ACP status

draft-ietf-anima-autonomic-control-plane-19

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 104:
  - draft-ietf-anima-autonomic-control-plane-19
- IETF 105:
  - draft-ietf-anima-autonomic-control-plane-20 (posted Monday_
  - Ongoing IESG DISCUSS
    - Eric Rescorla – reply to original -16 DISCUSS where included into -19/IETF104, but IESG term expired. Benjamin Kaduk took over reviewing and replying to that original discuss.
    - Benjamin Kaduk
      - reply to original -16 DISCUSS was included into -19/IETF104, received second reply to that last week. Reply to that included into -20
      - Took over reviewing for Eric Rescorla. Reply to that review (last week) also included into -20
      - New DISCUSS against -19 on ietf datatracker, reply to that also included into -20
    - Alissa Cooper / GENART (Elwyn)
      - Had opened discuss 8/1/2018. Reply on 8/8/2018.Not sure where reply got lost.
      - Send reminde
    - Mcr: overlooked github pull from beginning of the year
  - Outstanding issues
    - Finalize any missing magic words (256 bits ? Keylength) to have complete security profile information
    - Decide on format of ACP domain-information field.

Changes -> closed ?! (1)

Many smaller textual nits (thanks a lot, Ben!)

6.1.3 (was 6.1.2) – "ACP domain membership check"

– emphasizes how this includes action of a security association protocol (example IKEv2 proof of ownership of cert)

- **refers to relevant parts of rfc5280 (cert chain verification)**
- **refines that CRL/OCSP are skipped only in absence of getting the information for them via secure association protocol. E.g: with stapling we can always get revocation information.**

– New summary at end of section to restate purpose of steps of domain membership check.

6.1.5 (was 6.1.4) "Cert Renewal"

– added requirement for EST server certificate to have extended key use id-kp-cmcRA so clients can trust them when requesting refreshed CA certificates.

– explains how to set up EST server for multiple ACP domains.

Changes -> closed ?! (2)

6.1.5.1 GRASP objective for SRV.est

- **(Mcr) Changed TCP port for SRV.est from 80 to 443 (EST is using TLS).**
- **Added: Unknown elements in GRASP objective values MUST be ignored.**

6.1.5.3 CRLs

- **CDP distribution uses HTTP, not HTTPs (circular dependencies, payload authenticated).**

6.3 – DULL GRASP

- **explains why certs are not signaled in DULL grasp (certs in multicast packets). Relevant because security association protocols have options and would like to only signal cert hash or URL to be more efficient themselves.**

Changes -> closed ?! (3)

6.7 - Security association protocols intro (new)

- 5 new paragraph (biggest set of added text) to cover generic requirements (not specific to individual profiles like those for IPsec/DTLS).
- hop-by-hop hence no network wide MTI needed.
- must be able to signal directly full certificates.
- all security associations must have equivalent degree of security to not create "weakest link"
- L2 security (WiFi/MACSEC examples) may stand in for encryption, but may still need L3 security association for mutual authentication first. (no solutions included in this doc)
- Strong physical security may stand in for cryptographic -> ACP connect. But can never be autoconfiguring, so limited use (aka: in NOC room). (and of course limited use because most cases there is no physical security).

Changes -> closed ?! (4)

6.11.1.14 RPL routing unknown destination (diagnostic) (Ben DISCUSS)

- No requirement for this forwarding plane enhancemeent on “stupid” nodes (not able to be registrar, ACP-connect, configured root priority).

8.1.5 – GRASP via ACP connect

– removed suggestion for policy filtering of GRASP messages. Was mistaken to be a security aspect whilst it was really just too advanced policy considerations to bother in this text.

10.3.5.1 – ACP/ANI configuration

– Justification text why brownfield ANI MUST be explicitly configured (operator doesn't even bother to know what a MASA is, so attacker can more easily try to impersonate operator with vendor – with identity theft methods).

10.3.7 – "ACP configuration"

– added text about ACP-connect configuration and how simple it can be (one command, plug NOC nodes to that LAN port).

