22 July 2025

IETF 123 ACME

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note Really Well

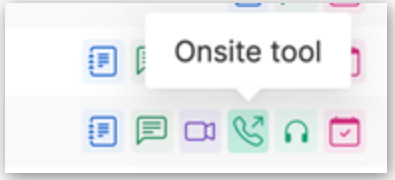
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 123 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.

Resources for IETF 123 Madrid

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

- Administrivia – Note Well, scribes, agenda bashing
- Document status – chairs

- Device attestation – Weeks
- ACME Client – Kathleen

- ACME auto-discovery - Mike
- ACME public key – Xialing Frank
- ACME RATS – Peter Liu
- Authority Token – Chris Wendt
- ACME Profiles – Aaron
- DNS Persist – Henry Birge-Lee
- ACME OpenID Federation – Leif Johansson

IETF

Document Status (1/2)

- We broke our dry spell! (since September-2023)
- ACME Renewal Information – Published as **RFC 9773**
- ACME extensions for .onion – Published as **RFC 9799**

- DTN NodeID – Went through another LC and ballot – now in the RFC Editor's queue.
- ACME Integrations – Still in RFC Editor's queue. Waiting on missref since July-2023.
  - draft-ietf-anima-brski-cloud is still not published.
- ACME Client – 4 new revision in May and June.
  - Have a presentation

Document Status (2/2)

- ACME Device Attestation – new revisions (-04) in May
  - Got a presentation
- ACME DNS Labeled with ACME Account ID Challenge
  - New revisions in May (-01)
  - New author – Antonios Chariton
  - No presentation today.

Presentations

ACME Client Challenge Types

(was: ACME End User Client and Code Signing Certificates)

Kathleen Moriarty

Draft adds 3 challenge types

Purpose: enable use of additional challenge types, considered strong authentication for use by ACME clients. Challenge types would fit into processes defined by CAs who would determine aspects such as the need for identity proofing to obtain credential.

- OTP
- PKI
- WebAuthn

Draft also clarifies that the CSR is independent of the challenge type in ACME and provides examples that include the OID for digital signatures for code signing and document signing.

Draft Status

Is the working group interested to see additional challenge types added for aligned use cases (e.g. workload identity, code signing, document signing)?

Once current reviews (and agreed additions) are made, is the WG okay to progress the draft to WGLC?

Thank you!

ACME Auto-Discovery

draft-vanbrouwershaven-acme-auto-discovery
draft-vanbrouwershaven-acme-client-discovery

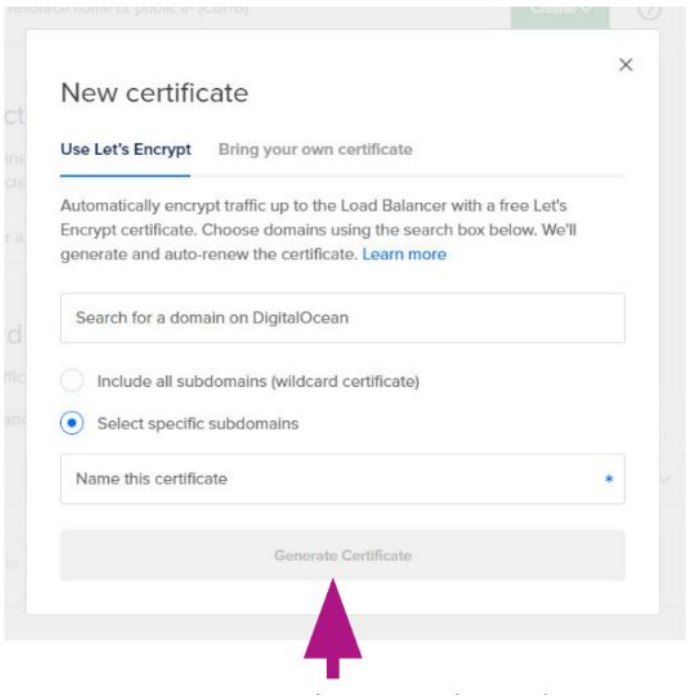
Mike Ounsworth
ACME 123

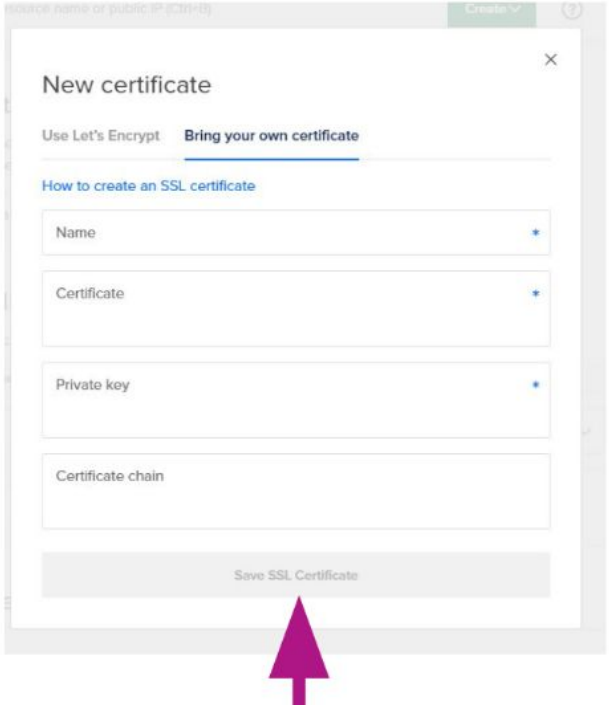
The Problem

With most Cloud Service Providers (CSPs), you can either:

1) use their choice of ACME prodiver (almost always Let's Encrypt), or

2) you can bring your own PEM file.





