ACP status
IETF 106 Singapore 2019

draft-ietf-anima-autonomic-control-plane-21

Toerless Eckert tte+ietf@cs.fau.de (Futurewei USA)
Michael Behringer michael.h.behringer@gmail.com
Steinthor Bjarnason sbjarnason@arbor.net

v1.0

Status

- IETF 105:
  - Described changes up to draft-ietf-anima-autonomic-control-plane-20
- Since then
  - Resolved open Discuss with Alicia -> closed DISCUSS
  - Attempted to resolve two remaining DISCUS from Ben Kaduk / Eric Rescorla
  - Ben had taken responsibility for Erics discuss after Eric left IESG.
  - No response yet from Benon -20 (posted on July 24)
  - Posted -21 to resolve IMHO all remining DISCUSS issues not addressed in -20
    - Want to keep current defined ACP domain information string (Ben was suggesting mayor rework)
      - Reason: We had dsicussion in IETF105 and ability to se/read rfc822address from existing (ioT) certificate libraries was recognized as good reason why current choise is simple.
    - Tried to close all open encryption detail gaps.

-20 -> -21 (1)

6.1.1 - ACP certificates

-20: MUST have ECDH public key

SHOULD be signed with ECDH, else MUST be signed with RSA

-21: ACP nodes MUST support RSA and ECDH public key

ACP certificates intended to be used beyond ACP:

- SHOULD use RSA key and RSA signature

ACP certificates intended to be used ONLY for ACP:

- MAY use ECDH public key and ECDH signature

MUST support 2048-bit RSA using SHA-256, SHA-384 or SHA-512
Elliptic Curve using NIST P-256, P-384, or P-521 as key lengths
as key length in ACP certificates/signatures.

Further certificate attributes: may follow CABFORUM recommendations

Reasoning: RSA more widely used, therefore MUST RSA, ECDH allows shorter key length at same security, unless we make it MUST, we can not build an ACP that leverages this benefit.

CABFORUM difficult to make normative reference, so just “may follow”

-20 -> -21 (2)

-21: 6.7 security associations

Any security association protocol MUST use PFS

may use secure channel protocol only to derive key for underlying strong L2 security (e.g.: MACSEC).

Explanation: to avoid duplication of encryption L2 / secure channel

-20 -> -21 (3)

-21: 6.8.2 TLS for GRASP

MUST offer TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

MUST NOT offer options with less than 256bit AES
or less than SHA384.

TLS for GRASP MUST include the "Supported Elliptic Curves" extension, it MUST support support the NIST P-256 (secp256r1) and P-384 (secp384r1(24)) curves [RFC4492].

GRASP TLS clients SHOULD send an ec_point_formats extension with a single element, "uncompressed".

For further interoperability recommendations, GRASP TLS implementations SHOULD follow [RFC7525].

Explanations: selected profiles (GCM_SHA384) where intersections between RFC7525 and Ben Kaduks examples given in his -19 review.

keep MUST requirements to minimum: This is all new code (GRASP), so no need to figure out more backward compatibility options.

Process

- IESG reviewers so far:
  - Owner: Terry Manderson (Yes) (left IESG)
  - Benjamin Kaduk (SEC) (closing DISCUSS with him)
  - Eric Rescorla (SEC) (left IESG)
  - Deborah Brungard
  - Ben Campbell (left IESG)
  - Alissa Cooper
  - Spencer Dawkins (left IESG)
  - Suresh Krishnan
  - Warren Kumari
  - Mirja Kühlewind
  - Alexey Melnikov
  - Adam Roach
- These reviews would have suffice to pass IESG review, except:
  - When members leave IESG, their review votes turn into pumpkins
  - Review needs to be restarted at least with additional IESG reviewers
  - But: Owner also had turned into pumpkin (Terry Manderson)
    - Logical new owner would have been WG AD (Ignas) but he recused himself
    - New owner AD will define process

Current status

- Closing current SEC review with Ben Kaduk
  - Forwarded what he sees as missing Ipsec parameters to IPsec expert.
  - Ben wants to bring up issue with ACP domain information encoding
    Need a slot for this on Wednesday ANIMA WG session to discuss in meeting
- Proposed new AD owner of document:
  - Eric Vyncke (INT)
    Can only finish review in January, but will meet in December to prep.
  - Plans to resubmit doc to IESG (two additional reviewers beyond him)
  - Authors will push out another revision to summarize changes (in changelog section) so as to give context to new IESG reviewers.
- Expressed concerns about process
  - To IESG about rule that leaving IESG member votes turn into pumpkins
  - Raised case with datatracker tool team to have a new notification for this condition:
    - Neither IESG, WG AD, chairs seem to have recognized this “missing reviews” condition earlier

Thank You!