

ACME

Extension for Public Key Challenges

[draft-geng-acme-public-key-05](#)

Geng Feng, [Wu Panyu](#), Xia Liang, [Chen Xin](#)

Huawei,

Huawei,

Huawei,

TrustAsia

IETF 125
Shenzhen

Update and Summary

- Present pk challenge
 - A Brief Overview of the Motivation;
 - Basic framework of pk-01 (including the optional removal of CSR);
 - **Web PKI**: Implement CSR removal using pk-01 (pk-dns-01, pk-http-01...);
 - **Non-Web PKI**: Issue certificates to devices/users;
- Other use cases:
 - Propose the integration of pk-01 and Opaque protocol;
 - Cross-domain in different PKIs;
- Our next steps
 - The document was subsequently split into pk-01 baseline and other use cases.

A Brief Overview of the Motivation

1 Web-PKI

In ACME, certificate requests require the client to submit a CSR (Certificate Signing Request)

However, **CSR in ACME can be a burden on client implementations.**

-> Implement CSR removal using pk-01

2 Non-Web PKI

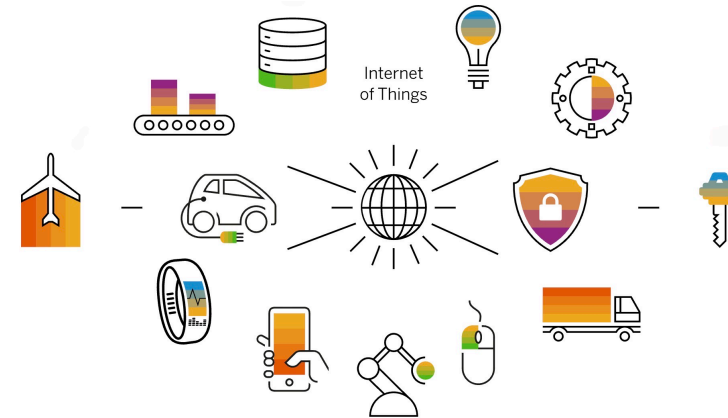
ACME today primarily automates Web PKI:

- server certificates
- DNS / HTTP resource validation

However, many modern systems are built around **public-key identities for users and devices.**

No domain names and public IP addresses, cannot open ports 80/443, and cannot modify DNS settings.

-> Issue certificates to devices/users using pk-01 (remove CSR)



