ACME Extension for Public Key Challenges

draft-geng-acme-public-key-00

Feng Geng, Panyu Wu, Liang Xia Huawei

IETF 121
Dublin, Ireland

Backgrounds

ACME (RFC 8555)

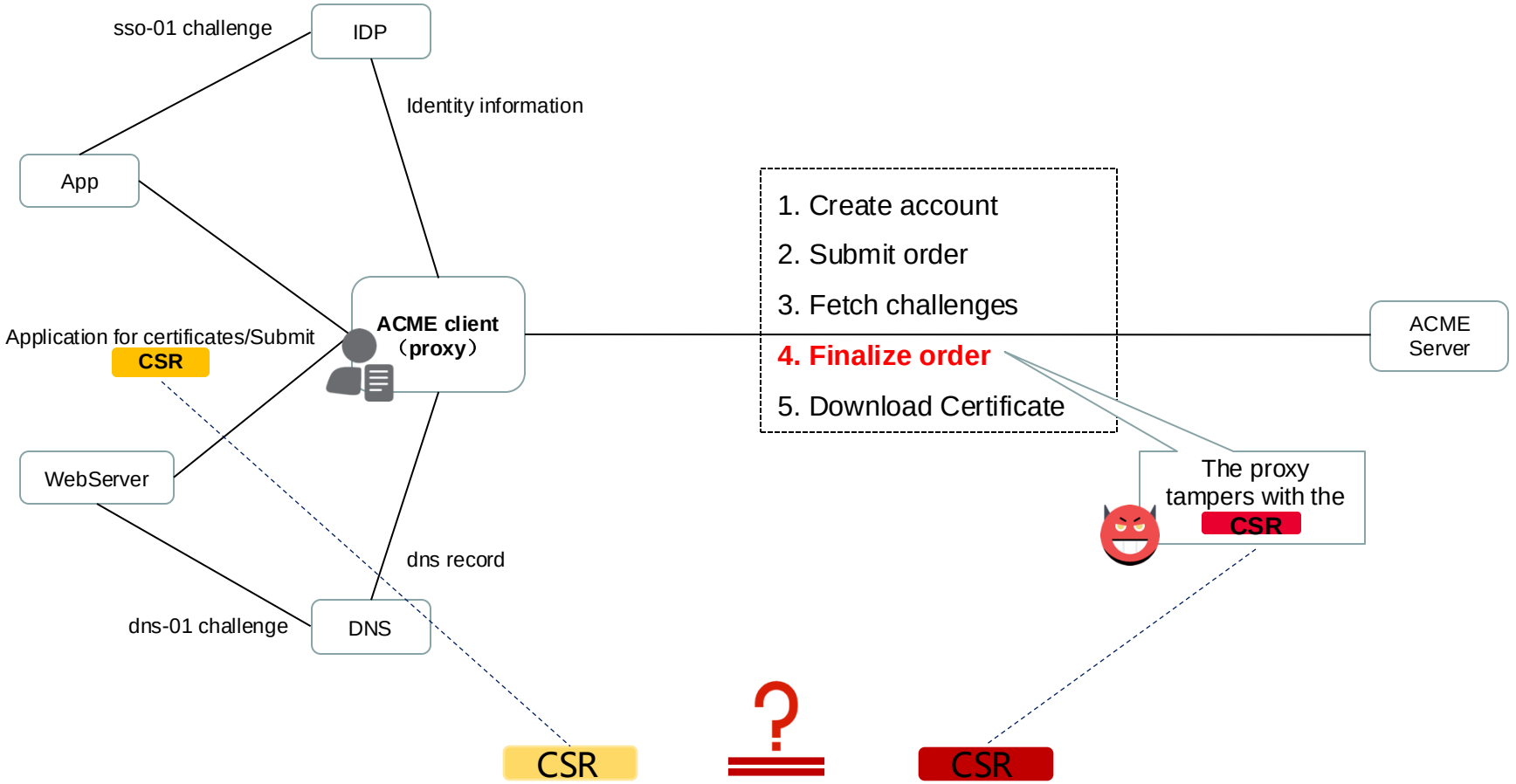
- Account Management
- Identifier Validation
- Certificate Issuance
- Certificate revocation and renewal

