Remote Attestation ProcedureS virtual BoF

January 16, 2019

Chairs:

Roman Danyliw

Nancy Cam-Winget

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)

Agenda

1. Agenda bashing, Logistics -- Chairs (2 mins)
2. Chair’s view of current work items for the working group as presented/discussed by RATS participants and options for proposed scope (15 min)
3. Scope and Charter Open Discussion (45min)
4. Next Steps (remaining time)

Observations by the IETF 103 RATS BoF Chairs

From the IETF 103 BoF, public and private discussions on the next steps

January 15, 2019

There are different visions for the WG

(per the draft charter language published during IETF 103)

	Charter Program of Work Reference	Scope 1 (post IETF 103)	Scope 2 (post IETF 103)	Scope 3 (per mailing list as of 01/15/2019)
Architecture/Use Cases	#1	Yes. Mobile phones, IoT. No RoT assumptions	Yes. PCs, routers, IoT. Assume TPM	Yes. Assume nothing about the protection of the key on host
Claims/Token Format	#2 – 3	Yes	Yes	Yes
Protocol to Convey Claims	#4	No	Yes	Yes (as extension with current protocol?)
Protocol to Appraise Claims	#5	No	Yes	No

Further Observations

(1) No ML push back on Scope 1 $\subset$ Scope 3 $\subset$ Scope 2

(2) Divergent views on ML on "Is a hardware RoT a normative requirements?" Does weak or strong guidance on RoT/TPM at all impact the details Program of Work Items #2 – 5?

(3) Divergent views on ML on capabilities of protocols to convey (Item #4) and appraise (Item #5) claims

Testing Understanding of Feedback

Areas of Consensus = Scope #1	Area of Consensus = Scope #3	Details that don't impact the Program Work Items	No Consensus
Architecture/Use Cases (Program of Work #1)	Protocol to Convey Claims (Program of Work #4) – capabilities of protocol requires discussion	Is a hardware RoT a normative requirements? Does weak or strong guidance on RoT/TPM? Use case and deployment details?	Protocol to Appraise Claims (Program of Work #5)
Claims/Token Format (Program of Work #2 – 3)	+ Scope #1 Items (#1 - #3)		

1. Specify a terminology, architecture and use cases that enable explicit (a set of verifiable assertion/claims is transported in the attestation) and implicit (a set of assertions/claims is implied by possession of a secret) attestation techniques. The architecture may include a system security model for the signing key material and involve at least the system component, system component provider, and the relying authority.
2. Standardize an information model for assertions/claims which provide information about system components characteristics scoped by the specified use-cases.
3. Standardize data models that implements and secures the defined information model (e.g., CBOR Web Token structures [RFC8392], JSON Web Token structures [RFC7519]).

4. Standardize interoperable protocols to securely convey assertions/claims.

Possible Next Steps

	Possible Next Steps	Required Actions/Caveats
1	WG #1 charters for Scope #1	• Update current charter language to remove Program of Work #4 – 5. • Plan for drafting detailed Security Considerations to address security concerns for a format without a protocol • Submit charter for IESG considerations
2	WG #1 charters for Scope #3	• Update current charter language to remove Program of Work #5. • Submit charter for IESG considerations
3	WG #1 charters for Scope #2	• Gain community consensus on Program of Work #5 • IETF 104 BoF?
4	WG #1 charters for Scope #1; and WG #2 charters for Scope #2 (relying on WG #1)	• More discussion required
5	?? Something else ??	