pk-01 basic Framework for Web/Non-Web PKI Environments



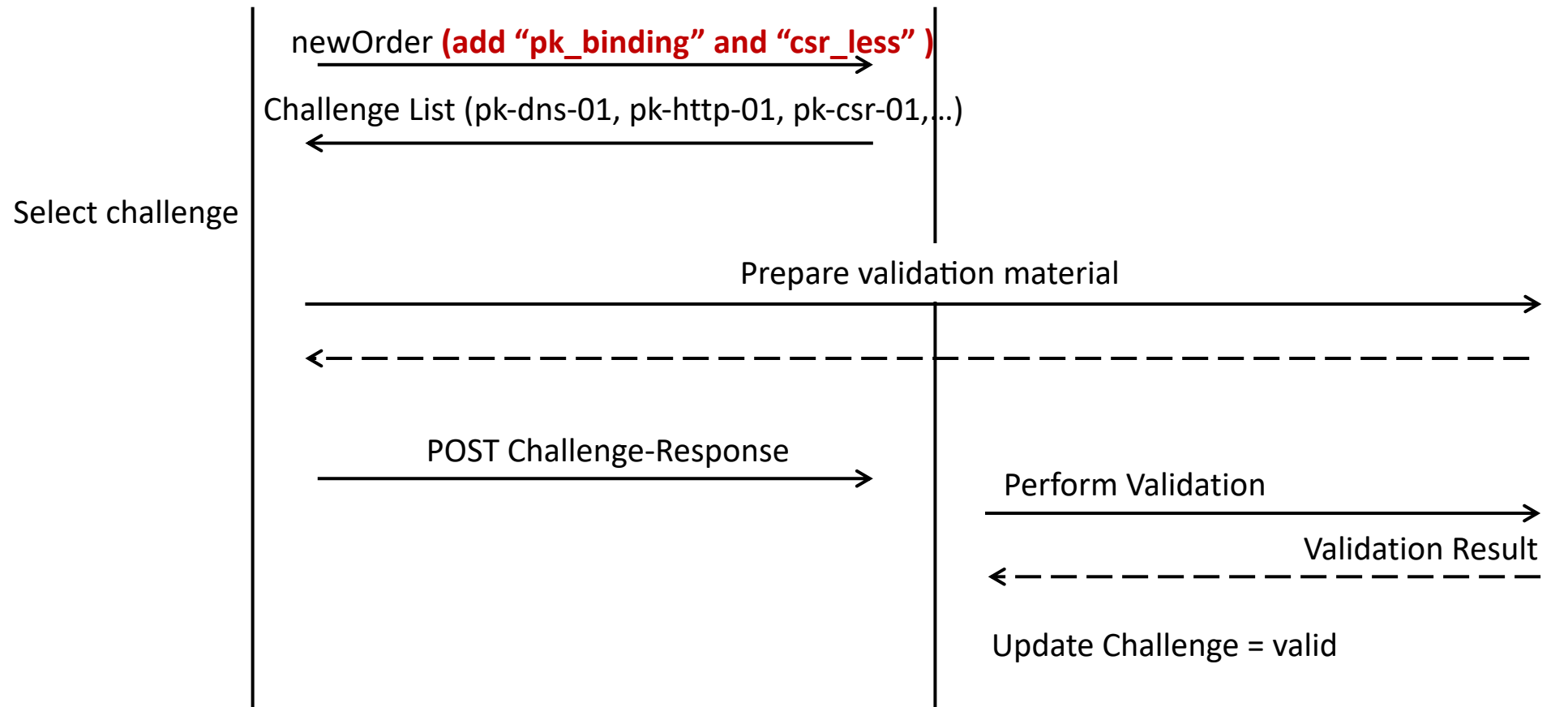
ACME Client



ACME Server



Identity Provider
(Web / no-Web IdP)



pk-01 Enables CSR Removal: Technical Feasibility

CSR Components Replaced by pk-01 Mechanism



CSR Component

| | | |
|----------------------|------------|--------------------------------------|
| Subject | - - - - -> | derived from order.identifiers |
| subjectPublicKeyInfo | - - - - -> | pk_binding |
| SAN extension | - - - - -> | order.identifiers |
| CSR signature | - - - - -> | pk-01 proof of key possession |

Replaced by in pk-01

All functional roles of the CSR are already fulfilled during the pk-01 challenge process. Therefore, a separate CSR object becomes unnecessary in the issuance workflow.

pk-01 Proof of Possession (PoP) in Web/Non-Web PKI

| PKI Context | Challenge Type | Challenge response value |
|--|----------------|---|
| Web PKI (Domain control + pk-01 signature) | pk-http-01 | token \ \ "." \ \ base64url(JWK_Thumbprint(accountKey)) \ \ "." \ \ base64url(Sign(claimedPrivateKey , token)) |
| | pk-email-01 | token \ \ "." \ \ base64url(JWK_Thumbprint(accountKey)) \ \ "." \ \ base64url(Sign(claimedPrivateKey , token)) |
| | pk-dns-01 | base64url(Sign(claimedPrivateKey , SHA-256(keyAuthorization))) |
| | pk-tls-alpn-01 | Sign(claimedPrivateKey , SHA-256(keyAuthorization)) |
| Non-Web PKI | pk-csr-01 | Public Key Authentication |
| | pk-cert-01 | Public Key Authentication |

