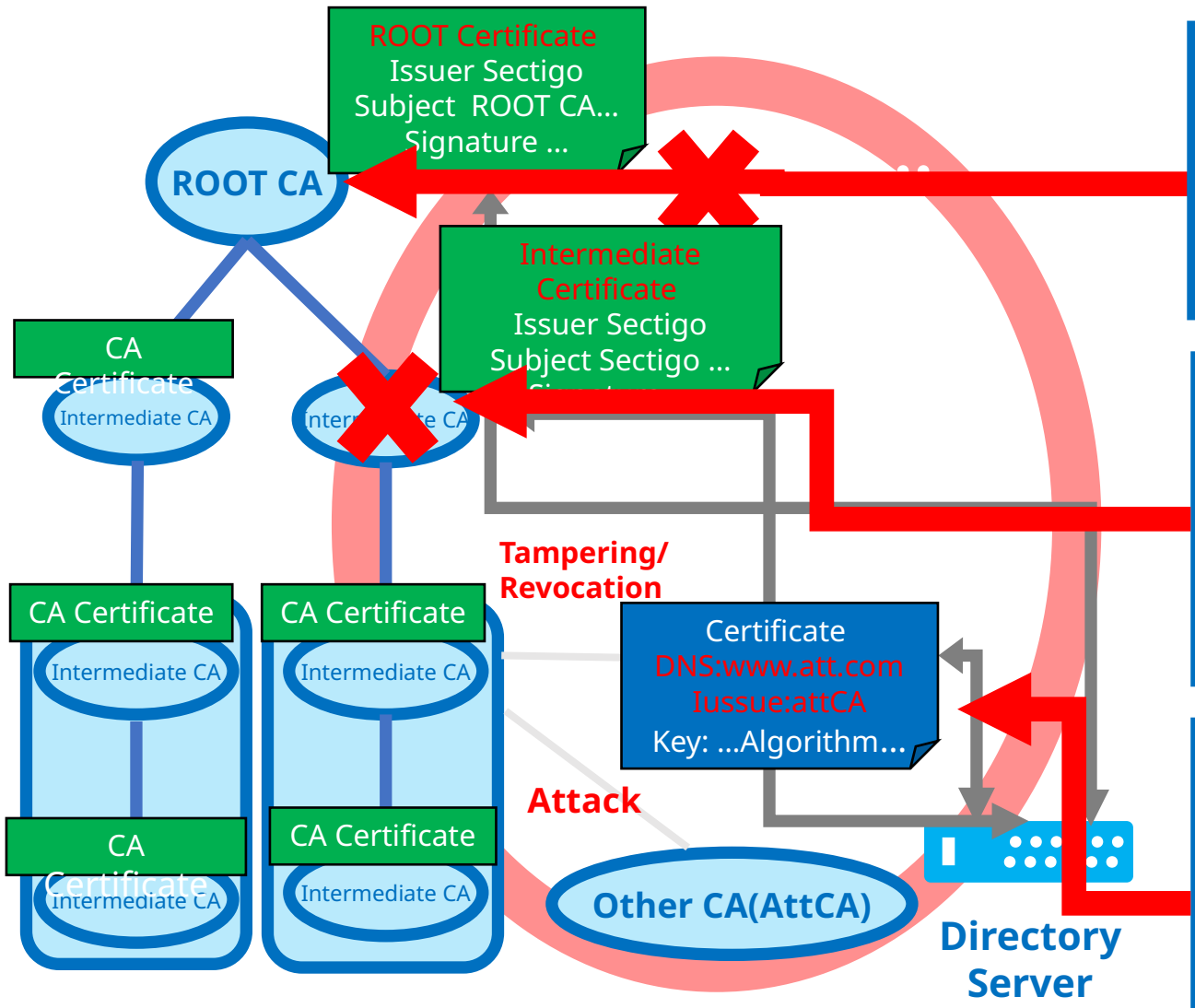
March 3, 2025

# motivation

The management of Web PKI certificate resources presents a challenge when the misalignment of ownership and management rights over certificate resources of one organization creating a risk of unilateral suspension and revocation by another competing organizations.

This situation undermines the stability of critical infrastructure and affects the integrity of authentication systems.