(1) leads to lack of issuer diversity.
(2) is completely un-tenable with a move to 45-day certs.

Refresher

draft-acme-autodiscovery

- Problem to be solved: As the owner of a website hosted in a Cloud Service Provider, I would like the CSP to use *my choice* of CA, not *their choice* of CA.
  Equivalently stated: As an ACME Bot, knowing only the DNS name that I'm requesting a cert for, discover which ACME server to reach out to.

- Core mechanism: an ACME discovery extension to the domain's DNS CAA record pointing to the authoritative ACME server(s) for that domain.
  - Side benefit: this mechanism provides a way to specify redundancy and fallback CAs for each domain.

Refresher

draft-acme-client-autodiscovery

- Problem to be solved: As a domain owner, I would like to tell my CA the set of ACME account keys belonging to the ACME bots for my CSP; this needs an abstraction layer so that CSPs are free to add new keys / rotate keys dynamically.

- Core mechanism:
  - As a CSP, I host a https://cspcorp.com/.well-known/acme-keys – a JWK bundle.
  - As a domain owner, I tell my CA that I authorize any ACME client with a key in https://cspcorp.com/.well-known/acme-keys to request certs for my domain.

Drafts looking for a new owner

- Drafts were initially driven by Entrust, who is no longer pursuing it.
  - I can stay as co-author for continuity, but I can't lead.
- I have had a few people reach out to me since 122, however:
- Draft needs at least one each from the community of implementers:
  - ACME Bot maintainer
  - Cloud Service Provider
- The drafts are fairly mature, with some minor quibbling to do about whether the CSP or the domain owner is the "subscriber", and who agrees to the TermsOfService.
  - Also need running code.

- If we don't get sufficient support to take over this pair of drafts, then I think they die.

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

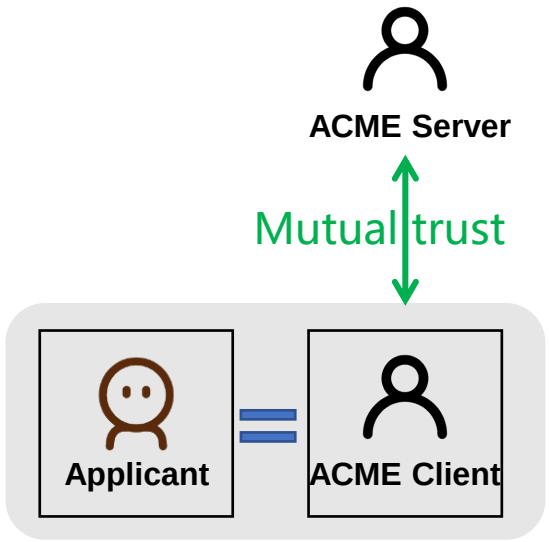
Added relevant background and security model.

- 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

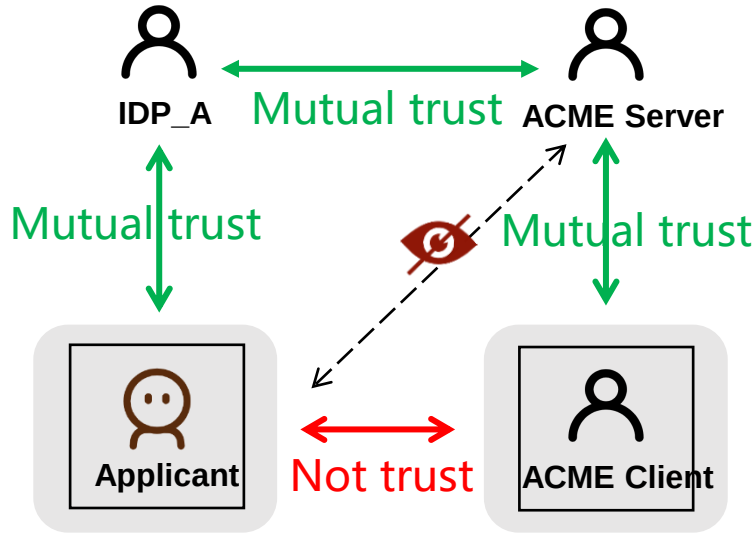


Deployed within a server, the applicant **grants all privileges to the ACME client**.

