

# TEEP Protocol

## draft-ietf-teep-protocol-15

Dave Thaler <dthaler@microsoft.com>

# Timeline

- March 27: IETF 116 discussed draft-12
- May 1: draft-13 posted
- May 3: WGLC started
- June 1: WGLC ended
- June 16: draft-14 posted
- July 3: draft-15 posted
- July 19: document shepherd writeup
- July 22: Hackathon 117 raised two issues
- GOAL: post -16 this week
- Shepherd can then submit to IESG once confirmed ready

# Normative references

- draft-ietf-rats-eat: submitted to IESG
- draft-ietf-suit-manifest: submitted to IESG
- draft-ietf-suit-trust-domains: WGLC done, revised I-D needed
- draft-ietf-suit-mti: getting ready for WGLC
- draft-ietf-suit-report: getting ready for WGLC

# Changes since IETF 116

# #341: Attesting TAM from Agent

- Akira pointed out the TEEP Architecture talked about the TEEP Agent being able to attest the TAM's trustworthiness
  - This wasn't in the TEEP protocol draft
- Agent->TAM: Error can contain supported freshness mechanisms, error code `ERR_ATTESTATION_REQUIRED` and opt. attestation challenge
- TAM->Agent: QueryRequest can opt. contain attestation payload
  - attestation-payload-format, attestation-payload, suit-reports

# Hackathon 117

# IETF 116: Error return for QueryResponse

- TEEP Agent can return error via TEEP messages
- TAM has no way to return an error, e.g. processing a Query Response
- Examples: TAM rejects QueryResponse based on AttestationResult, or lack of reachability to a Verifier, etc.
- Sometimes fix is to push a SUIT update to the Agent, but not always:
  - Multiple TAMs, transient errors, etc.
- Added to Update message, for symmetry with QueryResponse:
  - ? err-code => uint .size 1,
  - ? err-msg => text .size (1..128),

# #347: err-code and err-msg in Update message

- Draft -12 updated syntax but not behavioral section which always said TAM could update the components on the Agent
- Draft -12 said about other QueryResponse errors:
  - If these requirements are not met, the TAM **drops the message**. It **may** also do additional **implementation specific actions** such as logging the results.
- Unclear whether TAM can send Update with err-code and err-msg in such cases
- Discussed at hackathon among implementers, and PR generated

# Behavior changes in PR #348

- Errors in QueryResponse Processing:
  - “If these requirements are not met, the TAM drops the message **and sends an Update message containing an appropriate err-code and err-msg**. It may also do additional implementation specific actions such as logging the results.”
- Attestation failure:
  - “In this case, the TAM ~~can~~ **might** attempt to use TEEP to update any Trusted Components ... **If the TAM does not have permission to update such components (this can happen if different TAMs manage different components in the device), the TAM instead responds with an Update message containing an appropriate err-msg, and err-code set to ERR\_ATTESTATION\_REQUIRED.**”

# Editorial changes in PR #348

- Since many error codes can now flow in either direction, needed editorial wording changes in their definitions to be agnostic
- Examples:
  - “The TEEP ~~Agent~~ **implementation** does not support the TEEP protocol version indicated in the ~~request received~~ message.”
  - “A ~~TAM~~ **TEEP implementation** receiving this error might retry the ~~request last message it sent to the sender of this error at some later point~~ without using any TEEP extensions.”

# Error codes

- Either direction:
  - ERR\_PERMANENT\_ERROR
  - ERR\_UNSUPPORTED\_EXTENSION
  - ERR\_UNSUPPORTED\_MSG\_VERSION
  - ERR\_BAD\_CERTIFICATE
  - ERR\_ATTESTATION\_REQUIRED
  - ERR\_CERTIFICATE\_EXPIRED
  - ERR\_TEMPORARY\_ERROR
- Agent->TAM errors:
  - ERR\_UNSUPPORTED\_FRESHNESS\_MECHANISMS
  - ERR\_UNSUPPORTED\_CIPHER\_SUITES
  - ERR\_MANIFEST\_PROCESSING\_FAILED

# #349: kid in EAT profile, COSE Key Thumbprint

- TEEP EAT profile section says:
  - “Key Identification: COSE Key ID (kid) is used, where the **key ID is the hash of a public key** (where the public key may be used as a raw public key, or in a certificate). See Section 7.1.1.1 and Section 7.2.1.1 for discussion on the choice of hash algorithm.”
  - Hash algorithm sections say SHA-256
- draft-isobe-cose-key-thumbprint
  - Defines how to compute a hash of a COSE Key
- Should we:
  - a) normatively reference this new draft (slows down publication)
  - b) informatively reference draft
  - c) not reference the draft

# Next steps

- Any other issues?
- Plan to post -16 this week
- Do chairs want another WGLC?