Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 14 January 2024

O. Friel
R. Barnes
Cisco
R. Shekh-Yusef
Ernst & Young
M. Richardson
Sandelman Software Works
13 July 2023

ACME Integrations for Device Certificate Enrollment
draft-ietf-acme-integrations-17

Abstract

This document outlines multiple advanced use cases and integrations that ACME facilitates without any modifications or enhancements required to the base ACME specification. The use cases include ACME integration with EST, BRSKI and TEAP.

Table of Contents

1. Introduction

ACME [RFC8555] defines a protocol that a certification authority (CA) and an applicant can use to automate the process of domain name ownership validation and X.509 (PKIX) [RFC5280] 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 integration with EST [RFC7030]

* ACME integration with BRSKI [RFC8995]

* ACME integration with BRSKI Default Cloud Registrar [I-D.ietf-anima-brski-cloud]

* ACME integration with TEAP [RFC7170]

The integrations with EST, BRSKI (which is based upon EST), and TEAP enable automated certificate enrollment for devices.

Optionally, ACME for subdomains [I-D.ietf-acme-subdomains] offers a useful optimization when ACME is used to issue certificates for large numbers of devices in the same domain; it reduces the domain ownership proof traffic as well as the ACME traffic overhead. This is accomplished by completing a challenge against the parent domain instead of a challenge against each explicit subdomain. Use of ACME for subdomains is not a requirement.

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 defined in DNS Terminology [RFC8499], Section 2 and used in this document. Please refer to [RFC8499], Section 2 for a definition of these terms.

* Label

* Domain Name

* Subdomain

* Fully-Qualified Domain Name (FQDN)

The following terms are used in this document:

* BRSKI: Bootstrapping Remote Secure Key Infrastructures [RFC8995]

* Pledge: from [RFC8366], the prospective device attempting to find and securely join a domain. When shipped, it only trusts authorized representatives of the manufacturer.

* Certification Authority (CA): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs

* CMS: Cryptographic Message Syntax [RFC5652]

* CMC: Certificate Management over CMS [RFC5272]

* CSR: Certificate Signing Request [RFC2986]

* EST: Enrollment over Secure Transport [RFC7030]

* MASA: Manufacturer Authorized Signing Authority as defined in [RFC8995]

* PKCS: Public-Key Cryptography Standards [RFC8017]

* PKCS#7: PKCS Cryptographic Message Syntax [RFC2315]

* PKCS#10: PKCS Certification Request Syntax [RFC2986]

* RA: PKI Registration Authority [RFC2986]

* TEAP: Tunneled Extensible Authentication Protocol [RFC7170]

* TLV: Type-Length-Value format defined in TEAP [RFC7170]

3. Pre-requisites for Integration

In order for the EST server or TEAP server that is part of the BRSKI Registrar to use ACME to create new certificates it needs to have the ability to satisfy the dns-01 challenges that the ACME will issue.

The EST Registration Authority (RA) is configured with the DNS domain for which it will issue certificates. In the examples below, it is "example.com"

The EST RA is configured with a credential that allows it to update the contents of the DNS domain. This could be in the form of an [RFC3007] credential such as a TSIG key or a SIG(0) key. It could also be some other proprietary credential that allows the EST RA to update the database on the DNS provider directly. As a third option, the EST RA could maintain a zone itself, configured as a stealth primary, with a DNS NS zone cut pointing at the EST RA's DNS server.

4. ACME Integration with EST

EST [RFC7030] defines a mechanism for clients to enroll with a PKI Registration Authority by sending Certificate Management over CMS (CMC) [RFC5272] messages over HTTP. EST [RFC7030] Section 1 states:

"Architecturally, the EST service is located between a Certification Authority (CA) and a client. It performs several functions traditionally allocated to the Registration Authority (RA) role in a PKI."

EST [RFC7030] Section 1.1 states that:

"For certificate issuing services, the EST CA is reached through the EST server; the CA could be logically "behind" the EST server or embedded within it."

When the CA is logically "behind" the EST RA, EST does not specify how the RA communicates with the CA. EST [RFC7030] Section 1 states:

"The nature of communication between an EST server and a CA is not described in this document."

This section outlines how ACME could be used for communication between the EST RA and the CA. The example call flow leverages [I-D.ietf-acme-subdomains] and shows the RA proving ownership of a parent domain using the 'dns-01' challenge type, with individual client certificates being subdomains under that parent domain. ACME [RFC8555], Section 8.4 defines how the ACME client, which in this example is the EST RA, and ACME server interact with the DNS system. Please refer to ACME [RFC8555] for details on all relevant DNS operations.