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



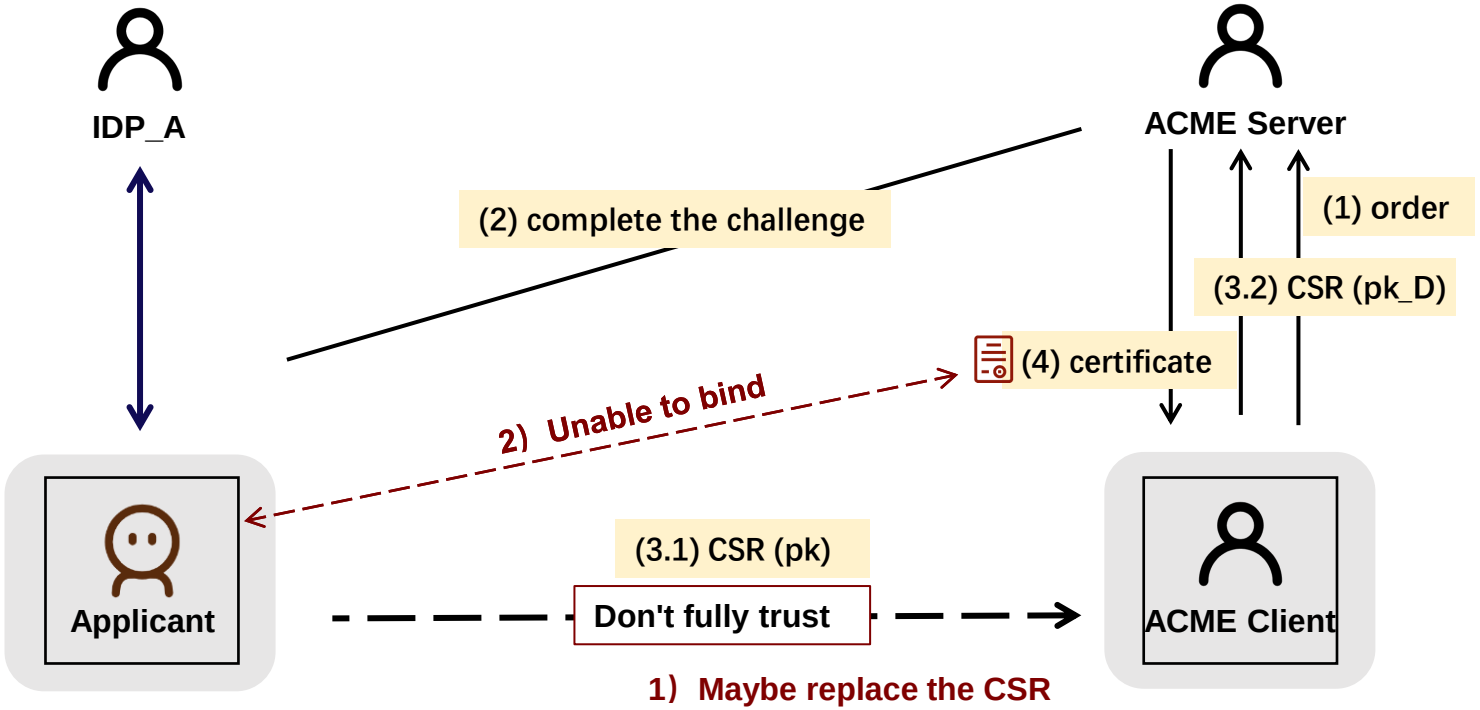
The applicant has registered the identity public key under IDP_A within the company and **does not fully trust the ACME client**.

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

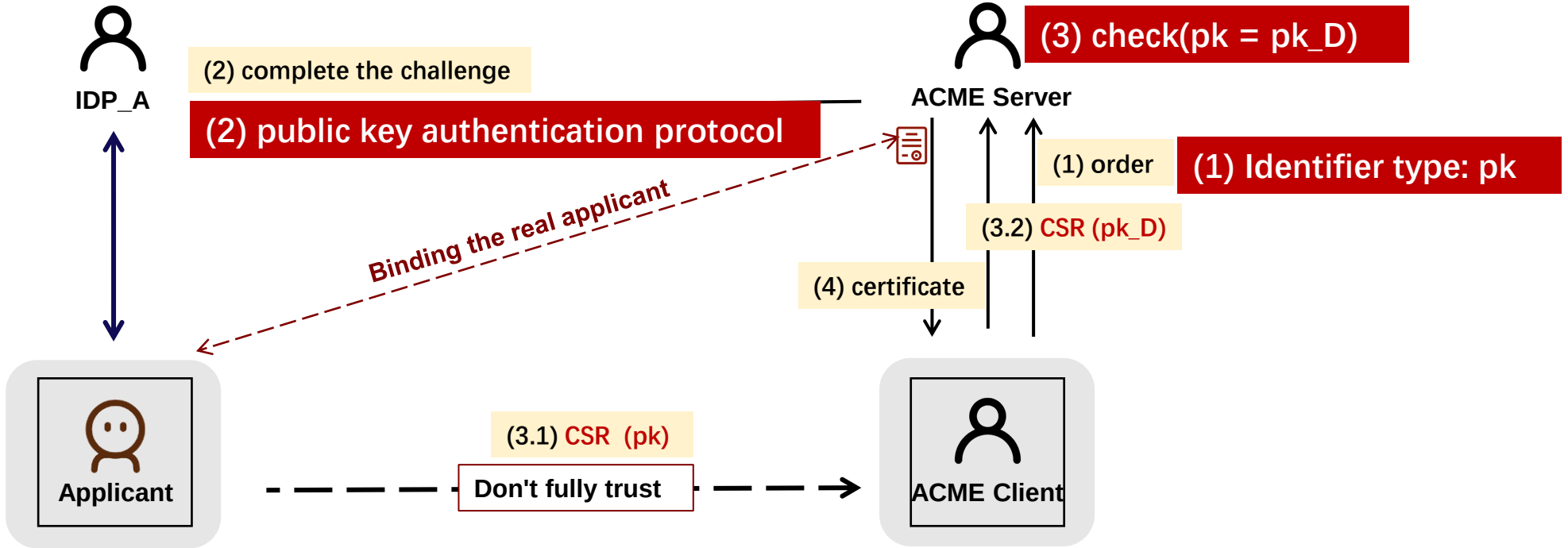
For the real applicants: Unable to confirm that the challenges they complete are only for their own certificate.

