ACME DTN Node ID Validation

BRIAN SIPOS

RKF ENGINEERING SOLUTIONS

IETF108

DTN Background

- DTN Architecture in RFC 4838
- Store-and-forward of Bundles
  - Similar to email over SMTP
- Overlay network
  - Rely on Convergence Layer adaptors for bundle transport between nodes
  - Late binding of Endpoint IDs
  - Bundle forwarding and routing
- End-to-end and per-hop security mechanisms

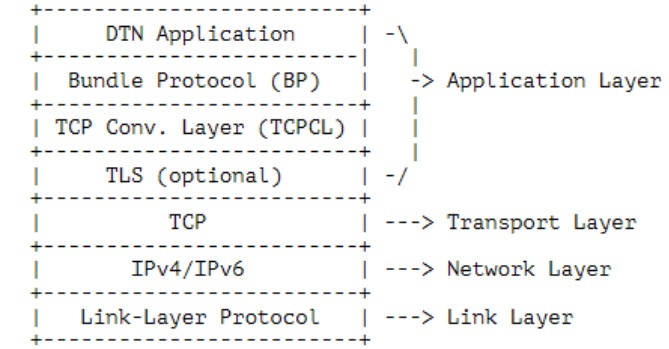
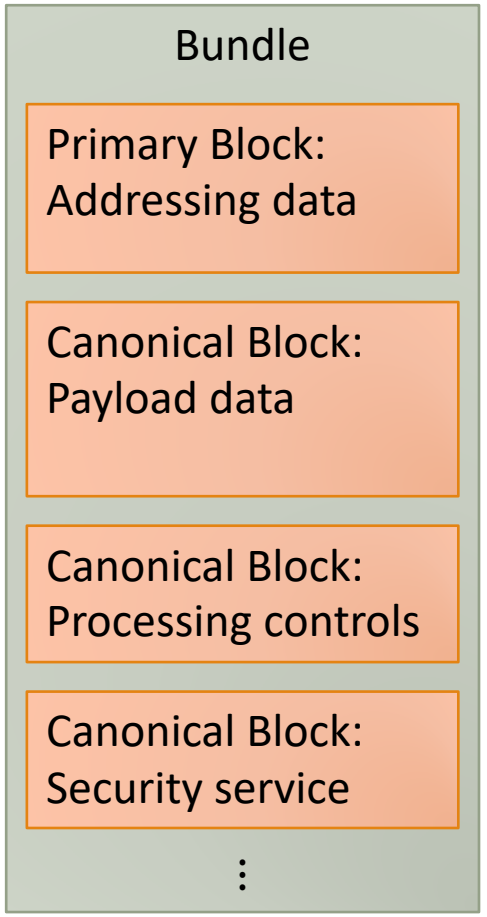


Figure 1: The Locations of the Bundle Protocol and the TCP Convergence-Layer Protocol above the Internet Protocol Stack

DTN Bundles

- The Bundle is the protocol data unit of DTN BP.
- A Bundle is composed of blocks.
  - One Primary block with addressing and bundle-wide parameters.
  - Sequence of Canonical blocks with type-code and block-type-specific-data.
- One canonical block is the Payload.
  - Administrative Record payloads are addressed to Node ID and processed by BP agent.
- Each bundle is stand-alone unit.
  - Addressed to an Endpoint ID
  - Sourced by a Node ID
  - Source of admin. Records can be replied-to.
- Bundle Security (BPSec) can be used to cryptographically sign, MAC, or encrypt blocks.



Motivations for Node ID Validation

- Proposed DTN TCP Convergence Layer Version 4 defines a PKIX certificate authentication mechanism.
  - Two modes of authentication: Node ID (as URI) and DNS name.
  - DNS name validation defined in RFC 6125.
  - URI validation is defined by TCPCL (RFC 6125 has only DNS-related definition).
- Question was raised “How should a CA validate a DTN claim?”
- ACME provides a well-established mechanism to do all the important bookkeeping needed by a CA.
  - Prefer this over ad-hoc mechanisms that don’t provide strong guarantees of fitness.

Proposed Validation Mechanism

- Very similar to proposed [draft-ietf-acme-email-smime].
  - New BP Administrative Record type defined.
  - Challenge Bundle supplies token-part1.
  - ACME server supplies token-part2.
  - Response Bundle combines token and generates Key Authorization result.
- Recommends Bundle Integrity cryptographic signing.
  - Useful to pass network security policy.
  - Not needed for validation itself.