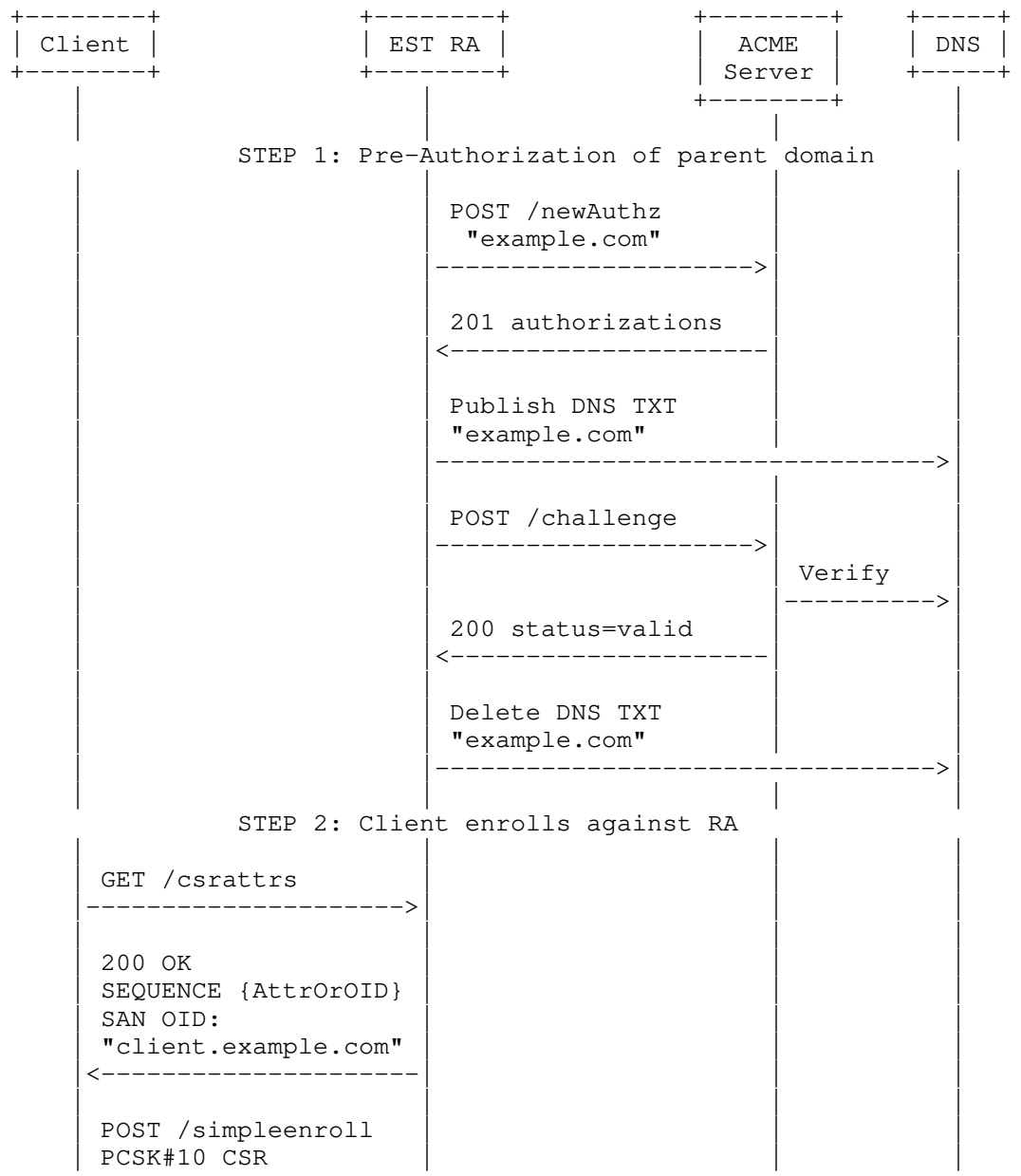
Use of [I-D.ietf-acme-subdomains] is an optional optimization that reduces DNS and ACME traffic overhead. The RA could of course prove ownership of every explicit client certificate identifier.

