Authentication and Authorization fo r Constrained Environment (ACE)

WG Chairs:

Kepeng Li, kepeng.lkp@alibaba-inc.com

Hannes Tschofenig, hannes.tschofenig@gmx.net

Security AD:

Kathleen Moriarty, Kathleen.Moriarty.ietf@gmail.com

Mailing List: ace@ietf.org

To Subscribe: https://www.ietf.org/mailman/listinfo/ace

Note Well

- Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:
  - The IETF plenary session
  - The IESG, or any member thereof on behalf of the IESG
  - Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
  - Any IETF working group or portion thereof
  - Any Birds of a Feather (BOF) session
  - The IAB or any member thereof on behalf of the IAB
  - The RFC Editor or the Internet-Drafts function
- All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).
- Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.
- A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
- A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Milestone Check

Time	Item
Done	Submit “Use cases and requirements” as a WG item
Done (Aug, 2015)	Submit “An architecture for authorization in Constrained Environments” as a WG item
Done (Oct, 2015)	Submit “Use cases and requirements” to the IESG for publication as an Informational RFC
Dec, 2015	Submit “An architecture for authorization in Constrained Environments” to the IESG for publication as an Informational RFC
Jan, 2016	Submit “Authentication and Authorization solution” specification as a WG item

Agenda

* Agenda Bashing (Chairs, 5 min)
* Actors (Carsten Bormann, 15 min)
    - http://datatracker.ietf.org/doc/draft-ietf-ace-actors/
* DCAF (Stefanie Gerdes, 20 mins)
    - https://tools.ietf.org/html/draft-gerdes-ace-dcaf-authorize-04
    - https://tools.ietf.org/id/draft-gerdes-ace-dcaf-sitr-00.txt
* ACE Solutions (Jorge Cuellar, 20 mins)
    - https://datatracker.ietf.org/doc/draft-cuellar-ace-solutions/
    - https://datatracker.ietf.org/doc/draft-cuellar-ace-pat-priv-enhanced-authz-tokens/
* Authorization using OAuth 2.0 (Ludwig Seitz, 20 min)
    - https://datatracker.ietf.org/doc/draft-seitz-ace-oauth-authz/
* Discussion about the solution direction (all, 55 min)
* DCAF COSE (Stefanie Gerdes, 10 mins)
    - https://datatracker.ietf.org/doc/draft-bergmann-ace-dcaf-cose/
* Wrap-up (Chairs, 5 min)

Solution Direction

- DCAF
- OAuth Profiling
- DCAF and OAuth Profiling
- Others?

Solution Comparison

Aspects	DCAF	OAuth Profiling
Architecture	Four entity architecture (with CAS). Protects both sides of the communication between C and RS.	Three entity architecture (No CAS). Protects only RS side.
Fit into Constrained Environments	Support of secure constrained device to constrained device communication. Both Client and RS can be constrained.	Use Token Introspection for constrained clients.

Communication Models	Client initiated ticket model, RS can be offline.
	Server initiated ticket model, client can be offline.
		Client and RS are offline;
		RS offline;
		Client offline;
		Always-on connectivity;
		Token-less authorization.

Security	Use symmetric session key between Client and RS. Other communications can be asymmetric.	Use both symmetric key and asymmetric keys.
Privacy	Does not need identifiers on the constrained-level that could be tracked.	
Implementations	?	?
Assumption	Minimal complexity on constrained device.	Maximum integration with OAuth.