# motivation



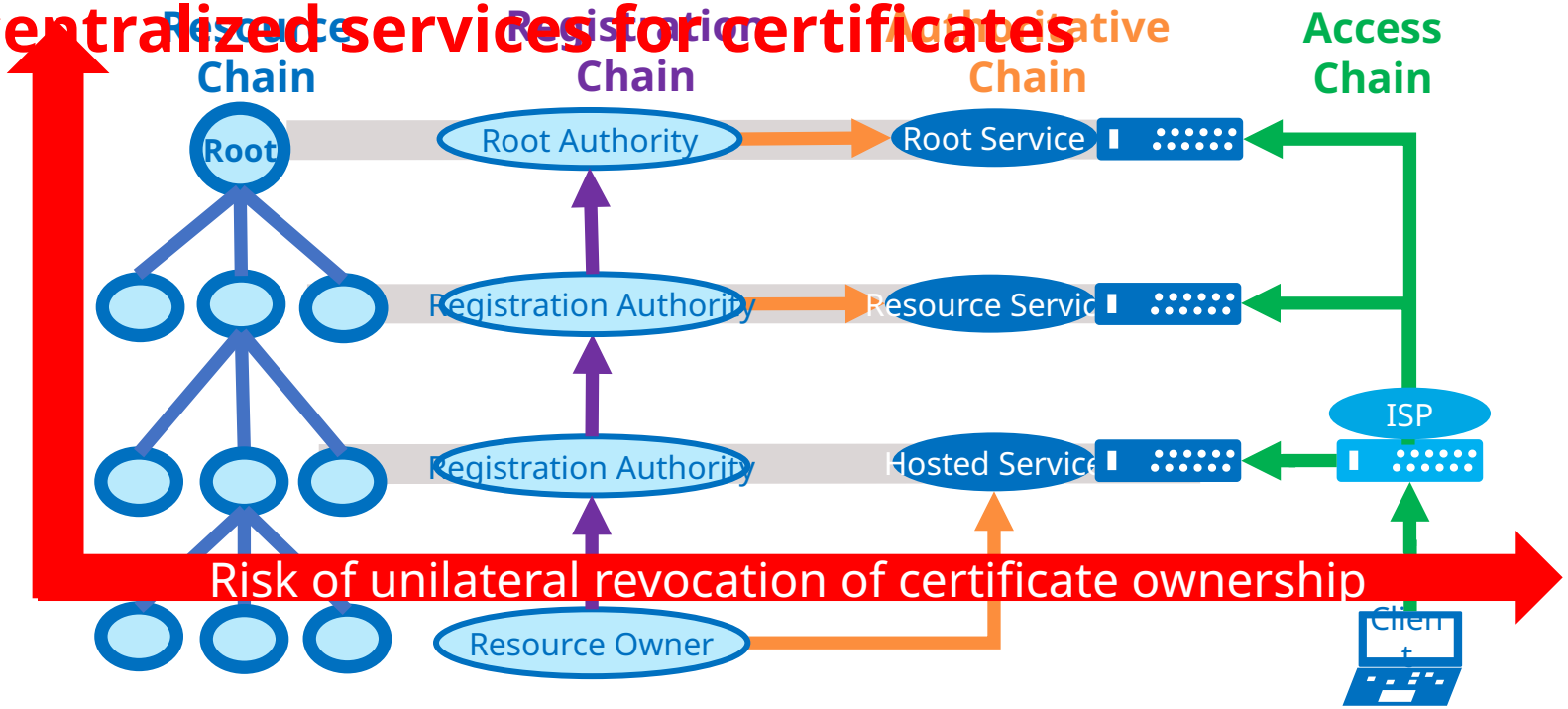

**Risk of root CA stop certificate service (Isolation and Blinding Risk)**: *Once a root CA registered in another competitive organization stops certificate issuance services or network interruption, it will cause certificate service interruption.*

**Risk of intermediate root deletion (Disappearance Risk)**: *Once an intermediate root registered under another organization's root CA is deleted, all certificate services issued by this intermediate root and its subordinate CAs will disappear.*