Desired WG Direction

- Currently drafted as Experimental.
  - The DTN protocols are entering Standards Track status.
  - No other ACME mechanisms currently validate URI claims.
- Proposed as “If you want to do this thing, here is the best way to achieve it.”
- Any desire by ACME WG to adopt a URI validation?
- Distinction between mandatory-to-implement and optional validation mechanisms?

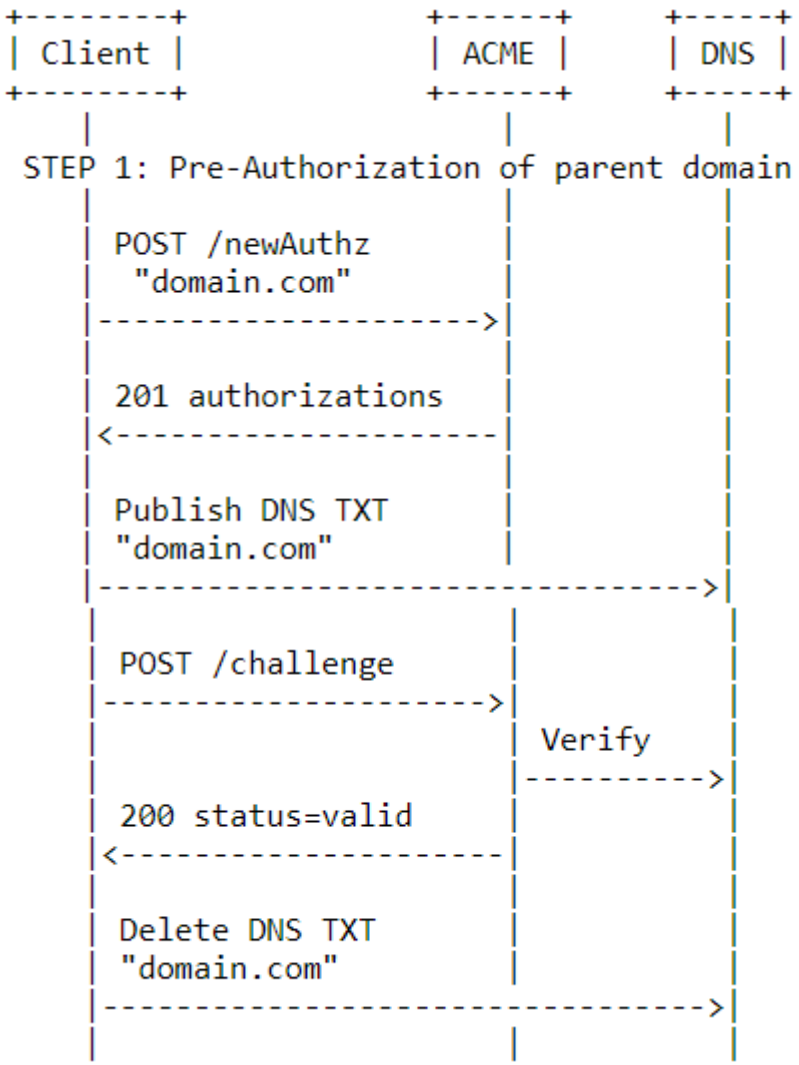
draft-friel-acme-subdomains-02

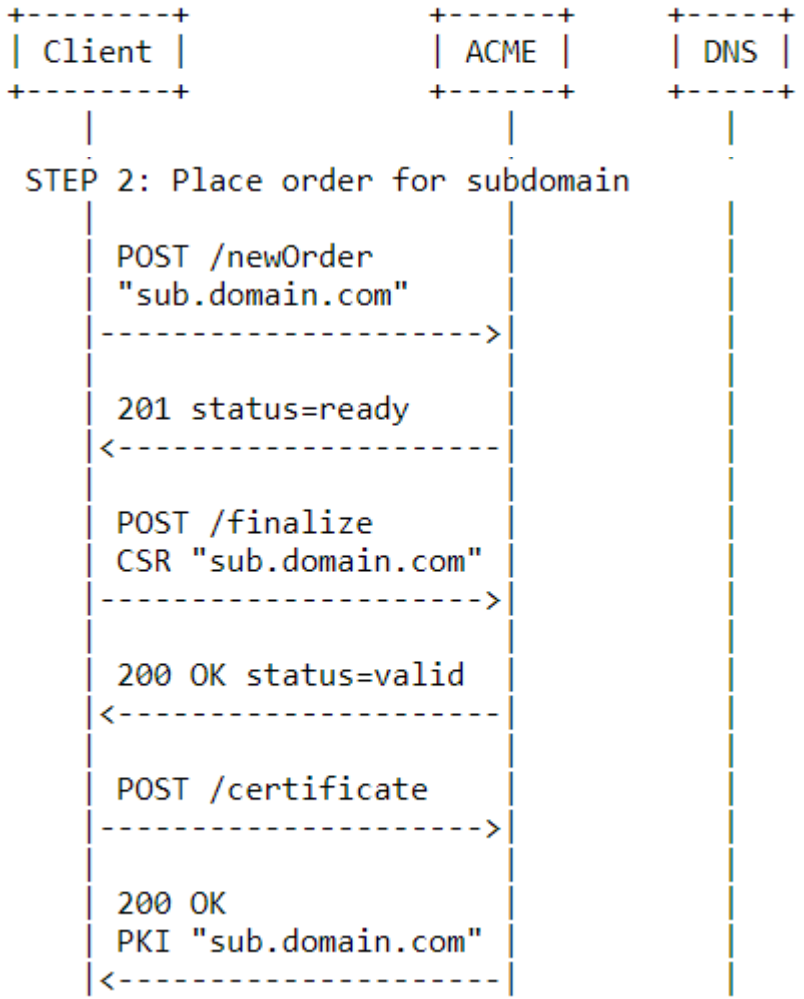
Friel, Barnes	Cisco
Hollebeek	DigiCert
Richardson	Sandelman Software Works

