ACME Extension for Public Key Challenges

draft-geng-acme-public-key-02

Feng Geng, Panyu Wu, Liang Xia
Huawei

IETF 123

Update

Present ACME pk-01 challenge

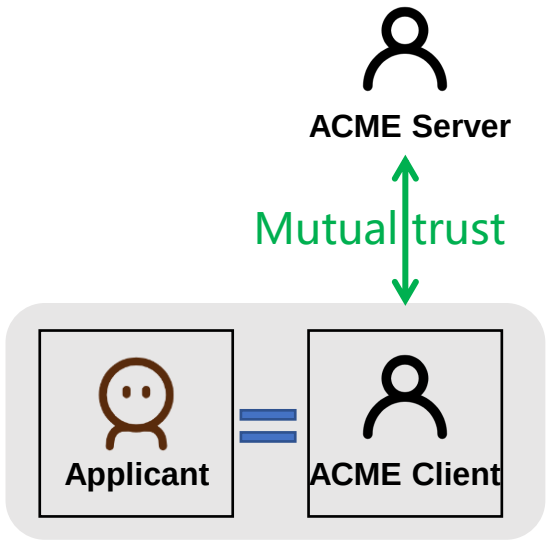
Added relevant background and security model.

- ACME server can use the public key authentication protocol to **verify that the real certificate applicant** behind the ACME client has control of the identity.

- **Defending against Public Key replacement attacks** (Replace the public key in the CSR);

Backgrounds – Two categories
Question： Can we only trust the ACME client?

resource category: YES

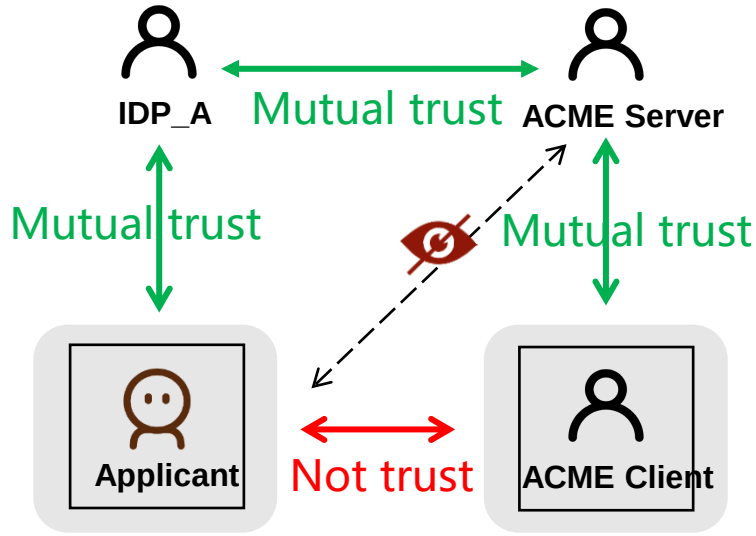


Deployed within a server, the applicant **grants all privileges to the ACME client**.

we can only trust the ACME client because it **possesses all the necessary information**, such as the client credentials, domain name, and the corresponding public key. If it were to act maliciously, there would be no way to prevent it.

Our work mainly

user/device category: NO



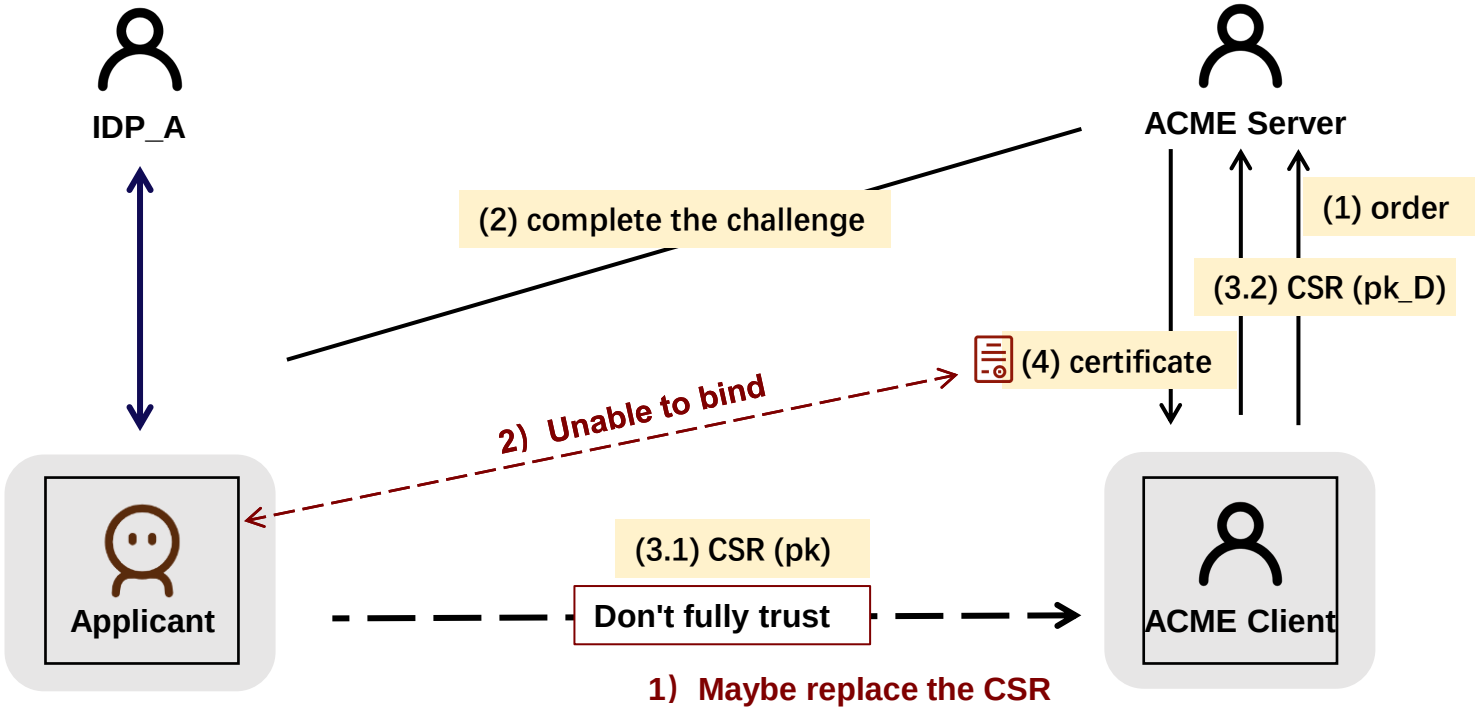
The applicant has registered the identity public key under IDP_A within the company and **does not fully trust the ACME client**.

