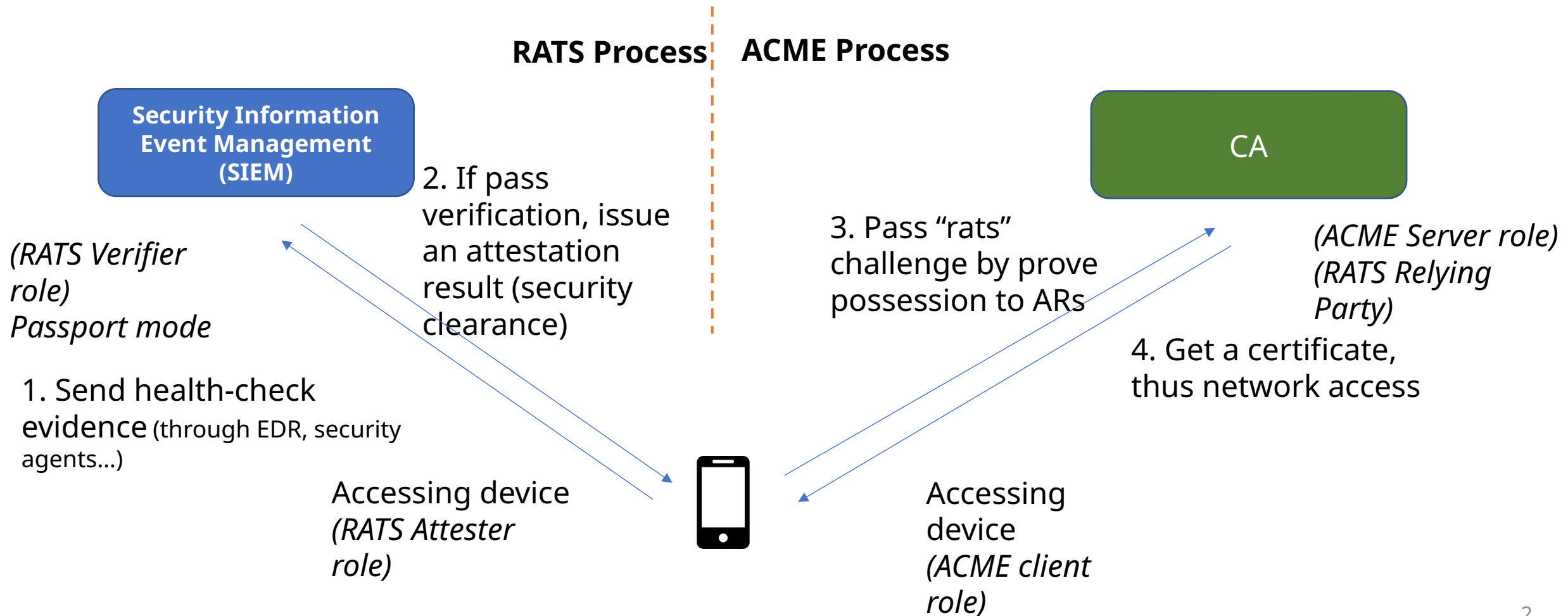


draft-ietf-acme-rats

Chunchi Peter Liu, Mike Ounsworth, Michael Richardson

IETF 125 Shenzhen

What: Grant certificates to devices that pass security checks



Why: Use Cases

1. Grant internal network access to enterprise employees, through a MDM software

- **An power company inspector visits many (100) power substations, connect to its small wifi (through EAP-TLS), download data, do inspection, and go to next. He wants automated certificate management.**
 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.

- The policies that apply to certain (cloud) Key Management Service (KMS) instances.
- TLS / OS / Docker stacks have been recently patched (ie ≤ 3 months old).
- Private key resides in FIPS level 3 hardware and has `non-exportable=true`.

Changes from last IETF

Adopted by the ACME working group! Thank you!

Had 2 design meetings:

- 25-12-15, 26-01-13

Closed 2 PRs -- thanks MikeO for leading the discussion!

- **#25 big editorial pass**
 - Greatly enriched the texts: introduction, motivation, purpose and status-quo analysis...
- **#26 MikeO big pass on protocol details**
 - **Suggested a lot of important “major design decisions” in the next page, got agreed on, except a few minor like nonce choices**

Opened several issues

- For future discussion: like encryption mechanisms (for evidence), more details for nonce usage flow, ...

Major Design Decisions Until Now

- **How will attestation challenge work with other challenges:**
 - The remote attestation challenge supplements the identifier challenges (complete at least one) rather than replaces them.
- **'remote-attestation' identifier value:**
 - **Dummy, not an actual identifier, but a property to be attested. Could be empty (which means no specific request).**
 - Because it is supplementary to other "main" identifiers.
- **Where to carry Attestation Evidences/Results/Endorsements:**
 - **POST Attestation Result to challenge URL – ✓**
 - As opposed to put attestation result in the /newOrder payload, or pre-authorization – ✗
- **Format of Attestation Evidences/Results/Endorsements:**
 - **RATS Conceptual Message Wrapper [I-D.ietf-rats-msg-wrap] or raw JSON**
 - Evidences could contain sensitive information thus will be encrypted. In a JWE envelope.
- **Where and how should the Server provide an attestation freshness nonce to the ACME client?**
 - The Client SHOULD use the freshness_nonce randomly generated by the server, provided in remote-attest-01 Challenge Object, as an attestation freshness nonce.

Open issues for discussion: Suggestions welcome

1. The `freshness_nonce` provided in the Challenge Object MAY / SHOULD / SHOULD NOT / MUST NOT be the same as the ACME nonce or the ACME Challenge URL?
2. The `verifierEncryptionCredential` in the challenge object is a URL from which the Client can fetch a public key for Evidence encryption. Should it be always JWK format?
3. Will be cases where the attestation challenge does act as proof-of-control of an identifier, such as validating a Serial Number DN component?

Next steps

- ACME-RATS design team meeting continue
- **Finishing up TODOs and EDNOTEs like**
 - compare & contrast with draft-ietf-acme-device-attest
- If you are interested in participating the discussion, email:
 - Liuchunchi(Peter) liuchunchi@huawei.com
 - Mike Ounsworth mike@ounsworth.ca
 - Michael Richardson mcr+ietf@sandelman.ca