Sub-domain certificates

- ACME (RFC 8555) allows an ACME server to issue certificates for a given identifier (e.g. a subdomain) without requiring a challenge to be explicitly fulfilled against that identifier
- An ACME server could issue a certificate for **sub.domain.com** where the ACME client has only fulfilled a challenge for **domain.com**
- An ACME server could issue certificates for a number of sub-domain certificates and only require a single challenge to be fulfilled against the parent domain

Sub-domains with pre-authorization





Updates since IETF106 / draft-01

1. Defines “basedomain” boolean field in authorization object to explicitly differentiate between parent or base domain authorizations and wildcard authorizations
2. Clarify that base domain authorizations may optionally be used with the pre-authorization workflow, but pre-authorization is not mandatory
3. Updated appendix to clarify that depending on the deployment use case, ACME server policy may conform to CA/Browser Forum Baselines, but subdomain certificates may be used in multiple other scenarios where CAB compliance is not required

Next steps

- Missing security considerations
- Adoption?

draft-ietf-acme-integrations

Friel, Barnes	Cisco
Shekh-Yusef	Auth0
Richardson	Sandelman Software Works

TL;DR

- Describes how ACME RFC 8555 can be integrated with multiple existing client / device certificate enrolment mechanisms without requiring any changes to ACME

Multiple Client / Device Integration Use Cases

1. EST
   - RFC 7030: Enrollment over Secure Transport
2. BRSKI
   - draft-ietf-anima-bootstrapping-keyinfra: Bootstrapping Remote Key Infrastructures
3. BRSKI Cloud Registrar
   - draft-friel-anima-brski-cloud: Specifies BRSKI behaviour with default cloud registrar
4. TEAP (with Updates)
   - RFC 7170 and draft-lear-eap-teap-brski : Tunnel Extensible Authentication Protocol

What has changed since IETF 106

- TEAP and TEAP-BRSKI sections collapsed into single section “ACME Integration with TEAP” section
- Baseline TEAP (RFC 7170) is missing some important certificate enrolment capabilities that are introduced in draft-lear-eap-teap-brski
  - CSR Attributes TLV: Allows a server to tell a client what list of attributes to include in the CSR request, similar to EST (RFC 7030)
  - Retry-After TLV: Allows a server to indicate to a client that the CSR request has been accepted for processing but a response is not yet available, similar to EST /simpleenroll 202 response code

Todo: Security Considerations

- No changes to referenced specification security considerations
  - EST (RFC 7030)
  - BRSKI (draft-ietf-anima-bootstrapping-keyinfra)
  - TEAP (RFC 7170)
- Security considerations still not reviewed and / or complete for
  - draft-lear-eap-teap-brski
  - draft-friel-anima-brski-cloud
- As this document is informational and does not change any of the referenced specifications, we expect the security considerations to be a summary of the referenced documents

Next Steps

- Reviewers please
- Feedback please

ACME for v3 Onion addresses draft

- Addresses are encoded ed25519 public keys
- Adds a new identifier type, “onion-v3”
- Adds a new challenge, “onion-v3-csr”
  - Server provides a nonce, client provides a nonce, client encodes nonces in a CSR extension and signs the CSR with the service private key. Server verifies key encoded in address verifies CSR.
- Doesn’t specify http-01 usage

Open questions

- Do we want to add a more straightforward version of the CSR challenge?
  - One solution would be to just sign over a single server provided nonce
- Do we want to specify usage with http-01?