Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 14, 2019

O. Friel
R. Barnes
Cisco

May 13, 2019

ACME Integrations
draft-friel-acme-integrations-00

Abstract

This document outlines multiple advanced use cases and integrations that ACME facilitates without any modifications or enhancements required to the base ACME specification. These use cases are not immediately obvious from reading the ACME specification and thus are explicitly documented here. The use cases include ACME issuance of subdomain certificates, and ACME integration with EST and TEAP.

Table of Contents

1. Introduction

ACME [RFC8555] defines a protocol that a certificate authority (CA) and an applicant can use to automate the process of domain name ownership validation and X.509 (PKIX) certificate issuance. The protocol is rich and flexible and enables multiple use cases that are not immediately obvious from reading the specification. This document explicitly outlines multiple advanced ACME use cases including:

- ACME issuance of subdomain certificates
- ACME integration with EST [RFC7030]
- ACME integration with BRSKI [I-D.ietf-anima-bootstrapping-keyinfra]
- ACME integration with TEAP [RFC7170]
- ACME integration with TEAP-BRSKI draft-lear-eap-teap-brski

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and

"OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are used in this document:

- o BRSKI: Bootstrapping Remote Secure Key Infrastructures [I-D.ietf-anima-bootstrapping-keyinfra]
- o CA: Certificate Authority
- o CMC: Certificate Management over CMS
- o CSR: Certificate Signing Request
- o EST: Enrollment over Secure Transport [RFC7030]
- o FQDN: Fully Qualified Domain Name
- o RA: PKI Registration Authority
- o TEAP: Tunneled Extensible Authentication Protocol [RFC7170]

3. ACME Issuance of Subdomain Certificates

A typical ACME workflow for issuance of certificates is as follows:

1. client POSTs a newOrder request that contains a set of "identifiers"

2. server replies with a set of "authorizations" and a "finalize" URI

3. client sends POST-as-GET requests to retrieve the "authorizations", with the downloaded "authorization" object(s) containing the "identifier" that the client must prove control of

4. client proves control over the "identifier" in the "authorization" object by completing the specified challenge, for example, by pubilshing a DNS TXT record

5. client POSTs a CSR to the "finalize" API

ACME places the following restrictions on "identifiers":

o section 7.1.4: the only type of "identifier" defined by the ACME specification is a fully qualified domain name

The only type of identifier defined by this specification is a fully qualified

o Section 7.4: the "identifier" in the CSR request must match the "identifier" in the newOrder request

The CSR MUST indicate the exact same set of requested identifiers as the initia

o Sections 8.3 and 8.4: the "identifier", or FQDN, in the "authorization" object must be used when fulfilling challenges via HTTP or DNS mechanisms

Construct a URL by populating the URL template [RFC6570] "http://{domain}/.well-known/acme-challenge/{token}", where:

* the domain field is set to the domain name being verified

The client constructs the validation domain name by prepending the label "_acme-challenge" to the domain name being validated

ACME does not mandate that the "identifier" in a newOrder request matches the "identifier" in "authorization" objects. This means that the ACME specification does not preclude an ACME server processing newOrder requests and issuing certificates for a subdomain without requiring a challenge to be fulfilled against that explicit subdomain. ACME server policy could allow issuance of certificates for a subdomain to a client where the client only has to fulfill an authorization challenge for the parent domain.

This allows a flow where a client proves ownership of "domain.com" and then successfully obtains a certificate for "sub.domain.com". The ACME pre-authorization flow makes most sense for this use case, and that is what is illustrated in the following call flow.

The client could pre-authorize for the parent domain once, and then issue multiple newOrder requests for certificates for multiple subdomains. This call flow illustrates the client only placing one newOrder request.

```
   +---------+            +-------+    +------+
   | Client  |            | ACME  |    | DNS  |
   +---------+            +-------+    +------+
       |                      |           |
    STEP 1: Pre-Authorization of parent domain
       |                      |           |
       | POST /newAuthz       |           |
       |  "domain.com"        |           |
       |--------------------->|           |
       |                      |           |
       | 201 authorizations   |           |
       |<---------------------|           |
       |                      |           |
       | Publish DNS TXT      |           |
       | "domain.com"         |           |
       |--------------------------------->|
```



```
       |                      |           |
       | POST /challenge      |           |
       |--------------------->|           |
       |                      | Verify    |
       |                      |---------->|
       | 200 status=valid     |           |
       |<---------------------|           |
       |                      |           |
       | Delete DNS TXT       |           |
       | "domain.com"         |           |
       |--------------------------------->|
       |                      |           |
    STEP 2: Place order for subdomain
       |                      |           |
       | POST /newOrder       |           |
       | "sub.domain.com"     |           |
       |--------------------->|           |
       |                      |           |
       | 201 status=ready     |           |
       |<---------------------|           |
       |                      |           |
       | POST /finalize       |           |
```

```
     | CSR "sub.domain.com" |           |
     |--------------------->|           |
     |                      |           |
     | 200 OK status=valid  |           |
     |<---------------------|           |
     |                      |           |
     | POST /certificate    |           |
     |--------------------->|           |
     |                      |           |
     | 200 OK               |           |
     | PKI "sub.domain.com" |           |
     |<---------------------|           |
```