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"}
```

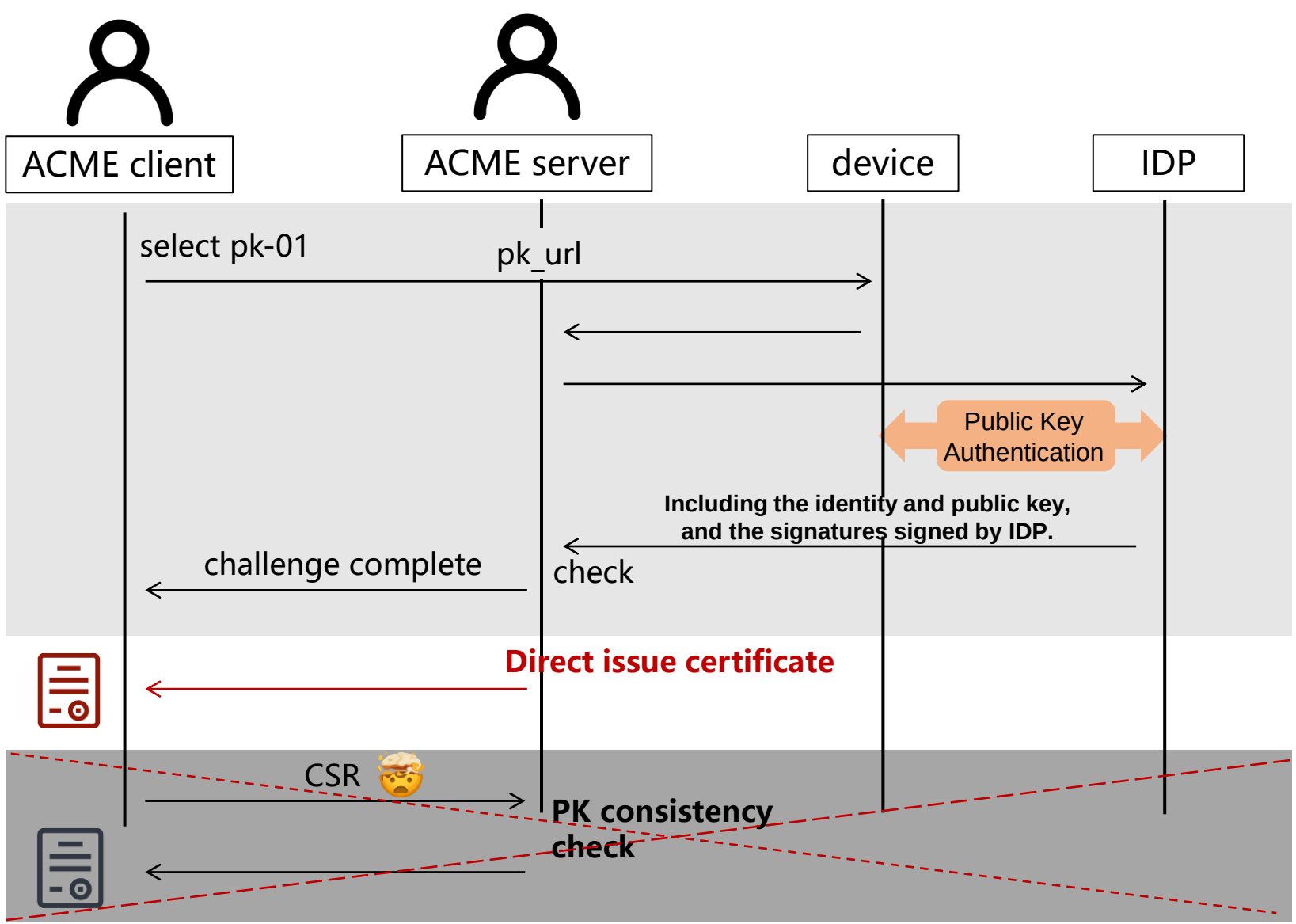
“pk” :

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



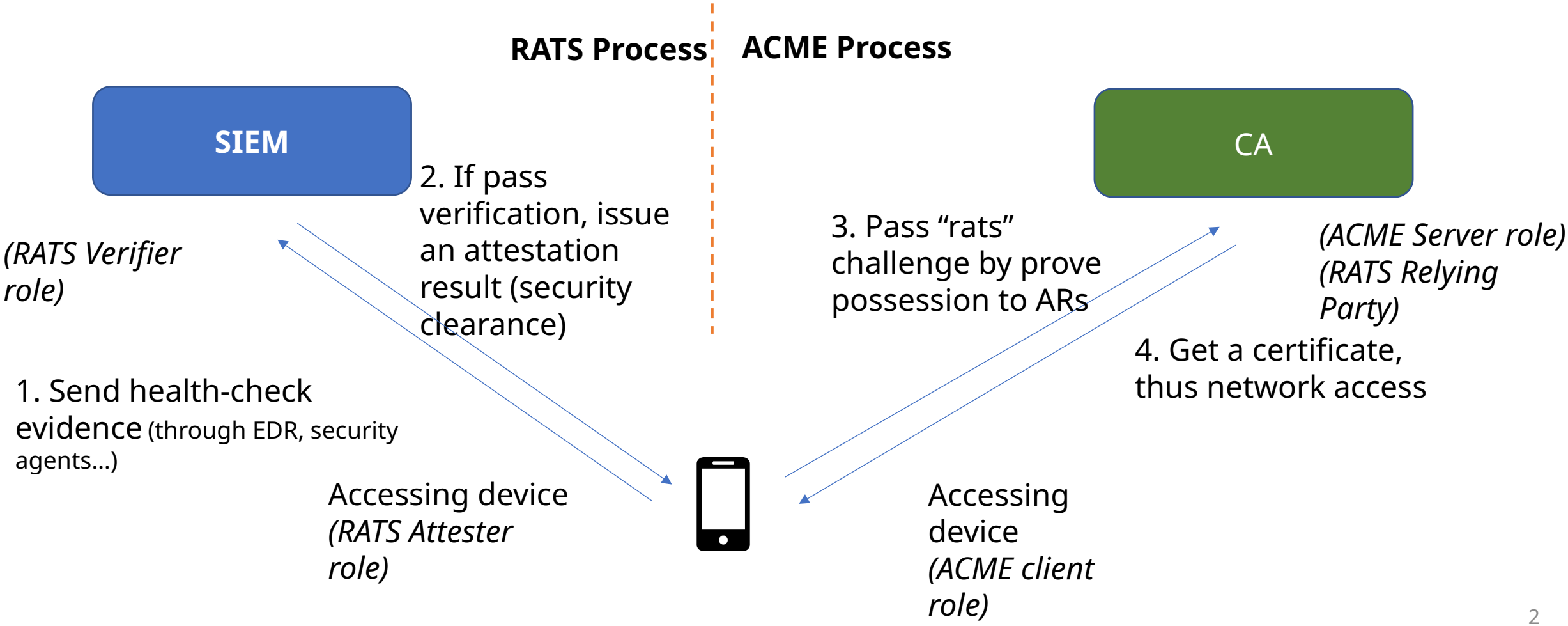
Thanks

draft-liu-acme-rats

Chunchi Peter Liu, Mike Ounsworth, Michael Richardson

IETF 123 Madrid

What: Grant certificates to devices that pass security checks



Why: Use Cases

1. **Grant internal network access to enterprise employees, through a MDM software**
    1. Continuous evaluation of endpoint security posture, plus
    2. Short-term certificates to ensure continuous evaluation

2. **An ACME server (cloud domain host service provider) might put a security policy on their ACME client (domain owner tenant). The ACME server may want to know certain security attributes of the private key or the platform.**
    - Private key resides in FIPS level 3 hardware and has `non-exportable=true`.
    - The policies that apply to certain (cloud) Key Management Service (KMS) instances.
    - TLS / OS / Docker stacks have been recently patched (ie <= 3 months old).

Changes from last IETF

Had 2 design meetings

1. Provided a real use case, current practices, and analyses
2. Narrowed down design choices

A real use case

- **An power company inspector visits many (100) power substations, connect to its small wifi, download data, do inspection, and go to next.**

1. **(at HQ) Inspect the device is trustworthy: ACME-RATS** or TEAP-RATS
   - Do only once, get a cert, which works everywhere
2. **(at substation) Authenticate to the wifi using EAP: EAP-TLS or Tunneled EAP (wifi: WPA-enterprise)**

- **Choices:**
  - ❑ **Use EAP-TLS:** show up with a certificate, where inspector company root CA installed at every substation.