Related standards

challenges	identifiers	rfcs/drafts	status	goals
dns-01	dns	rfc8555	standard	Issuance of Web PKI certificates proving control of server-side resources（provision a DNS TXT record for your domain）
http-01	dns/ip	rfc8555/8737/8738	standard	Issuance of Web PKI certificates proving control of server-side resources（a file on your web server）
email-reply-00	email	rfc8823	standard	Issuance of certificates for e-mail（with S/MIME）
tls-alpn-01	dns/ip	rfc8555/8737/8738	standard	Issuance of Web PKI certificates proving control of server-side resources（provisioning virtual host at your domain’ s IP address）
dns-account-01	dns	draft-ietf-acme-scoped-dns-challenges-00	draft active	Multiple accounts can operate a domain at the same time without conflict
onion-csr-01	dns	draft-misell-acme-onion-03	draft active	Issuing certificates for onion domains, onion domains can't use the normal http-01/dns-01 challenge
tkauth-01	TNAuthList	rfc9447/9448	standard	Issuance of STI (Secure Telephone Identity) certificates
sso-01	email	draft-biggs-acme-sso-01	draft expired	Issuance of end-user client certificates, required in the standard to support only email type identifiers. Cisco webex support.
device-attest-01	permanent-identifier	draft-acme-device-attest-03	draft active	Issuing end-user client certificates, reusing WebAuthn attestation to achieve challenge authentication for devices. Apple MDM support.
otp-01	Not yet clear	draft-ietf-acme-client-07	draft expired	Support for end-user client, device client and code signing certificates (based on one-time passwords)
cert-01	Not yet clear	draft-ietf-acme-client-07	draft expired	Support for end-user client, device client and code signing certificates (based on pre-authorized certificates)
ppkp-01	Not yet clear	draft-ietf-acme-client-07	draft expired	Support for end-user client, device client and code signing certificates (based on WebAuthn)

Only check the control over the requested identity!

Problems in the automatic issuance of certificates



Public Key Consistency Not Check

PK replacement attack: the public key in the final CSR has been replaced to apply for the mismatched certificate.

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 not 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.

ACME pk-01 Challenge：Protocol Process

Step 1: A certificate request order **whose identifier uses pk, csr, or selfsign-cert** and whose value contains **the public key**.

Step 2: The server creates a response challenge based on the order's identifier type: **pk-01: {type: "pk-01", pk_url:"", pk_provider.""}**

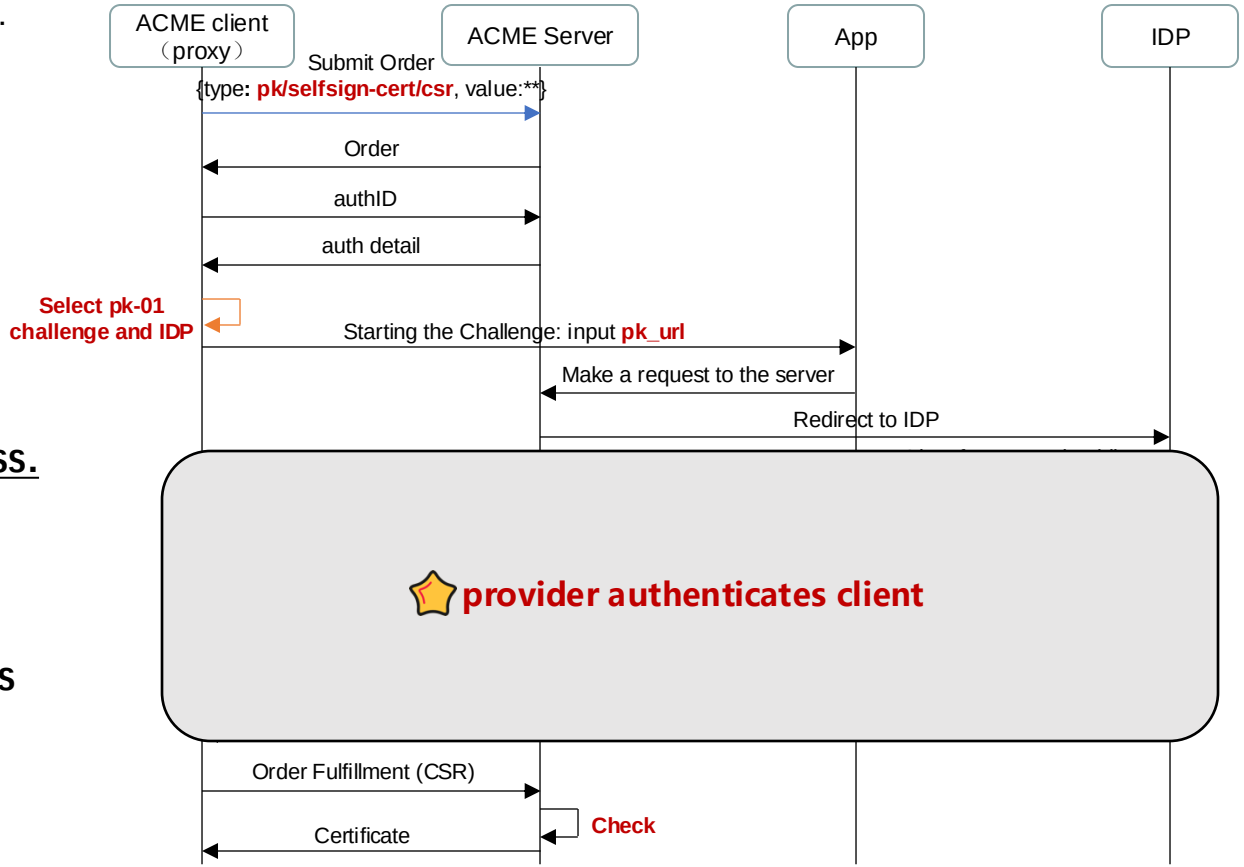
Step 3: Client gets pk-01 type challenge and selects trusted IDP server.