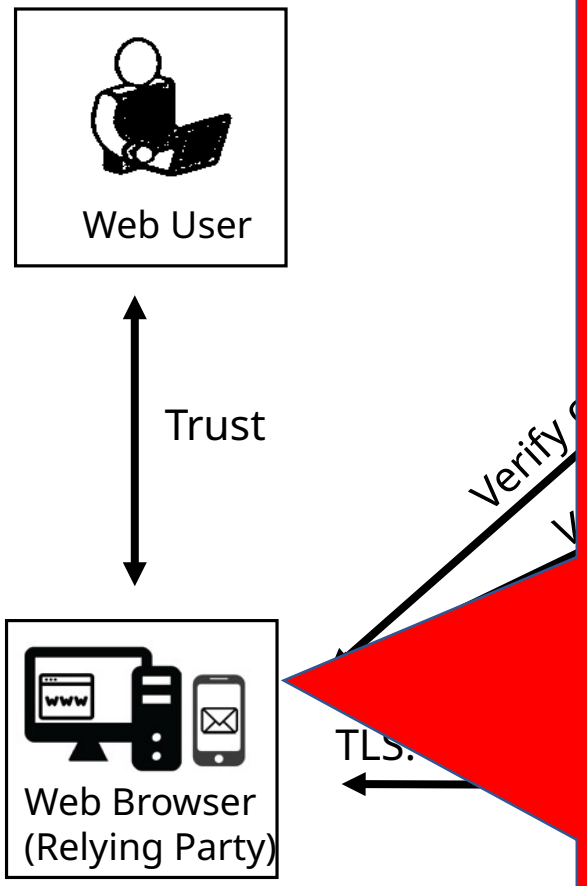
**Risk of certificate being tampered with or revoked (Hijacking Risk)**: *CA is attacked or performs malicious revocation operations, and issues certificates containing false information, causing the website to be hijacked, and the revocation will directly cause the website certificate to be unusable.*

# motivation

- In a hierarchical architecture, superiors control subordinates, and subordinates have ownership but lack control
- There is a conflict between the network sovereignty and the CA jurisdiction
- Economically, most certificates are provided by minor institutions, leading to a trend of centralized services for certificates



# Simple Localized management framework

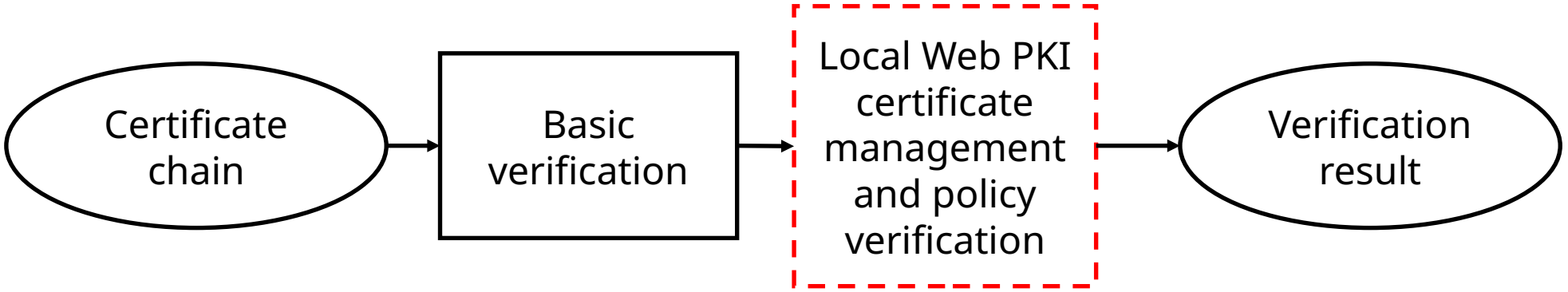



**Trust originates from Localize management**

**In this framework, by localized certificate management with fine-grained configuration. the web user such as a nation or a large group can acquire the trust from the Web browser (relying party), which is responsible to verify the certificate issued by the corresponding CA during TLS communication with Web server, where the Web browser (relying party) can judge by itself whether the target certificate is legal or not according to the local certificate management repository, which is used to store the fine-grained certificate management policies configured by the system manager as per the instructions and data released by the trusted authoritative institutions.**

*Currently, no specific standards exist for these scenarios, some Internet browsers may provide related configurations that ignore all certificate errors or are similar to whitelists. However, generally ignoring all SSL/TLS certificate verification errors is considered unsecure and poses serious security risks.*

# Simple Localized management framework




After the basic certificate verification process, the browser or its proxy verifies whether the target certificate exists in the whitelist items of the current certificate management policy repository configured locally. If so, it further checks whether the certificate status error happened during the basic certificate verification process is the same as the error specified in the user configured policy, such as certificate being reclaimed or expired etc., If so, the current target certificate is still considered valid.

Additionally, according to the policy configured in the certificate management repository, such as the local blacklist certificate list, the browser or its proxy verifies whether the target certificate exists in the blacklist list. If so, regardless of any errors in the basic certificate verification process, the current target certificate should be considered invalid and the corresponding network certificate status should be displayed

# Simple Localized management framework

```
{
  "Version": 1,
  "LocalCertWhiteFilters": {
      "ErrorNo": Type Int,
      "CertWhiteFilters": [
          "comment": Type String,
      }
    ],
  }
}
```