4. ACME Integration with EST

EST [RFC7030] defines a mechanism for clients to enroll with a PKI Registration Authority by sending CMC messages over HTTP. EST section 1 states:

Architecturally, the EST service is located between a Certification Authority (

EST section 1.1 states that:

For certificate issuing services, the EST CA is reached through the EST server;

When the CA is logically "behind" the EST RA, EST does not specify how the RA communicates with the CA. EST section 1 states:

The nature of communication between an EST server and a CA is not described in

This section outlines how ACME could be used for communication between the EST RA and the CA. The example call flow shows the RA proving ownership of a parent domain, with individual client certificates being subdomains under that parent domain. This is an optimisation that reduces DNS and ACME traffic overhead. The RA could of course prove ownership of every explicit client certificate identifier.

The call flow also illustrates how the RA can include relevant domain information in the CSR request to ACME that the client may not have knowledge of. For example, a device or pledge may know its MAC address and serial number and only include that as its identifier in a CSR request. The RA could insert the domain information into the CSR request. Additionally, for privacy reasons, the RA may not want to divulge MAC or serial number information to the CA and could additionally assign an opaque random identifier to the device.

```
+---------+            +---------+            +-------+    +------+
| Pledge |             | EST RA |             | ACME |     | DNS |
+---------+            +---------+            +-------+    +------+
    |                      |                      |           |
               STEP 1: Pre-Authorization of parent domain
    |                      |                      |           |
    |                      | POST /newAuthz       |           |
    |                      |  "domain.com"        |           |
    |                      |--------------------->|           |
    |                      |                      |           |
    |                      | 201 authorizations   |           |
    |                      |<---------------------|           |
    |                      |                      |           |
    |                      | Publish DNS TXT      |           |
    |                      | "domain.com"         |           |
    |                      |---------------------------------->|
    |                      |                      |           |
    |                      | POST /challenge      |           |
    |                      |--------------------->|           |
    |                      |                      | Verify    |
    |                      |                      |---------->|
    |                      | 200 status=valid     |           |
    |                      |<---------------------|           |
    |                      |                      |           |
    |                      | Delete DNS TXT       |           |
    |                      | "domain.com"         |           |
```



```
    |                      |---------------------------------->|
    |                      |                      |           |
               STEP 2: Pledge enrolls against RA
    |                      |                      |           |
    | POST /simpleenroll   |                      |           |
    | PCSK#10 "MAC/serial" |                      |           |
    |--------------------->|                      |           |
    |                      |                      |           |
```

```
       | 202 Retry-After      |                      |           |
       |<---------------------|                      |           |
       |                      |                      |           |
                  STEP 3: RA places ACME order
       |                      |                      |           |
       |                      | POST /newOrder       |           |
       |                      | "pledgeX.domain.com" |           |
       |                      |--------------------->|           |
       |                      |                      |           |
       |                      | 201 status=ready     |           |
       |                      |<---------------------|           |
       |                      |                      |           |
       |                      | POST /finalize       |           |
       |                      | CSR "pledgeX.domain.com"         |
       |                      |--------------------->|           |
       |                      |                      |           |
       |                      | 200 OK status=valid  |           |
       |                      |<---------------------|           |
       |                      |                      |           |
       |                      | POST /certificate    |           |
       |                      |--------------------->|           |
       |                      |                      |           |
       |                      | 200 OK               |           |
       |                      | PKI "pledgeX.domain.com"         |
       |                      |<---------------------|           |
       |                      |                      |           |
                  STEP 4: Pledge retries enroll
       |                      |                      |           |
       | POST /simpleenroll   |                      |           |
       | PCSK#10 "MAC/serial" |                      |           |
       |--------------------->|                      |           |
       |                      |                      |           |
       | 200 OK               |
       | PKCS#7 "pledgeX.domain.com"                 |           |
       |<---------------------|                      |           |
```


5. ACME Integration with BRSKI

BRSKI [I-D.ietf-anima-bootstrapping-keyinfra] is based upon EST [RFC7030] and defines how to autonomically bootstrap PKI trust anchors into devices via means of signed vouchers. EST certificate enrollment may then optionally take place after trust has been established. BRKSI voucher exchange and trust establishment are based on EST extensions and the certicicate enrollment part of BRSKI is fully based on EST. Similar to EST, BRSKI does not define how the EST RA communicates with the CA. Therefore the mechanisms outlined in the previous section for using ACME as the communications protocol between the EST RA and the CA are equally applicable to BRSKI.