Step 4: The client starts the challenge authentication process.

Step 5: Client completes the order and submits the certificate request CSR.

Step 6: ACME server checks whether the pk in the CSR file is consistent with the pk in the order.

Step 7: Client completes downloading of new certificate.



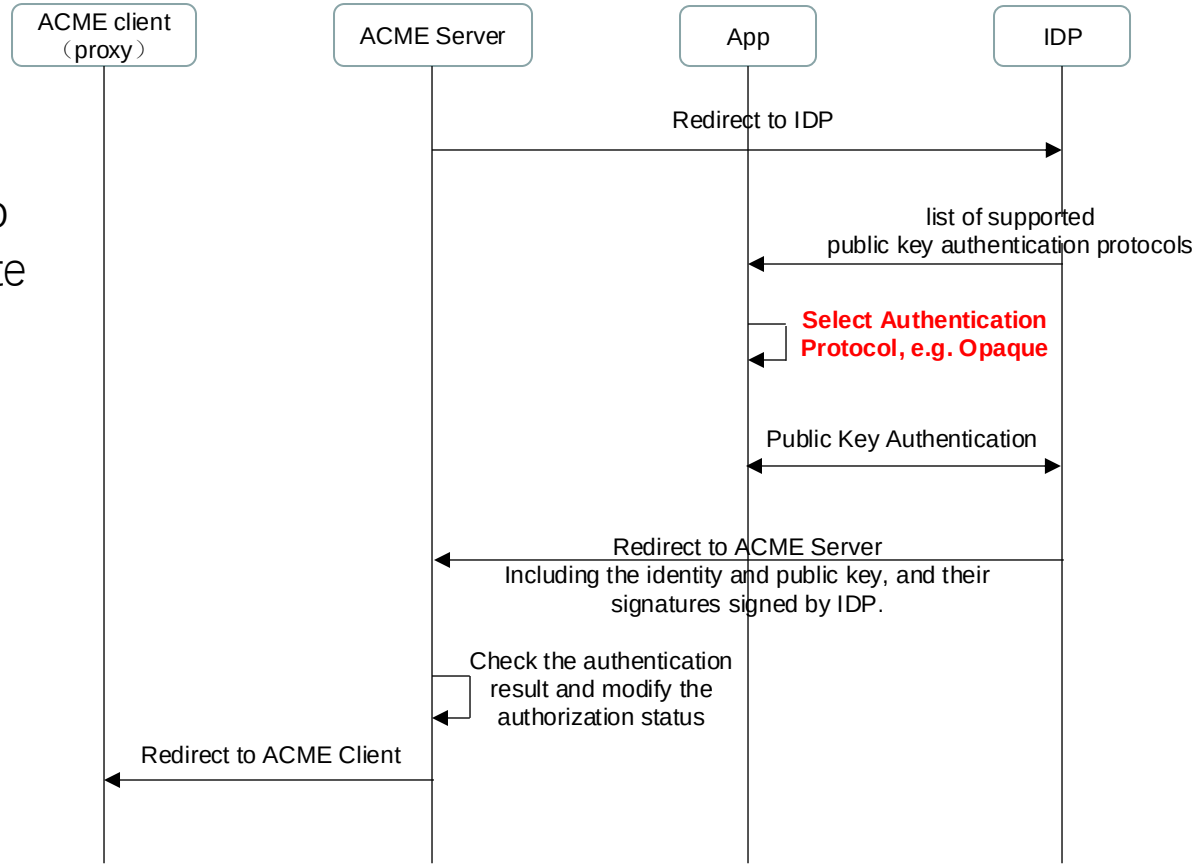
Public Key Authentication & Order Fulfillment

Step 1: The ACME server receives the request and redirects it to the IDP server.

