ACP status
IETF 102 Montreal 2018

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

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

v1.0
Status

• IETF101:
  • draft-ietf-anima-autonomic-control-plane-13
    • WG was in IETF last call (from Feb 2018)
    • Cleared IESG review Terry Manderson, Deborah Brungard, Spencer Dawkins, Warren Kumari Mirja Kuehlewind. 5 more IESG votes to go additional ones from Pascal Thubert (IOTDIR), Joel Halpern, Elvyn Davies (GenART)
    • ... No technical changes but a good amount more explanatory text added

• IETF 102:
  • draft-ietf-anima-autonomic-control-plane-16
  • On IESG Telechat beginning of August
Changes

• Many detail clarifications from various reviewers
• New 1.1: Applicability and Scope
• Terminology added: in-band, out-of-band management, registrar
• 6.1.3.3 Certificate Revocation List Handling
• 6.1.3.4 Lifetime of Certs (suggest short as being now easy to handle)
• 6.1.3.5 Re-enrollment (suggest Registrar can re-enroll easily after expiry)
• 6.1.3.6 Failing Certificate (node figures out if it should re-enroll)
• Split informative section:
  • 10. ACP operations – Informative, but important
    • NEW: Registrars, OLD: Diagnostics, Enabling/Disabling ACP
  • 11 Background and futures - informative, could become appendix if IESG wants
    • ALL OLD discussions about why decisions were made, what could be done in future.
Registars

• ACP document previously tried to stay clear of documenting Registrars
  • Thought this was job of BRSKI
  • But anybody can be a Registrar, not just BRSKI
  • And a BRSKI registrar who does not care about ACP would not need to care about ACP information field handling
    • ACP address assignment that the registrar needs to do as part of enrolment
    • ACP information field in certificate already documented in ACP, not BRSKI
  • Aka: needed text to describe what a registrar is IN ACP document
    • Ensure BRSKI is not considered a normative reference for any ACP node
      • ANI node: ACP + BRSKI (MUST do ACP, MUST do BRSKI)
    • Make it clear any other protocol can be used by registrars
      • Netconf Zerotouch for example
    • Registrar does not need to be software!!!
      • Makes range of options more obvious (IMHO)
ACP Registrar operations

worst case example

NOW HIRING!
ACP DOMAIN REGISTRAR!
No experience required !!!
Anybody can apply

ACP Registrar

Domain: lake

ACP

Domain Admission Controller

Address allocation database
Chick6: fd89b714f3db0000200000064000006

Certificate Authority

Domain Registrar

Optional
Get permission to admit pledge

Allocate Address

Make CA Sign pledge certificate

Optional
For secure/ANI
Pledges:
Get voucher

MASA
Registrar behavior

• 6.10.7 – ACP registrars (normative)
  • Responsible that pledge gets domain certificate with ACP info.
  • BRSKI or any other method (If you want to call ACP device ANI device, MUST use BRSKI)
  • Responsible to allocate address (may outsource). Discusses when/why different possible addressing sub-schemes should be assigned to new ACP nodes. Address persistence across renewals.

• 10.2 ACP Registrar (informative) – “operational aspects”
  • Textual explanation of prior slide picture – without any of the fun
    • Registrar interactions, registrar parameters,
    • Certificate renewal and limitations
    • ACP registrars with Sub-CA (very useful option to deal with rogue registrars).
    • Centralized control policies (multiple registrar, central admission policy)
Thank You!