  - ❑ **Use Tunneled EAP**: Eduroam model. Authenticate not at the spot, but call home. Better scales or control lifecycle. Overdone? (put as an option)
    - TEAP solution might not be deployable: Phone maker need to implement TEAP (no control over). Apple said not doing TEAP, only EAP-TLS

Current practices and why they are not good enough

1. As an inspector, **you *can* type EAP-password** for wifi
   - × Different campus, different WiFis, different passwords. Remember all?
   - × Good password management needs rotation. That makes you re-type every two weeks.
   - × Revocation/rotation requires IAM message RADIUS server.

2. As an inspector, your MDM can **receive passwords and usernames** over **application layer connection** from the MDM server. Then, your MDM do the **“radius-password”** (EAP-MSCHAPv2 RADIUS+802.1X) for you.
   - × Passwords can be **phished**(user side)/**leaked**(during transmission)/**stolen**(device side)
   - × No MFA. No binding of trusted/usual devices.
   - × Certificates include accessing device identities while knowledge of password do not.
   - × Device identity visibility at RADIUS client/AP/switch– allowing more flexible network access policy.

Design decisions

- **Use ACME-RATS to get certificates is a good idea**
- **Use EAP-TLS to authenticate the certificate and access**
- **Put attestation result in the /newOrder payload**
  - Challenge is NOT the right place to carry remote attestation results
    - **Because**: Challenges are for proving ownership of identifiers, not system attributes.
    - Technical problem: The client is only required to respond to ONE challenge.