The following call flow shows how ACME may be integated into a full BRSKI voucher plus EST enrollment workflow. For brevity, it assumes that the EST RA has previously proven ownership of a parent domain and that pledge certificate identifiers are a subdomain of that parent domain. The doain owernship excahnges between the RA, ACME and DNS are not shown. Similarly, not all BRSKI interactions are shown and only the key protocol flows involving voucher exchange and EST enrollment are shown.

```
   +--------+             +--------+             +------+     +------+
   | Pledge |             | EST RA |             | ACME |     | MASA |
   +--------+             +--------+             +------+     +------+
       |                      |                      |           |
                  NOTE: Pre-Authorization of "domain.com" is complete
       |                      |                      |           |
                  STEP 1: Pledge requests Voucher
       |                      |                      |           |
       | POST /requestvoucher |                      |           |
       |--------------------->|                      |           |
       |                      | POST /requestvoucher |           |
       |                      |--------------------------------->|
       |                      |                      |           |
       |                      | 200 OK Voucher       |           |
       |                      |<---------------------------------|
       | 200 OK Voucher       |                      |           |
       |<---------------------|                      |           |
       |                      |                      |           |
                  STEP 2: Pledge enrolls against RA
       |                      |                      |           |
       | POST /simpleenroll   |                      |           |
       | PCSK#10 "MAC/serial" |                      |           |
       |--------------------->|                      |           |
       |                      |                      |           |
       | 202 Retry-After      |                      |           |
       |<---------------------|                      |           |
```

```
       |                      |                      |           |
                  STEP 3: RA places ACME order
       |                      |                      |           |
       |                      | POST /newOrder       |           |
       |                      | "pledgeX.domain.com" |           |
       |                      |---------------------->|           |
       |                      |                      |           |
       |                      | 201 status=ready     |           |
       |                      |<---------------------|           |
       |                      |                      |           |
       |                      | POST /finalize       |           |
       |                      | CSR "pledgeX.domain.com"         |
       |                      |---------------------->|           |
       |                      |                      |           |
       |                      | 200 OK status=valid  |           |
       |                      |<---------------------|           |
       |                      |                      |           |
       |                      | POST /certificate    |           |
       |                      |---------------------->|           |
       |                      |                      |           |
       |                      | 200 OK               |           |
       |                      | PKI "pledgeX.domain.com"         |
       |                      |<---------------------|           |
       |                      |                      |           |
                  STEP 4: Pledge retries enroll
       |                      |                      |           |
       | POST /simpleenroll   |                      |           |
       | PCSK#10 "MAC/serial" |                      |           |
       |---------------------->|                      |           |
       |                      |                      |           |
       | 200 OK               |
       | PKCS#7 "pledgeX.domain.com"                 |           |
       |<---------------------|                      |           |
```

6. ACME Integration with TEAP

TEAP [RFC7170] define a tunnel-based EAP method that enables secure communication between a peer and a server by using TLS to establish a mutually authenticated tunnel. TEAP enables certificate provisioning within the tunnel. TEAP does not define how the TEAP server communicates with the CA.

This section outlines how ACME could be used for communication between the TEAP server and the CA. The example call flow shows the TEAP server proving ownership of a parent domain, with individual client certificates being subdomains under that parent domain. This is an optimisation that reduces DNS and ACME traffic overhead. The