Changes -> closed ?! (5)

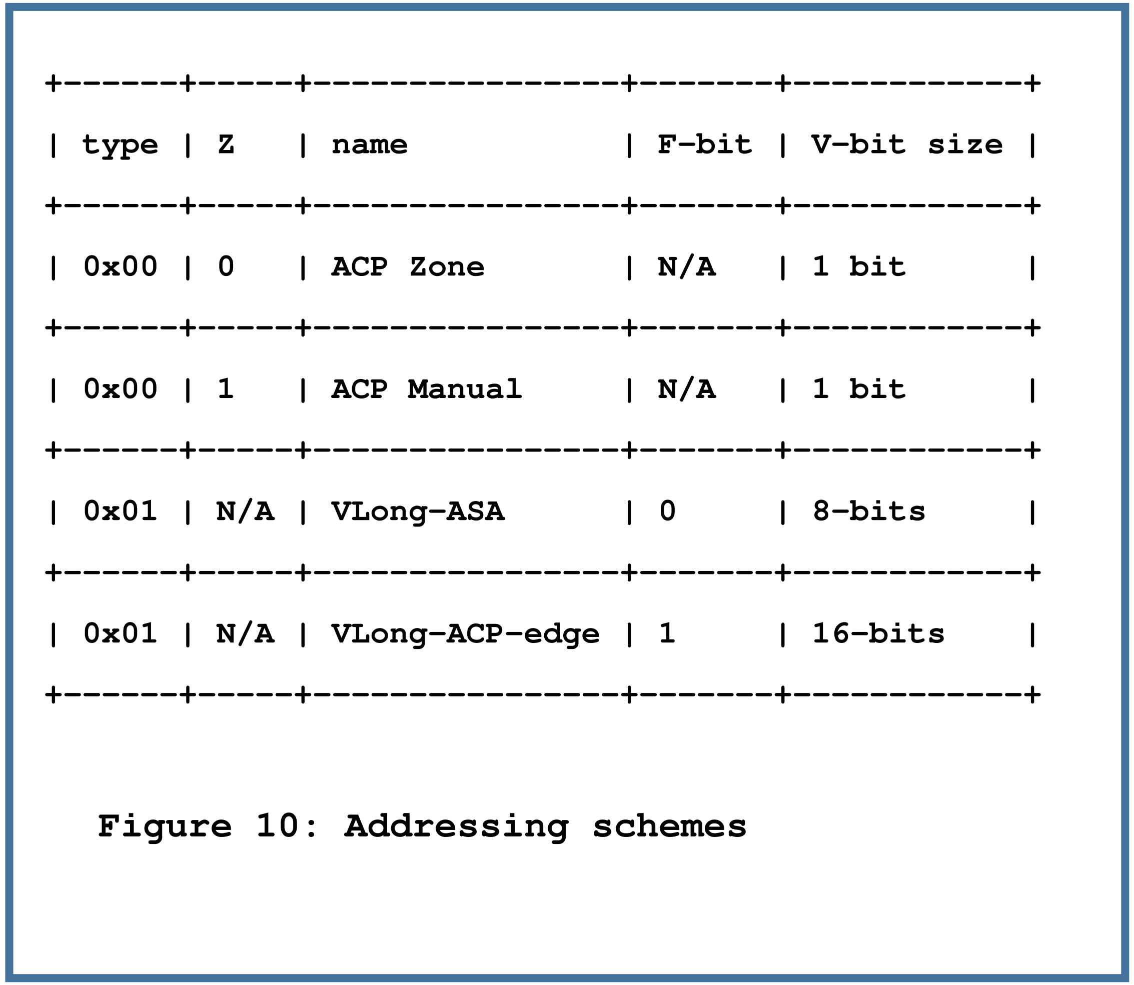
A.6 - "dual-stage security association negotiation via GRASP"

- Previously agreed in WG review to remove - added RFC editor note to remove before publication.

A.7 - Diagnostics

- LLDP etc. noting that exposing IDevID may in more security conscious environments be undesirable (optimize attacks by knowing what device is for example).

