rats identifier and challenge type

IETF 121

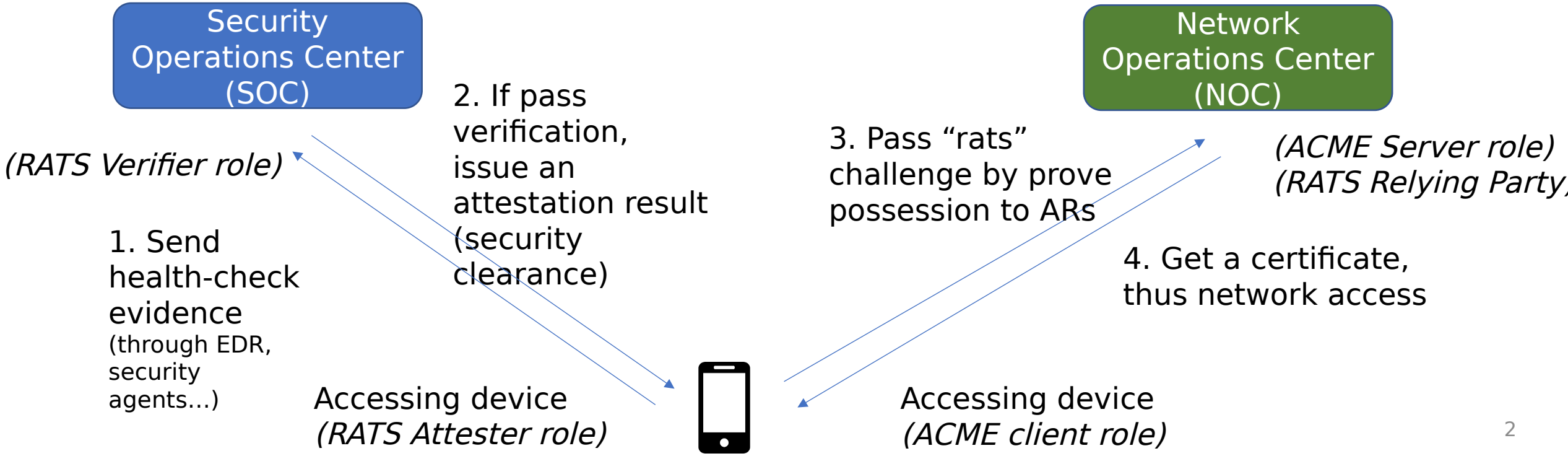
Dublin, Nov 6, 2024

Chunchi (Peter) Liu

liuchunchi@huawei.com

Why – client side certificates for mutual TLS
use case: Grant internal **enterprise network access** (certificates) to devices that pass security checks

- Enterprise usually have 2 teams: Security ops team and Network ops team, where to draw the line is always hard. This work helps them collaborate.



What it is –
issue certificate to devices that possess a valid attestation result

- Identifier: “rats”
  - Which uniquely identifies an attestation result
- “Challenge” type: “rats”
  - Verify attestation result validity using rats approaches (e.g. EAT jws signature)

How –
add identifier to…

- /newOrder Request Object
  - Payload identifier array

```
"identifiers": [
  { "type": "rats", "value": "0123456789abcdef" },
],
```

- Order Object of a client Account Object in Server

- Challenge Object in an Authorization

```
"challenges": [
  {
    "type": "rats",
    "url": "https://example.com/acme/chall/prV_B7yEyA4",
    "status": "pending",
    "token": "DGyRejmCefe7v4NfDGDKfA",
  },
```

The value of this identifier: hash of an AR

(uniquely identifies an AR)

How – reuse the keyAuthorization string
rats challenge type

- The ACME client send the keyAuthorization string to the challenge url
- The authorization string contains an base64url plain encoded AR
  - Replace thumbprint(accountKey) with attestationResult

keyAuthorization = token || '.' || base64url(attestationResult)

- The ACME Server takes out the attestationResult, verifies its validity as a Relying Party.

- If pass, change “status” from “pending” to “valid”. Otherwise “invalid”

Not certificate policies

- The ACME WG charter states: “The ACME working group is not reviewing or producing certificate policies or practices.”

- This work is NOT about certificate policies– the ACME server can decide what **claims/properties** in an AR to look for, on their own. This work is only about validating the attestation result as a new challenge type.

- This work also allows many customizations– period to refresh the certs… but not necessary to define in this document

Looking for feedbacks, collabs...

- draft-liu-acme-rats-00
- https://github.com/liuchunchi/draft-liu-acme-rats

Issues:

- Passport model vs Background check model, how to request specific claims to check
- CMWs instead of EATs?
- Where to encapsulate the attestation result
  - In a keyAuthorization String plaintext / in a Payload of a proper JWS object
- Value format of rats identifier
  - Hash of AR (of a credential) / identifier of an attester identity(perm-identifier) / others
- …

- liuchunchi@huawei.com


```
{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "SS2sSl1PtspvFZ08kNtzKd",
    "url": "https://example.com/acme/chall/Rg5dV14Gh1Q"
  }),
  "payload": base64url({
    "attObj": base64url(/* WebAuthn attestation object */),
  }),
  "signature": "Q1bURgJoEslbD1c5...3pYdSMLio57mQNN4"
}
```

Some discussions before this session w/ Mike and Thomas

device-attest-02 ACME challenge object example:

```
{
  "type": "device-attest-02",
  "url": "https://example.com/acme/chall/Rg5dV14Gh1Q",
  "status": "pending",
  "token": "evaGxfADs6pSRb2LAv9IZf17Dt3juxGJ-PCt92wr-oA" -- A background check evidence MUST include this in the evidence.
  "attestType": ["tcg-dice-manifest-evidence", "tcg-dice-UCCS-evidence] -- Value from the registry defined by https://datatracker.ietf.org/doc/html/draft-ietf-lamps-csr-attestation-14#name-initial-registry-contents
  "attestClaimsHint": ["OS patch level", "FIPSmode"] -- Needs a new IANA registry?
}
```

Challenge response from ACME client example

```
{
  "protected": base64url({
    "alg": "ES256",
    "kid": "https://example.com/acme/acct/evOfKhNU60wg",
    "nonce": "SS2sSl1PtspvFZ08kNtzKd",
    "url": "https://example.com/acme/chall/Rg5dV14Gh1Q"
}),
  "payload": Base64URL(<CMW>),
}),
  "signature": "Q1bURgJoEslbD1c5...3pYdSMLio57mQNN4"
}
```