   TEAP server could of course prove ownership of every explicit client
   certificate identifier.

```
   +--------+             +-------------+          +------+    +-----+
   | Pledge |             | TEAP-Server |          | ACME |    | DNS |
   +--------+             +-------------+          +------+    +-----+
       |                         |                      |           |
                  STEP 1: Pre-Authorization of parent domain
       |                         |                      |           |
       |                         | POST /newAuthz       |           |
       |                         |  "domain.com"        |           |
       |                         |--------------------->|           |
       |                         |                      |           |
       |                         | 201 authorizations   |           |
       |                         |<---------------------|           |
       |                         |                      |           |
       |                         | Publish DNS TXT      |           |
       |                         | "domain.com"         |           |
       |                         |--------------------------------->|
       |                         |                      |           |
       |                         | POST /challenge      |           |
       |                         |--------------------->|           |
       |                         |                      | Verify    |
       |                         |                      |---------->|
       |                         | 200 status=valid     |           |
       |                         |<---------------------|           |
       |                         |                      |           |
       |                         | Delete DNS TXT       |           |
       |                         | "domain.com"         |           |
       |                         |--------------------------------->|
       |                         |                      |           |
       |                         |                      |           |
                  STEP 2: Establsh EAP Outer Tunnel
       |                         |                      |           |
       |  EAP-Request/           |                      |           |
       |   Type=Identity         |                      |           |
       |<------------------------|                      |           |
       |                         |                      |           |
       |  EAP-Response/          |                      |           |
```

```
       |   Type=Identity         |                      |           |
       |------------------------>|                      |           |
       |                         |                      |           |
       |  EAP-Request/           |                      |           |
       |   Type=TEAP,            |                      |           |
       |   TEAP Start,           |                      |           |
       |   Authority-ID TLV      |                      |           |
       |<------------------------|                      |           |
       |                         |                      |           |
```



```
       |  EAP-Response/          |                      |           |
       |   Type=TEAP,            |                      |           |
       |   TLS(ClientHello)      |                      |           |
       |------------------------>|                      |           |
       |                         |                      |           |
       |  EAP-Request/           |                      |           |
       |   Type=TEAP,            |                      |           |
       |   TLS(ServerHello,      |                      |           |
       |   Certificate,          |                      |           |
       |   ServerKeyExchange,    |                      |           |
       |   CertificateRequest,   |                      |           |
       |   ServerHelloDone)      |                      |           |
       |<------------------------|                      |           |
       |                         |                      |           |
       |  EAP-Response/          |                      |           |
       |   Type=TEAP,            |                      |           |
       |   TLS(Certificate,      |                      |           |
       |   ClientKeyExchange,    |                      |           |
       |   CertificateVerify,    |                      |           |
       |   ChangeCipherSpec,     |                      |           |
       |   Finished)             |                      |           |
       |------------------------>|                      |           |
       |                         |                      |           |
       |  EAP-Request/           |                      |           |
       |   Type=TEAP,            |                      |           |
       |   TLS(ChangeCipherSpec, |                      |           |
       |   Finished),            |                      |           |
       |   {Crypto-Binding TLV,  |                      |           |
       |   Result TLV=Success}   |                      |           |
       |<------------------------|                      |           |
       |                         |                      |           |
       |  EAP-Response/          |                      |           |
```

```
        |  Type=TEAP,             |                      |           |
        |  {Crypto-Binding TLV,   |                      |           |
        |  Result TLV=Success}    |                      |           |
        |------------------------>|                      |           |
        |                         |                      |           |
        | EAP-Request/            |                      |           |
        |  Type=TEAP,             |                      |           |
        |  {Request-Action TLV:   |                      |           |
        |    Status=Failure,      |                      |           |
        |    Action=Process-TLV,  |                      |           |
        |    TLV=PKCS#10}         |                      |           |
        |<------------------------|                      |           |
        |                         |                      |           |
                  STEP 3: Enroll for certificate
        |                         |                      |           |
        | EAP-Response/           |                      |           |
```



```
        |  Type=TEAP,             |                      |           |
        |  {PKCS#10 TLV:          |                      |           |
        |  SAN:"MAC/serial"}      |                      |           |
        |------------------------>|                      |           |
        |                         | POST /newOrder       |           |
        |                         | "pledgeX.domain.com" |           |
        |                         |--------------------->|           |
        |                         |                      |           |
        |                         | 201 status=ready     |           |
        |                         |<---------------------|           |
        |                         |                      |           |
        |                         | POST /finalize       |           |
        |                         | CSR "pledgeX.domain.com"         |
        |                         |--------------------->|           |
        |                         |                      |           |
        |                         | 200 OK status=valid  |           |
        |                         |<---------------------|           |
        |                         |                      |           |
        |                         | POST /certificate    |           |
        |                         |--------------------->|           |
        |                         |                      |           |
        |                         | 200 OK               |           |
        |                         | PKI "pledgeX.domain.com"         |
        |                         |<---------------------|           |
        |                         |                      |           |
```

```
|   EAP-Request/          |                       |           |
|    Type=TEAP,           |                       |           |
|    {PKCS#7 TLV,         |                       |           |
|     Result TLV=Success} |                       |           |
|<------------------------|                       |           |
|                         |                       |           |
|   EAP-Response/         |                       |           |
|    Type=TEAP,           |                       |           |
|    {Result TLV=Success} |                       |           |
|------------------------>|                       |           |
|                         |                       |           |
|   EAP-Success           |                       |           |
|<------------------------|                       |           |
```

7. ACME Integration with TEAP-BRSKI

TEAP-BRSKI draft-lear-eap-teap-brski defines... and its very similar to the TEAP proposal in the prevous section.

8. IANA Considerations

[todo]

9. Security Considerations

[todo]

10. Informative References

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-20 (work in progress), May 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,

DOI 10.17487/RFC2119, March 1997,
<https://www.rfc-editor.org/info/rfc2119>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", RFC 7170, DOI 10.17487/RFC7170, May 2014, <https://www.rfc-editor.org/info/rfc7170>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

Appendix A. Comments

Authors' Addresses

Owen Friel
Cisco

Email: ofriel@cisco.com

Richard Barnes
Cisco

Email: rlb@ipv.sx