we don’ t necessarily trust the ACME client because it **does not possesses the applicant private key**, by which we can rely on the applicant itself and the introduced public key authentication protocol to verify whether the certificate public key corresponds to the applicant's private key.

Security Model

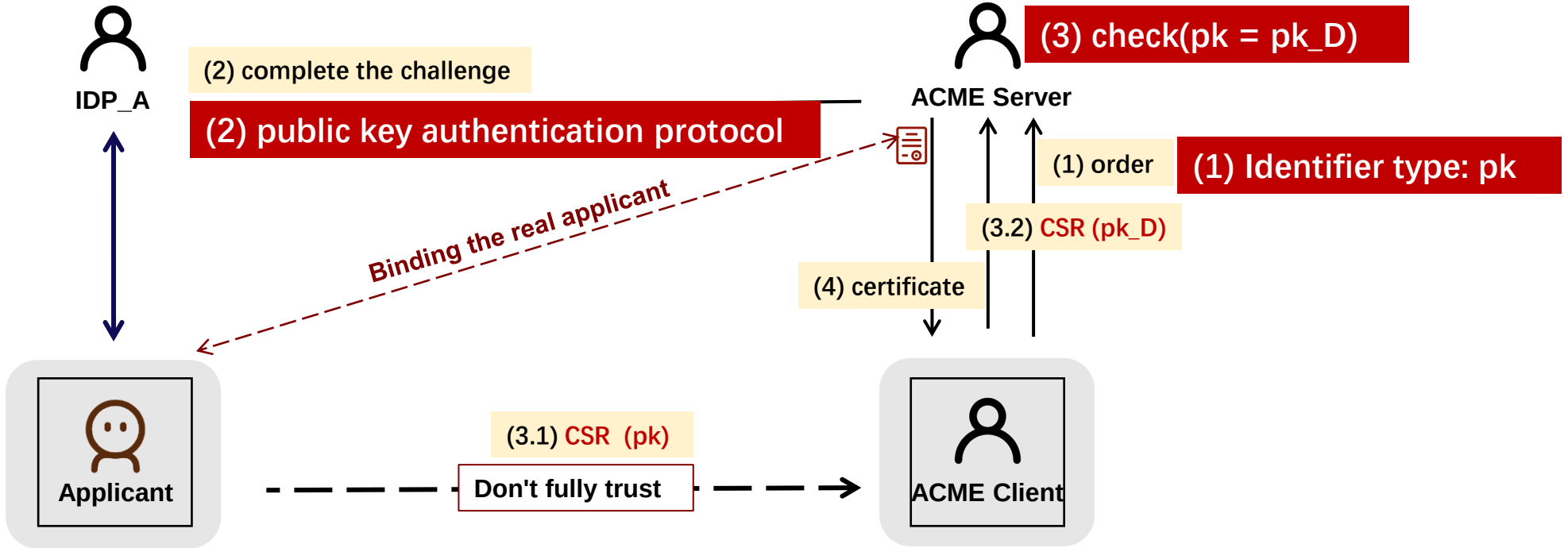
For the real applicants: Unable to confirm that the challenges they complete are only for their own certificate.