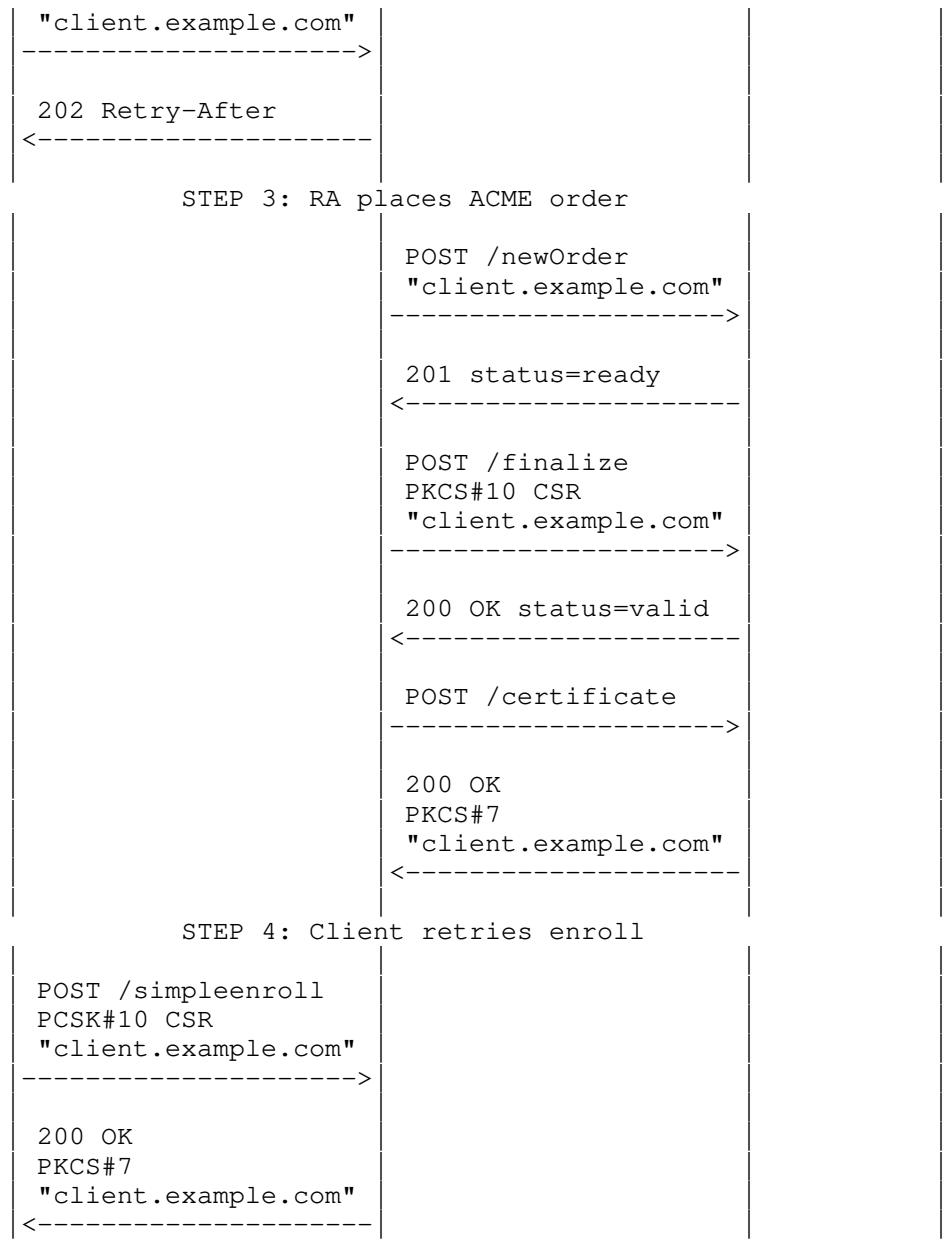
The call flow illustrates the client calling the EST /csrattrs API before calling the EST /simpleenroll API. This enables the server to indicate what fields the client should include in the CSR that the client sends in the /simpleenroll API. CSR Attributes handling are discussed in Section 8.2.

If the CSR includes an identifier that the EST RA does not control, the RA MUST respond with a 4xx HTTP [RFC9110] error code. Refer to section Section 8.5 for further details on error handling.

The call flow illustrates the EST RA returning a 202 Retry-After response to the client's simpleenroll request. This is an optional step and may be necessary if the interactions between the RA and the ACME server take some time to complete. The exact details of when the RA returns a 202 Retry-After are implementation specific.

This example illustrates, and all subsequent examples in this document illustrate, the use of the ACME 'dns-01' challenge type. This does not preclude the use of any other ACME challenges, however, examples illustrating the use of other challenge types are not documented here.




"client.example.com"
202 Retry-After
STEP 3: RA places ACME order
POST /newOrder
"client.example.com"
201 status=ready
POST /finalize
PKCS#10 CSR
"client.example.com"
200 OK status=valid
POST /certificate
200 OK
PKCS#7
"client.example.com"
STEP 4: Client retries enroll
POST /simpleenroll
PCSK#10 CSR
"client.example.com"
200 OK
PKCS#7
"client.example.com"

5. ACME Integration with BRSKI

BRSKI [RFC8995] is based upon EST [RFC7030] and defines how to autonomically bootstrap PKI trust anchors into devices via means of signed vouchers. The signed vouchers are issued by the Manufacturer Authorized Signing Authority (MASA) service as described in BRSKI.