    - A separate system-level remote attestation could complement the identity challenge.

Remaining problems

Trust assumptions:

- How does (potentially external) ACME Server trust the AR generated by the (potentially internal) Verifier? Assume ACME Server trust Verifier?
  - may work inside of a multinational company, or in a consortium-ish relationship

Next steps

- ACME-RATS design team meeting continue
- ACME-RATS side meeting in Tuesday 7-9 PM
- If you want in, email:
  - Liuchunchi(Peter) liuchunchi@huawei.com
  - Mike Ounsworth mike.ounsworth@entrust.com
  - Michael Richardson mcr+ietf@sandelman.ca
- Hope to call for adoption at Montreal.

IETF123 – Madrid
ACME

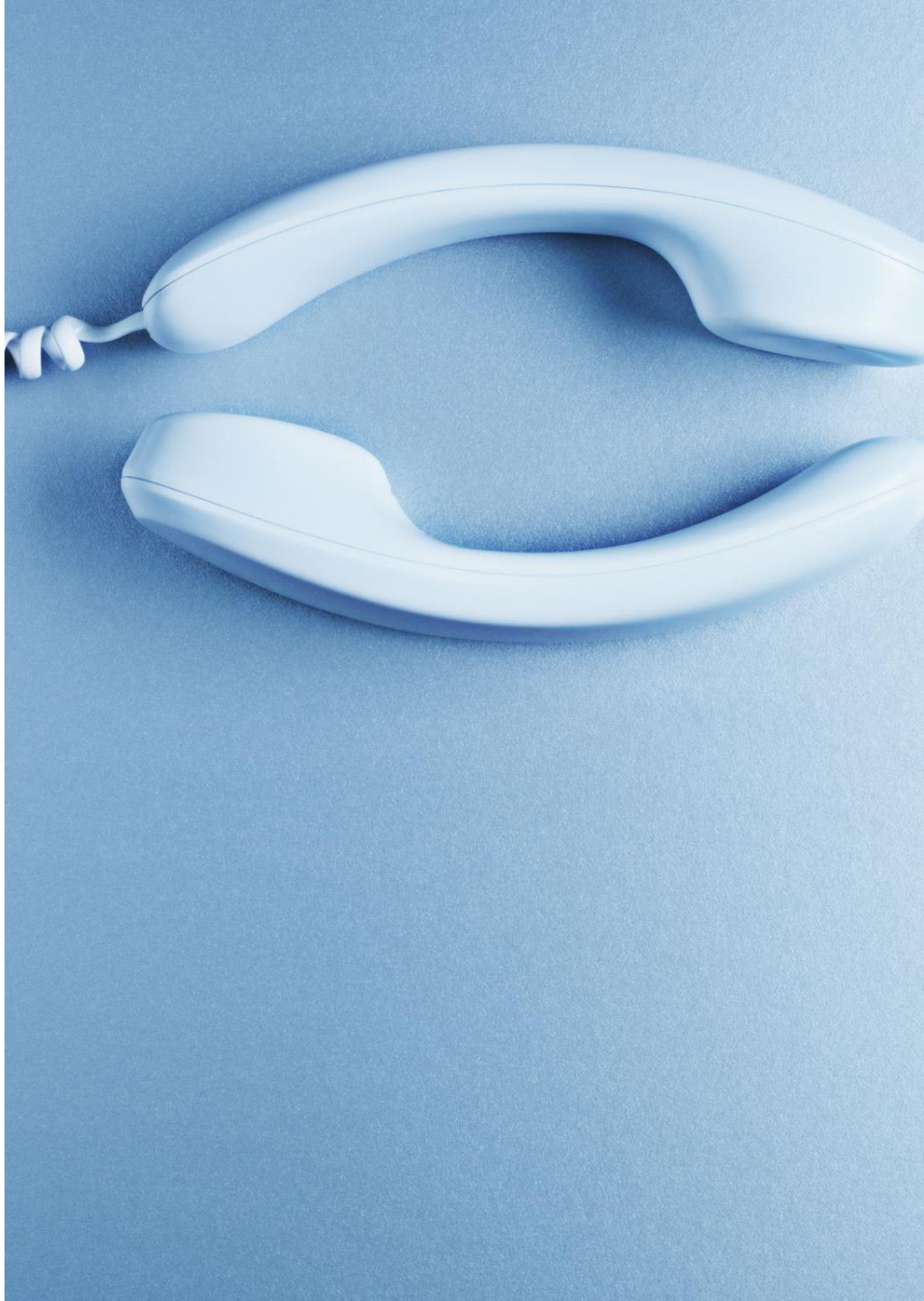
JWTClaimConstraints Authority Token Profile

draft-wendt-acme-authority-token-jwtclaimcon-03

Chris Wendt, David Hancock

Introduction to JWTClaimConstraints Authority Token Draft

- Defines an **Authority Token Profile** for ACME challenge validation specific to JWTClaimConstraints defined in STIR WG.
- Extends the existing Authority Token validation model [RFC9447] to include **JWTClaimConstraints** extension [RFC8226] and extended by **EnhancedJWTClaimConstraints** [RFC9118].



New ACME Challenge

- Defines new ACME Challenge Identifier Type: **JWTClaimConstraints**
- We have existing **TNAuthList Authority Token**
- Want to validate likely STIR cases where both **TNAuthList** and **JWTClaimConstraints** extensions are requested to be added to a certificate and the challenges are validated separately.
- New draft provides examples, want to validate our interpretation of the use of **multiple challenges** is correct

Examples – Authority Token

JWTClaimConstraints Authority Token