The optional CSR removal mechanism: Field definitions

Order Submission Stage

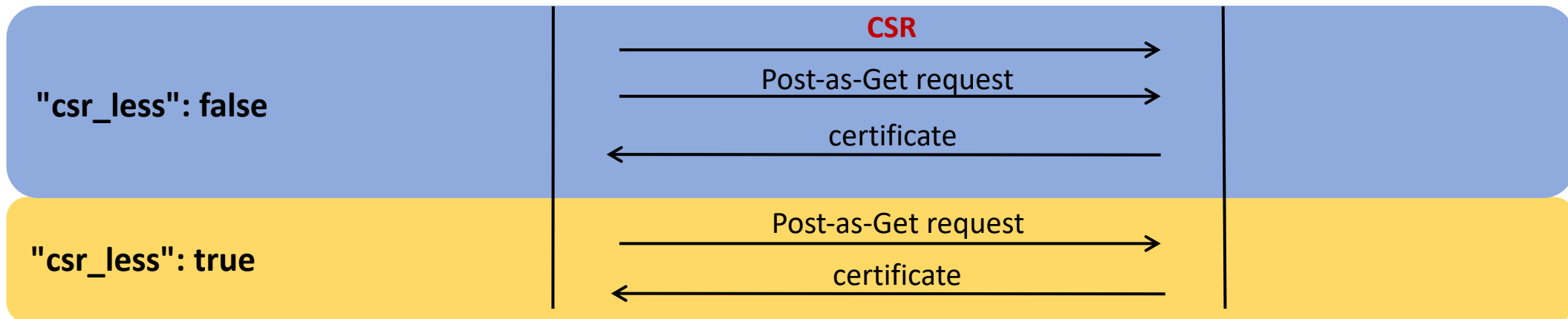
```
{
  "identifiers": [
    { "type": "dns", "value": "example.com" }
  ],
  "pk_binding": {
    "type": "dns-01",
    "public_key": "<Applicant public key, Base64URL-encoded SubjectPublicKeyInfo (SPKI)>"
  },
  "csr_less": true
}
```