Step 2: The IDP server requires the requesting party to perform authentication to verify that it holds the private key corresponding to the public key.

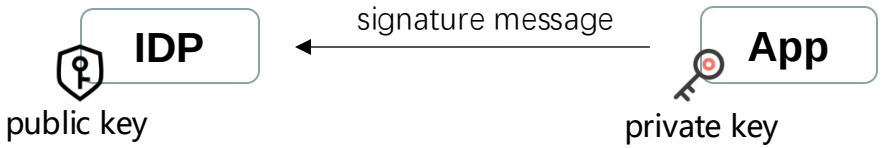
Step 3: After successfully authenticating the identity, the IDP returns the user's information and the logged-in device public key information to the ACME server.

ACME server checks whether the device public key is consistent with the public key in the order. For identifiers of type csr and selfsign-cert, identity consistency checks are also required.

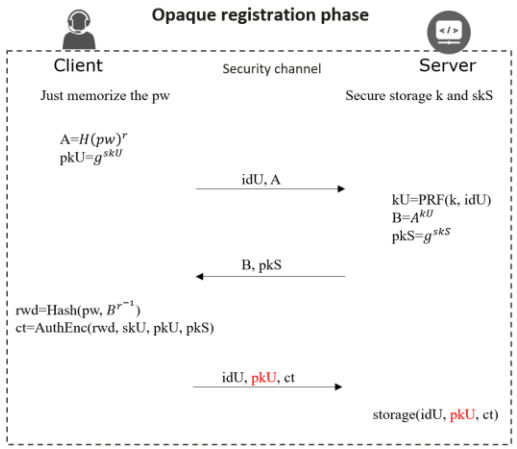


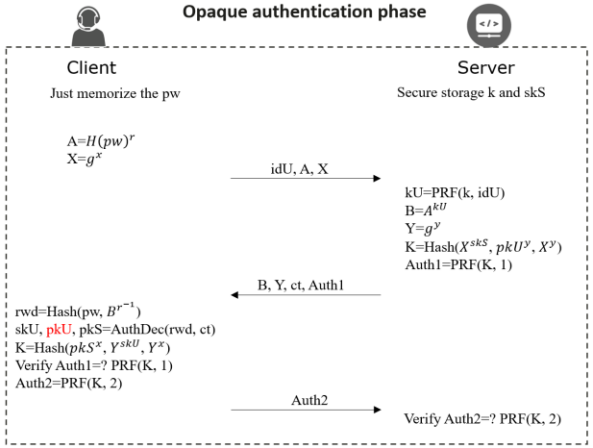
Existing Public Key Verification Protocols

- challenge public key signature and verify signature (for example, **WebAuthn**)



- **Opaque/AKE** (draft-irtf-cfrg-opaque-17)



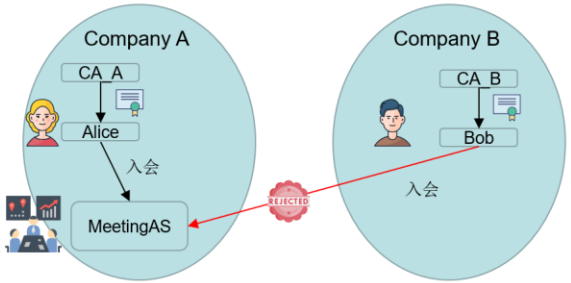


- **non-interactive zero-knowledge (NIZK) discrete logarithm equality (DLEQ) proof**

……

Usecase1 : ACME + aPAKE/Opaque

Shared public equipment participants



Identity credentials are tied to a person's identity, and identity credentials representing a person's identity need to be persistently stored on a trusted device.

However, on **semi-trusted devices, it is not possible to persistently save the user's personal credentials in order to avoid causing personal identity leakage.**

Authentication in cross-domain scenarios.

Someone from Company B needs access to an internal meeting at Company A.

- Certificate Public Key Encryption (one time pw)
- Opaque register one time pw
- ACME interim certificate of one classification at a time

Next Step

- Continue refinement and improvement
- Welcome comments and collaboration