The format of the certificate management repository can be defined based on JSON files and database table:

```
Table LocalCertWhiteFilters (
        id                  INTEGER PRIMARY KEY,
        Version             INTEGER DEFAULT 1,
        ErrorNo             INTEGER DEFAULT 201,
        serialNumber        INTEGER DEFAULT NULL,
        subjectName         BLOB DEFAULT NULL,
        subjectAltName      BLOB DEFAULT NULL,
        comment             STRING DEFAULT NULL,
);
```

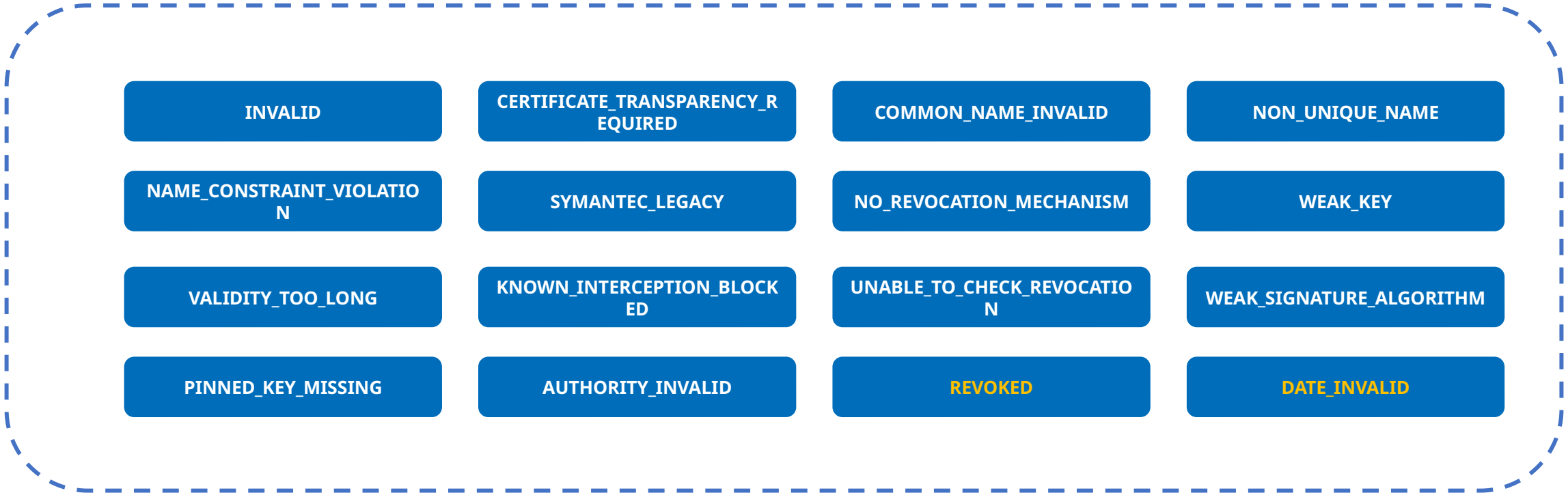
```
Table LocalCertBlackAssertions (
        id                  INTEGER PRIMARY KEY,
        Version             INTEGER DEFAULT 1,
        serialNumber        INTEGER NOT NULL,
        subjectName         BLOB DEFAULT NULL,
        subjectAltName      BLOB DEFAULT NULL,
        issuerName          BLOB DEFAULT NULL,
        issuerAltName       BLOB DEFAULT NULL,
        comment             STRING DEFAULT NULL,
);
```

certificate issuer;

- "Comment" is the annotation for this configuration item.

# Simple Localized management framework

This draft supports fine-grained configuration for the List of Certificate Error Types:



# Security considerations and Conclusion

This mechanism addresses the security issues of domain name certificate resources in network infrastructure, namely the risk of unilateral suspension and revocation of certificate ownership due to the mismatch between ownership and management rights of certificate resources; Cleverly resolving the contradiction between unity and autonomy, key infrastructure improvement and stability, compatible with the contradiction between existing and smooth substitution, compatible with existing authentication systems, enabling stakeholders in the network to smoothly replace existing authentication, cope with the impact of malicious revocation of important industry certificates, and ensure the safe and normal operation of important industry systems. For this reason, Internet browsers (relying parties or their agents) conforming to this mechanism can autonomously decide and process any certificate and its verification results asserted by the local certificate management database according to local management requirements.

This mechanism is applicable to the implementation and application of the Internet browser certificate resource management system based on Web PKI, and it is applicable to ensuring the smooth operation of the secure network access related to the business of an organization, without being subject to the management and control of other organizations that may have competitive interests; The Internet browser local certificate management specifications defined in this section are universal, and can also be applied to other similar network security applications and environments of different types based on PKI mechanism.

# Thanks