ACE WG
Friday, March 29, 2019
1050 - 1250, Morning session II
Grand Ballroom

==[Agenda]==

(3) EST over secure CoAP (10 min)
- presenter: Peter van der Stok
- draft: draft-ietf-ace-coap-est
WGLC concluded; all comments believed to have been acted on.
(Note: PKIX-cert can return either PKCS7 or PKIX-cert object, so draft needed to be enhanced to allow for this.)

(4) ACE-OAuth and Parameters (15 min)
draft: draft-ietf-oauth-authz, draft-ietf-oauth-params
presenter: Ludwig Seitz
Hannes Tschoefenig: which interface is being referred to in the requirement for secure communication “binding response to request”? - token interface, introspection, or resource server interface
Karan Saini: should the draft specify values for rate limitation? - likely to be very application-specific. Please ask this question via the list.
LS noted (updates 17-19) the possibility of terminological confusion around “authorization information” and “acccess information” - the latter referring specifically to information an AS sends to the client in an access token response.
Security considerations for multi-RS audiences: symmetric PoP keys or access token protection keys are not OK under these circs, because they don’t distinguish between members of the group. Draft updated accordingly
R Wilton - with what? - with a requirement to the effect that symmetric keys ?must/should not be used in these circumstances.
HTschoefenig: Did you include the resource parameter as well as the audience parameter? - framework defines a mapping for audience, but not for resource curreently, though recognises that this would be useful and would not require a significant change.
Parameter mapping: LS has now created a mapping table to ensure that parameter mapping updates are reflected in all the required places (e.g. in the framework *and* in the params specification).
In response to q from HTschoefenig: Processing instructions for cnonce were updated for imprecisely-synchronised clocks. This is just one of a number of mechanisms available for handling roughly-synchronised clocks; DTLS’ mechanism for handling this was generic enough to merit inclusion in the framework as a generalisable technique.
(5) DTLS Profile for ACE (15 min)
- presenter: Ludwig Seitz (for Göran Selander)
- draft: draft-ietf-ace-dtls-authorize
Status: publication not requested yet, but a new version is imminent.
Göran Selander: 08 is already on Github, but the version currently Datatracker is 07
(6) Key Provisioning for Group Communication (10 min)
- presenter: Francesca Palombini
- draft: draft-ietf-ace-key-groupcomm
LSeitz- if a KDC has to deal with different groups, it should do so by defining different Resources, so that each group‘s requests go to a different server endpoint.
CBormann - what does a ‘leave’ parameter in single quotes mean, in terms of expected data format? - take to list
Peter vd Stok: makes sense to me to add finer granularity to the SCOPE parameter.
LSeitz - recommend loooking at CBor’s (expired) AIF draft (AuthZ Information

Format).
Peter vd Stok: Key Redistribution Initiated by KDC; are you talking about multicast here? - yes
Daniel Migault: better to say “we don’t deal with this”, at least for this draft.
LS - try to avoid having clients obliged to listen on the network for an interrupt, because this is costly in terms of battery power for constrained devices.
(7) Group OSCORE (10 min)
- presenter: Marco Tiloca
- draft: draft-ietf-ace-ey-groupcomm-oscore
Please come to Montreal prepared to try OSCORE at the hackathon...
(8) MQTT-TLS Profile (15 min)
- presenter: Çiğdem Şengül
- draft: draft-sengul-ace-mqtt-tls-profile
- Adoption call by chairs
MQTT: OASIS pub-sub protocol running over TCP, with TLS recommended.
MQTT broker is, for ACE purposes, treated as a resource server.
LS - “Token in CONNECT” specification looks like it needs better (some) protection against replay attacks. - Yes, will consider including a random value in the signed package.
CS - Is the WG in favour of adoption?
LS - lots of visible IoT deployments using MQTT, so in favour of adoption
Dave Robin - supportive, esp. for fine-grained
Hannes Tschoefenig: “MQTT is significant though unpopular”; supportive
Peter vd Stok: important to support the ace-key-groupcomm work
Daniel M: will take the adoptn request to the list. No opposiing voices in the room.
Time Permitting Items
(9) Client Disadvantaged (5 min)
- presenter: Ludwig Seitz
- draft: draft-secheverria-ace-client-disadvantaged
Clients in “disadvantaged networks”; these are “like constrained networks, but worse”. e.g. intermittent, frequently interrupted, limited connection; high risk of sabotage, impersonation, device capture.
(e.g. law enforcement, first response, military...)
Introduces conflicting requirements for token lifetime - i.e. you don’t want to depend on being able to get frequent token updates, but the negative impact of long-lived tokens could be significant if a device is compromised.
Jim Schaad (as individual): doc was interesting but only partially addressed the problem scope.
Carsten Bormann: the DTN WG already works on this, so worth finding out if there’s overlap and possibility of information exchange (in both directions).
(10) Alternative Enrolment Protocols
- presenter: Göran Selander (as himself)
- draft: draft-selander-ace-coap-est-oscore
“Protecting EST payloads with OSCORE”
draft-selander-ace-coap-est-oscore
(The corresponding draft on using COAPS (DTLS) is already done, as the WG asked for that to be done first)
est-oscore turns out to ne able to reuse much of EST-coaps enrolment protocol, with a few differences, but the rationale remains the desire to have a protocol that can handle non-DTLS devices by using OSCORE.
Peter vd Stok: can’t see this being used in general certificate distribution, but can definitely envisage it in BRSKI deployments
C Bormann: we could use up some vacant time by exploring the use of est-oscore to distribute certificates other than X.509.
(11) Open Mic
(12) Closing and Summary (chairs, 5 min)
- presenters: chairs
Jim Schaad: EDHOC summary posted on secdespatch list; please go there to express

your views, whether +ve or -ve. Goal appears to be to create a WG without going through the BoF process first.
Ben Kaduk: please make any comments on the list specific.
CBor: ACE might be a “customer” of EDHOC - so would ACE WG be in favour of the WG? CORE was in favour.
HT: “What I heard was that CORE was happy not to do EDHOC’s proposed work in CORE... so not quite the same thing.
Roman Daniliw: one challenge with EDHOC formation was that the conversation was v distributed. Please bring it to secdespatch. We think the proposal write-up is complete.
Göran: please review the list archive if unclear about what has been raised/explored/discussed/decided in the EDHOC formation process; we think the critical requirement areas have been discussed.
Francesca Palombini: please mention the interim sessions.
Jom Schaad (as chair): CORE and CBOR have held alternating weekly meetings. ACE planning to schedule interims between now and Singapore, and will poll the mailing list in search for a consistent and convenient time.
Ari Keränen: seems to be support for both the group and its proposed way forward.