```
{
    "protected": base64url({
      "typ":"JWT",
      "alg":"ES256",
      "x5u":"https://authority.example.org/cert"
    }),
    "payload": base64url({
      "iss":"https://authority.example.org",
      "exp":1640995200,
      "jti":"id6098364921",
      "atc":{"tktype":"JWTClaimConstraints",
        "tkvalue":"F83n2a...avn27DN3",
        "ca":false,
        "fingerprint":"SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:
         D3:BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"}
    }),
    "signature": "9cbg5JO1Gf5YLjjz...SpkUfcdPai9uVYYQ"
  }
```

Examples – Authority Token Request

Body of the POST to the ”Authority” validating allowed JWTClaimConstraints extension

```
{
      "atc": {
        "tktype":"JWTClaimConstraints",
        "tkvalue":"F83n2a...avn27DN3",
        "ca":false,
        "fingerprint":"SHA256 56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3
          :BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9:38:E3"
      }
    }
```

And Response:

```
HTTP/1.1 200 OK
  Content-Type: application/json

  {"token": "DGyRejmCefe7v4N...vb29HhjjLPSggwiE"}
```

Examples – Basic Claim restrictions

```
SEQUENCE {
    mustExclude [2] {
      SEQUENCE {
        IA5String 'attest'
        IA5String 'origid'
        IA5String 'div'
        IA5String 'rph'
        IA5String 'sph'
        IA5String 'rcd'
        IA5String 'rcdi'
        IA5String 'crn'
        }
      }
    }
```

Examples – RCD Claim restrictions