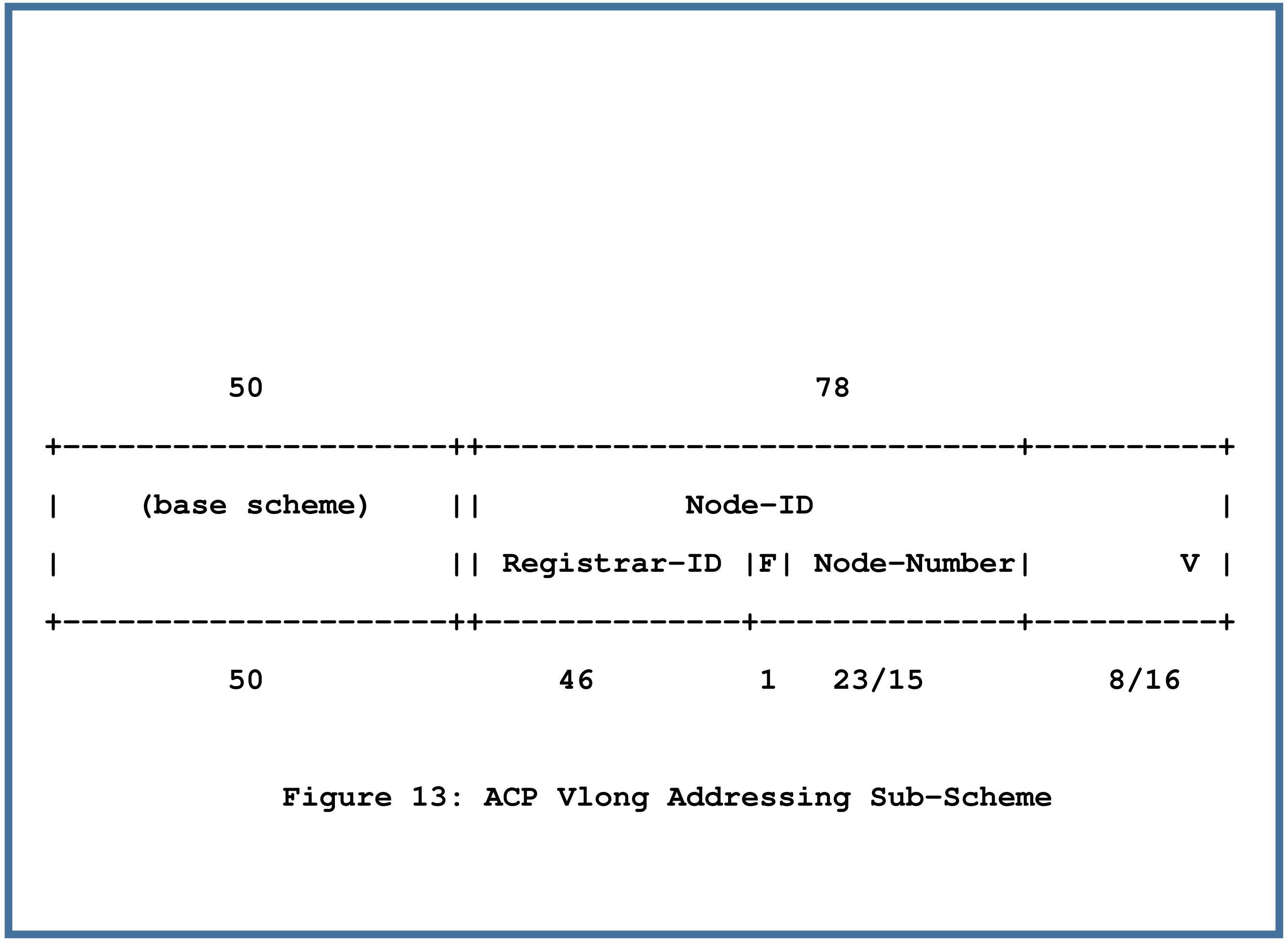
Best ASCI art awards



```
+------+-----+----------------+-------+------------+
| type | Z   | name           | F-bit | V-bit size |
+------+-----+----------------+-------+------------+
| 0x00 | 0   | ACP Zone       | N/A   | 1 bit      |
+------+-----+----------------+-------+------------+
| 0x00 | 1   | ACP Manual     | N/A   | 1 bit      |
+------+-----+----------------+-------+------------+
| 0x01 | N/A | VLong-ASA      | 0     | 8-bits     |
+------+-----+----------------+-------+------------+
| 0x01 | N/A | VLong-ACP-edge | 1     | 16-bits    |
+------+-----+----------------+-------+------------+
```

Figure 10: Addressing schemes

Winner



```
          50                               78
+---------------------++-----------------------------+----------+
|    (base scheme)    ||          Node-ID                       |
|                     || Registrar-ID |F| Node-Number|        V |
+---------------------++--------------+--------------+----------+
          50                  46         1   23/15         8/16
```