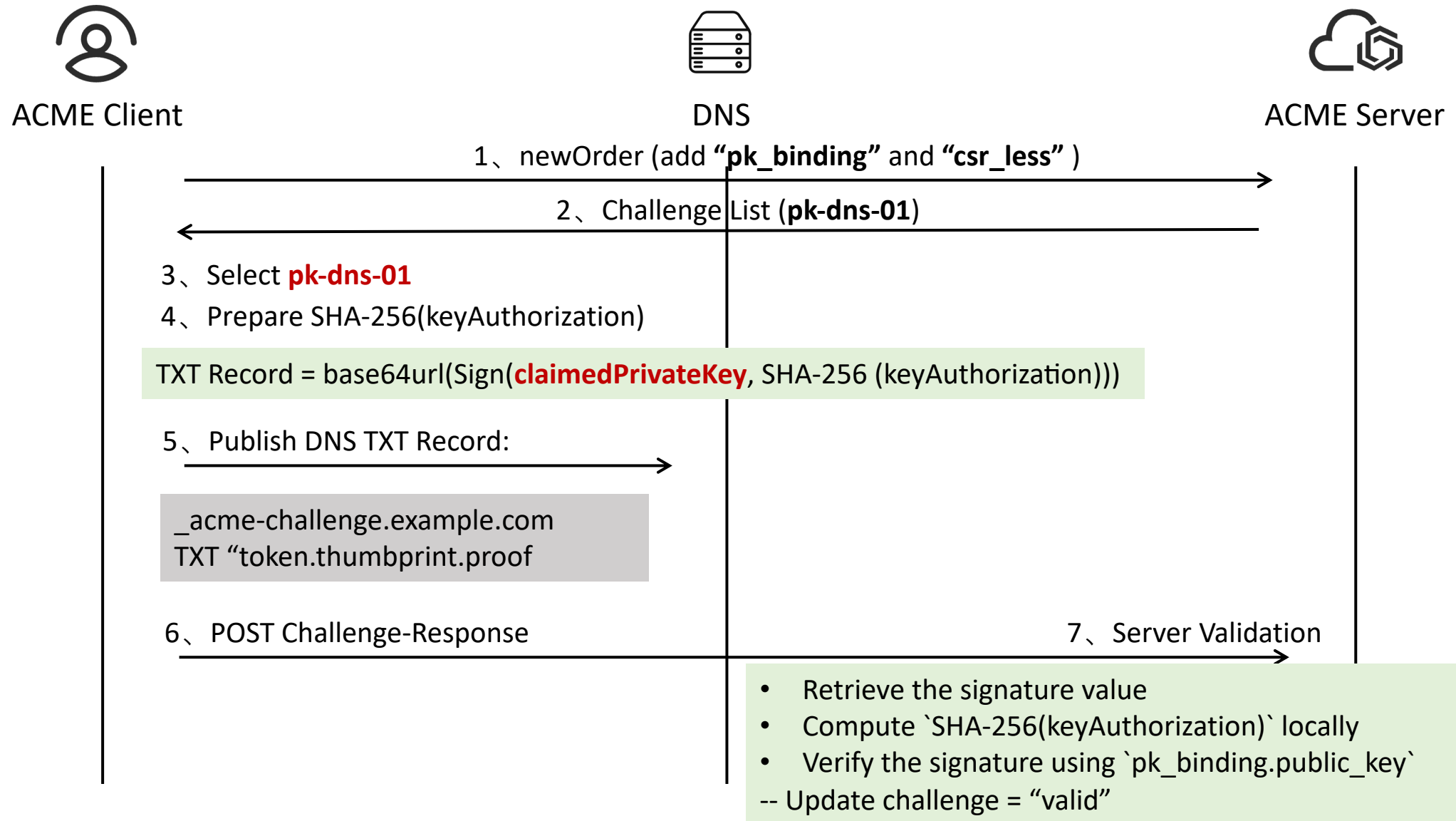
ACME Client



ACME Server

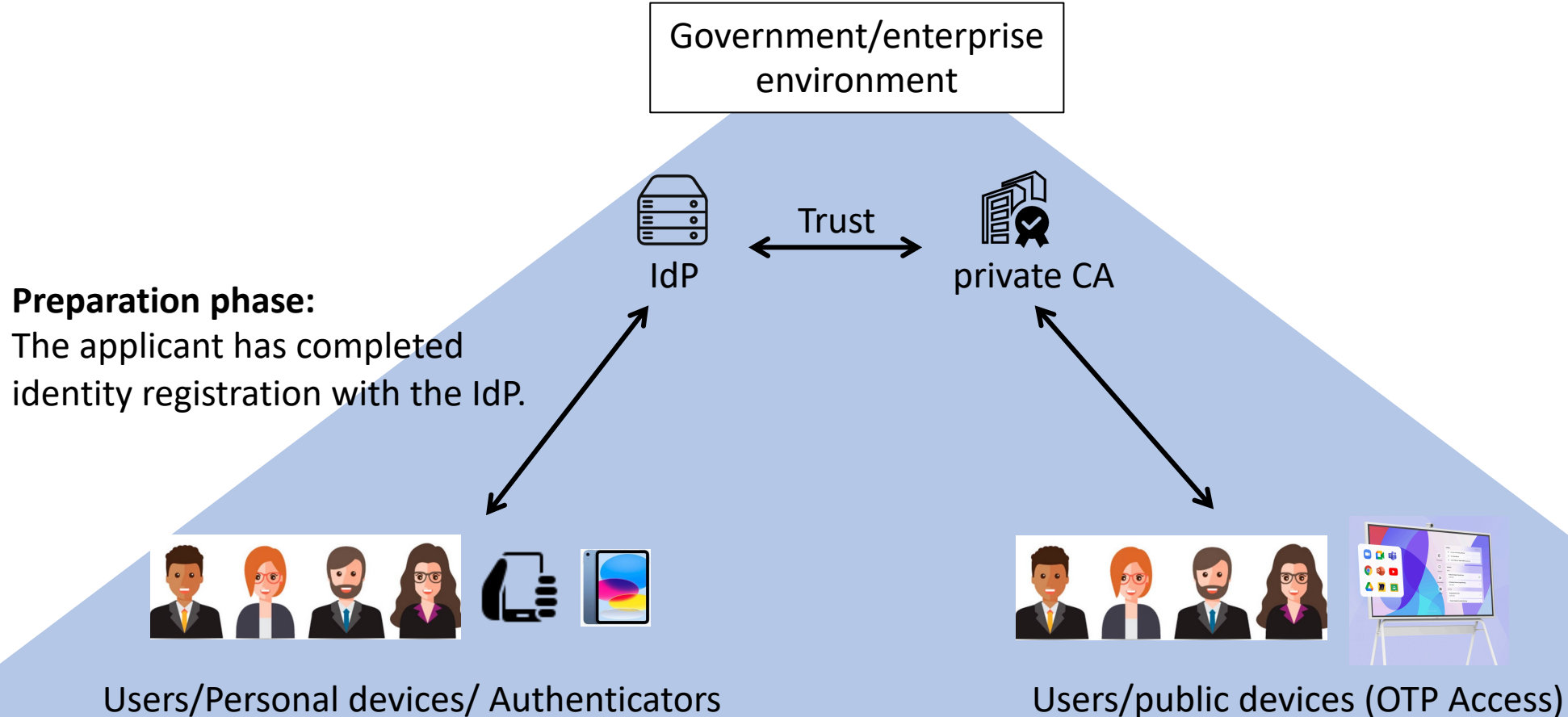


Process Flow for Removing the CSR from dns-01 [pk-dns-01]



Non-Web PKI - Issue certificates for users/devices

- ✓ Automated Certificate provisioning for Internal Network Devices (Government and Enterprises)
- ✓ Automated Certification for IoT Devices
- ✓ Automated Certification for 5G/6G Edge Nodes
- ✓ Automated Certification for V2X/TSP Platforms
- ✓




Combined with OPAQUE [Split into a second draft]

This solution enables users to securely recover and verify their public key identities using a password **on public terminals or IoT devices**, thereby fully automating the certificate application process.


Applicant


ACME Server


IdP (RFC 9807)

1. opaque-registration

newOrder (Identifier: pk)

2. Challenge Initiation

Challenge (Token, pk_url)

3. Online AKE & Token Binding

GenerateKE1(pwd, Context=Token)

KE1 (Includes token)

KE2 (Includes Envelope)

RecoverCredentials & PoP: Sign(SKtemp, Token)

KE3 + [PKtemp, sign]

ServerFinish & Verify PoP

4. Assertion Generation and Forwarding

Assertion: Token, PKtemp, ID

POST Challenge-Response (with Assertion)

Verify the signature and validity of the token
Update the challenge status to "valid"

Next Steps

- Split pk-01 into a separate draft, recently updated to **version-05**

New additions:

- Introduced four Web-oriented challenge variants: pk-dns-01, pk-http-01, pk-tls-alpn-01, and pk-email-01
 - Added the pk_binding to unify binding mechanisms across both Web/non-Web PKI scenarios in the newOrder request
 - Introduced an optional csr_less flag to indicate whether CSR can be omitted during finalization
 - Generalized the definition of IdP to include entities such as DNS and HTTP servers
 - Refactored the original pk-01 into two non-Web variants: pk-csr-01 and pk-cert-01
- After the document is updated, we will issue a Call for Adoption (CfA).

- Prepare a separate draft regarding the integration of the ACME and OPAQUE protocol
- Prepare a draft specifying how to use an existing certificate from a different PKI