```
SEQUENCE {
    permittedValues [1] {
      SEQUENCE {
        SEQUENCE {
          IA5String 'rcd'
          SEQUENCE {
            UTF8String '"nam": "James Bond"'
            }
          IA5String 'crn'
          SEQUENCE {
            UTF8String '"For your ears only"'
            }
          }
        }
      }
    mustExclude [2] {
      SEQUENCE {
        IA5String 'attest'
        IA5String 'origid'
        IA5String 'div'
        IA5String 'rph'
        IA5String 'sph'
        IA5String 'rcdi'
        }
      }
    }
```

Next Steps

- Seeking WG review and adoption as a working item.
- Will also keep STIR working group in loop for SME input into STIR related details.

Persistent DNS Validation in the ACME protocol

IETF 123 Madrid

Henry Birge-Lee
Princeton University

Motivation for persistent validation

- Traditionally, ACME dns-01 requires the client to perform a DNS record “change” by uploading a random token to “_acme-challenge”
- Increasingly, cloud providers are offering an issuance delegation service where “_acme-challenge” is CNAMEd to a cloud-provider controlled zone
- When a CNAME is used at “_acme-challenge” the DNS change in question is not occurring in the actual zone of the domain being validated but instead in the zone pointed to by the “_acme-challenge” CNAME
- When dns-01 validation follows a CNAME, it is no longer enforcing a true DNS record change but instead confirming that a particular static value is in place in the zone in question which indicates the domains desire to complete DCV

Activity at CA/Browser Forum

- The widespread prevalence of CNAME DNS challenge completion led to a discussion at the CA/Browser Forum about whether a CA could run such a service on behalf of its subscribers
- This resulted in the failed ballot SC-082 which would have explicitly permitted CAs to instruct subscribers to install CNAMEs instead of actual challenge verification TXT records
- Root programs didn’t like that the original intent of the method was to perform a DNS change but the CNAME technique is actually a static DNS value

Solution: permit validation using a “persistent” static value

- Defined in newly proposed ballot SC-088 https://github.com/slghtr-says/servercert/pull/3
- CAs and Root programs have spoken favorably for the new ballot which invents a new method for persistent DNS change
- This method is designed to strongly support automation
- Syntax and security controls are much better than the original CNAME method

Advantages over existing CNAME method

1. the infrastructure serving the zone used for ACME challenges could be compromised (potentially affecting many domains that all pointed to that same shared infrastructure)
2. CAs need to perform another potentially plaintext DNS lookup to complete the dns-01 challenge
3. only one CNAME record can exist at a label preventing this technique from delegating control to multiple cloud providers
4. availability issues with the ACME challenge zone could impact certificate availability
5. the ACME client needs an additional communication channel to communicate with the ACME challenge zone
6. a unique CNAME value must be provided to each of a cloud provider's customers otherwise this technique creates a major security breach between customers
7. a separate DNS zone and automated DNS infrastructure must be provisioned making this technique less practical for smaller operators.

Syntax of persistent validation in SC-088

- _validaton-persist.example.com IN TXT “authority.example; accounturi=https://authority.example/acct/123”
- authority.example: a valid CAA domain name for the CA signing the certificate
- accounturi: the ACME account that is allowed to request certs using this method

Proposed ACME dns-persist-01 method

- Uses the same syntax for checking records

- Method string name “dns-persist-01”
- Contains no token parameter (validation record can be fully derived by client before contacting ACME server)
- `GET /acme/authz/1234/1 HTTP/1.1 Host: example.com`
- `HTTP/1.1 200 OK { "type": "dns-persist-01", "url": "https://example.com/acme/authz/1234/1", "status": "pending" }`

Security considerations

- A stable persistent zone change has always been capable of satisfying the dns-01 challenge given that an adversary can upload a CNAME record that points to an adversary controlled zone
- If we assume the access level required to upload a CNAME record and a TXT record are similar, permitting validation using a stable TXT record provides comparable security to the existing dns-01 challenge
- This method does imply an ACME account compromise can easily lead to misisusance. However, ACME account compromises can already lead to misissuance due to validation reuse
- Eliminating the need for live DNS credentials on ACME clients or extra services that exist solely to serve ACME challenges overal improves security

Questions

Feel free to contact me at: birgelee@princeton.edu

Draft is at: https://birgelee.github.io/birgelee-acme-dns-persist-01/draft-birgelee-acme-dns-persist.html (updated intro and abstract since first send to list)

Additional security analysis: https://groups.google.com/a/groups.cabforum.org/g/servercert-wg/c/4tATbCpQRpM/m/8mH-SX87BAAJ

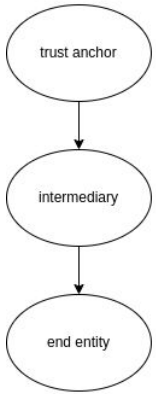
Will be on datatracker soon

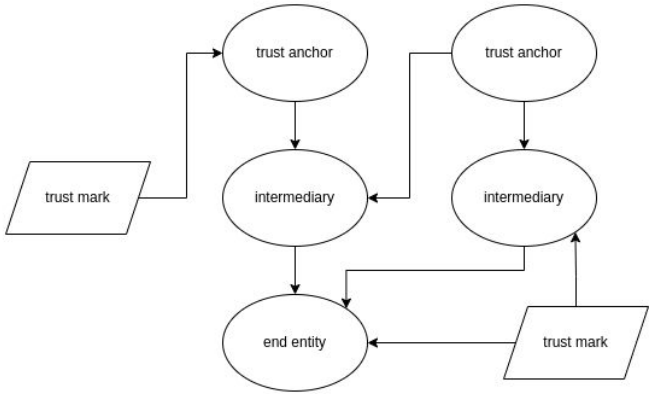
ACME OpenID Federation

Giuseppe deMarco by way of Leif Johansson

OpenID Federation

- OpenID Federation is a way to build identity federations at scale
- “A PKI with everything you need for multiple overlapping hierarchies turned on by default”





https://openid.net/specs/openid-federation-1_0.html
https://www.youtube.com/watch?v=XjZnDFsXGwE

draft-demarco-acme-openid-federation

- Issue an X.509 certificate based on proof-of-control of an OpenID fed entity
- A mechanism for bridging between OpenID Federation and “classical” PKI

Motivating examples

- EUID wallet client access certificates
- Object signing certificates “derived” from OpenID Federation

Implementation status

https://github.com/tgeoghegan/oidf-box built around Pebble and Lego, two well-known ACME implementations.

AOB