For the ACME server: Cannot confirm whether the real applicant behind the ACME client itself owns the private key corresponding to the certificate;



pk-01 – solution concept and process

- **For the real applicants**: Unable to confirm that the challenges they complete are only for their own certificate. —— **By adding pk identifiers to the order, the pk in the challenge phase and in the final certificate issuance phase are consistent.**
- **For the ACME server:** Cannot confirm whether the real applicant behind the ACME client itself owns the private key corresponding to the certificate. —— **The ACME server verifies that the applicant behind the ACME client has control over the identity via a public key authentication protocol.**



Solution – new ACME Extension for PK Challenges : ACME pk Identifier Type

```
"identifier": { "type": "pk", "value":"MIGfMA0GC***GbQIDAQAB"}
"identifier": { "type": "selfsign-cert", "value":"MIIHSDCC***AU1GH3xQ="}
"identifier": { "type": "csr", "value":"MIICljCCA***RL64+taHbP"}
```

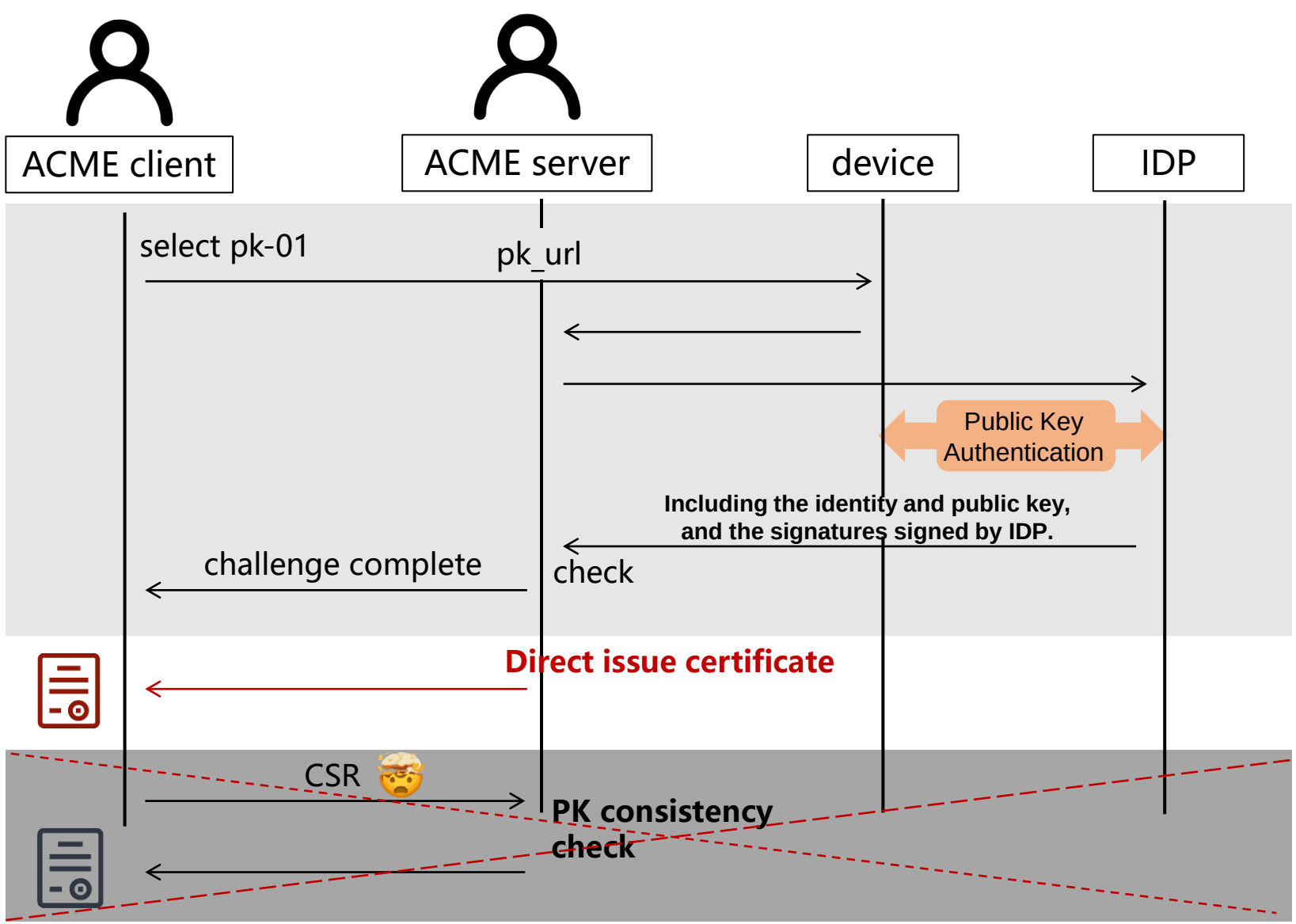
“pk” :

Used to request a certificate for a specific public key.
Example: requesting a certificate for a **device** that is tied to a user's identity.

“csr” / “selfsign-cert” :

Used to request certificates for applicants who need to be identified.
I.e., it requires **binding of specific identity information**.

Optional Solution – remove the final CSR process



Thanks