Figure 13: ACP Vlong Addressing Sub-Scheme

2nd place

Encoding of ACP domain-information into Cert

- Currently: rfc822Name (IA5String) object, rfc822 encoding:
    - ***ACPRFC+acpaddr+options@acpdomain***
    - Lots of reasons named: backward compatibility, ease of coding (no new ASN.1),…
- Bens DISCUSS:
    - Assign new otherName code point for this (IANA), proposes one-off-binary encoding (no ASN.1 struct)
- Toerless thinking:
    - Need human readable / NOC backend tool processable string standard representation. Why two enodings then.
    - local@domain is a common for identities anyhow (just the options make it a bit more awkward)
- Toerless counterproposal in -20 replies
    - Use of otherName is fine if
        - We can safely assume its as easy to code with worst available ASN.1 libraries as rfc822Name (IOT libraries ?!)
        - Unmodified diagnostic tools would be able to show new field if it also was IA5String (BER/DER are TLV AFAIK, so theoretically possi ble)
    - Keep human readable string encoding (maybe slightly improve)
        - Now its just a typical local@domain identity, not necessarily constrained by rfc822 rules
        - No 64 byte limit for local part
        - Could even bring back Brians preferred ipv6 address representation (including ":" between octets). But would make it 25% longer
        - Any other changes to make it look even nicer possible (ideally without length extension)

Security profiles - certificates

- New text in 6.1.1 – generic ACP cert requirements
  - MUST be compliant with RFC5280 (most encoding, not really profiles, just cert-chain algorithm beyond encoding)
  - Minimum fields in ACP cert is whatever is needed for ACP domain membership check
  - Anything beyond that is whatever operator needs for any other authentication/authorization he wants to use ACP certs for
  - Diagnostics nice: include device identifiers from IDevID (but “privacy”) risk
- CRYPTO:
  - MUST have ECDH key, Should be signed with ECDH Key, otherwise MUST be signed with RSA key (doh ?). *Reason: ECDH is shorter (need all space in ACP cert for domain info string (grin).)*
    - Implies required ability of any secure channel protocols to deal with these certs.
  - *WHAT CRYPTO PARAMETERS ARE MISSING:*
    - *Minimum signing key length ?! – What are good ECDH suggestions, RSA suggestions (256 bit for RSA ?!)*
  - COMPLAIN (see also “no whining sticker”):
    - Found no good RFC for this
    - Good documents for security protocols bail on this issue. E.g.: RFC8247 (IKEv2 requirements):
    - *Cryptographic recommendations regarding certificate validation are out of scope of this document. What is mandatory to implement is provided by the PKIX community*
      - *No required reference when this RFC went through IESH review ? How can IKEv2 implementations interop, if their certs do not ?*

Security profiles – IPsec/IKEv2

- 6.7.1.1 – Native IPsec/IKEv2 secure channel association
  - Relying on discovered Ipsec/IKEv2 parameter requirements – RFC8221/RFC8247
  - Ipsec (forwarding plane)
    - Stripped down to just one profile – no backward compatibility needed now (new solution) – looking for maximum perfor mance
  - IKEv2
    - no stripping down from RFC8247 ("it's just software").
  - Note that we can still do later different IKEv2 "IoT" profiles – it's just hop-by-hop no need for MTI, reme mber ?
  - CRYPTO:
  - IKEv2 MUST use "PKCS #7 wrapped X.509 certificate" (0) (see [IKEV2IANA] (for ACP cert authentication
  - IKEv2 MUST signal all intermedia certs if there is a chain.
  - IPsec MUST support ESP with ENCR_AES_GCM_16 ([RFC4106])
    - AFAIK: GCM removes need for separate integrity hash to be specified.
  - MUST NOT allow NULL encryption
  - MAY support any other crypto profiles as long as they do not lead to a lower security.
  - *WHAT crypto Parameters are missing ???*

Security profiles – secure channels via DTLS

- Existing text passed IESG review ?!
- Only had to add BCP 195 to existing RFC7525 reference

Security profiles – ACP GRASP e2e/p2p via TLS

- 6.8.2 (ACP as security / transport substrate for GRASP)
  - *Notes for presentation*
  - *P2p ACP GRASP just uses TCP (relies on ACP secure channel), only end-to-end GRASP uses TLS.*
    - *When we add full support for IoT devices not supporting TCP, we would need to add requirements for non-TCP e2e GRASP to existing non-IoT devices unless we do not want any-to-any communication anymore (GRASP is just placeholder for "any e2e control connect)*
  - Added requirement reference to RFC7525 (toerless forgot it was not just DTLS but also TLS)

  - Ongoing discuss with Ben what security profile(s) to demand:
    - "TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 a
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - Specify a RSA/ECDSA key size (and elliptic curve for ECDSA)
    - Nature of the ECDHE or DHE.

  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 sounds good ?
    - (just because it helps me avoid having to think aout further implications of ECDSA ?)

    - No idea what "nature" means
    - Will start reaching out to more people for help if no suggestion from Ben

Thank You!