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 certificate 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 integrated into a full BRSKI voucher plus EST enrollment workflow. For brevity, it assumes that the EST RA has previously proven ownership of the certificate identifier. This ownership proof could have been by fulfilling an authorization challenge against the explicit identifier "pledge.example.com", or by fulfilling an authorization challenge against the parent domain "example.com" leveraging [I-D.ietf-acme-subdomains].

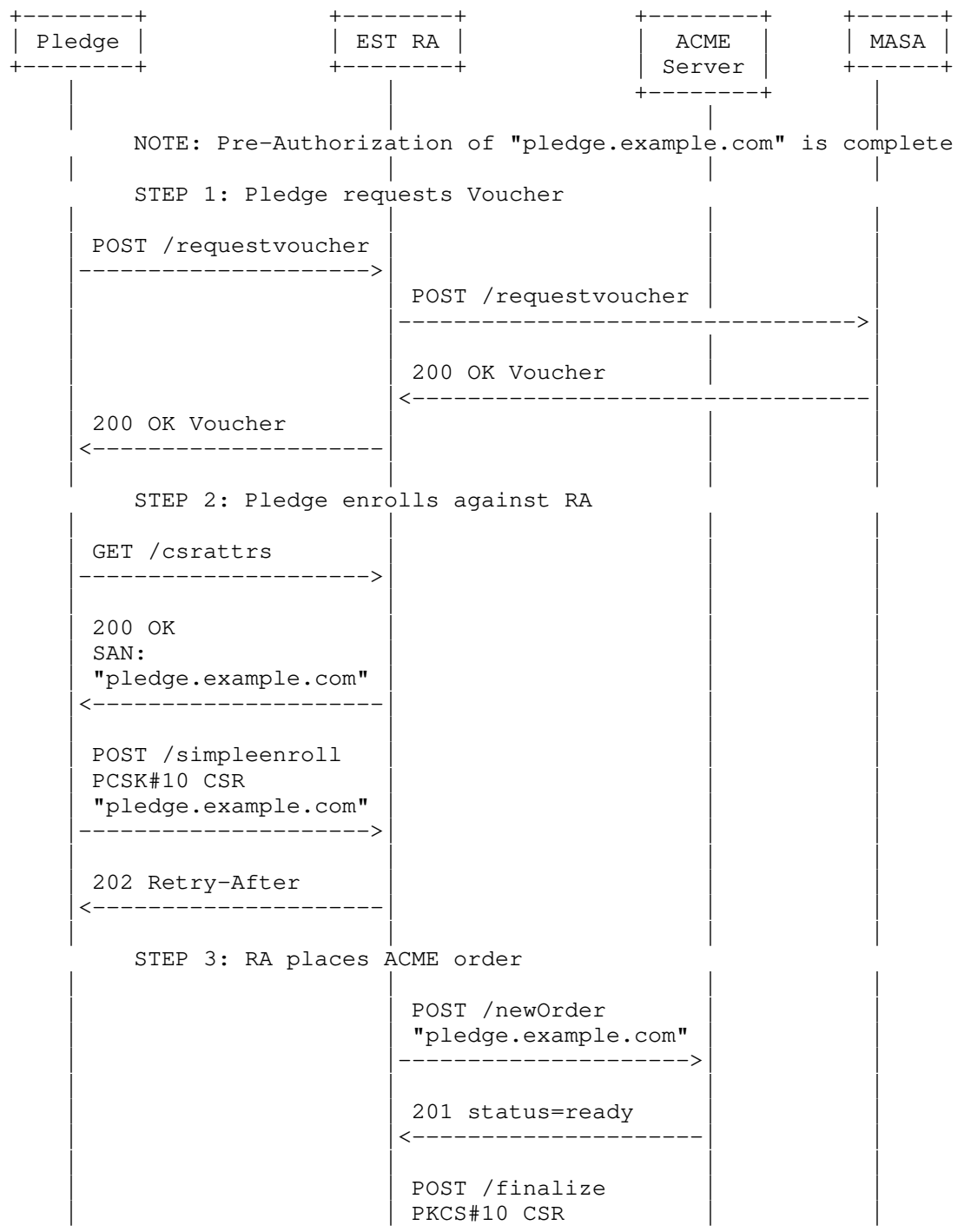
The domain ownership exchanges between the RA, ACME and DNS are not shown. Similarly, not all BRSKI interactions are shown and only the key protocol flows involving voucher exchange and EST enrollment are shown.

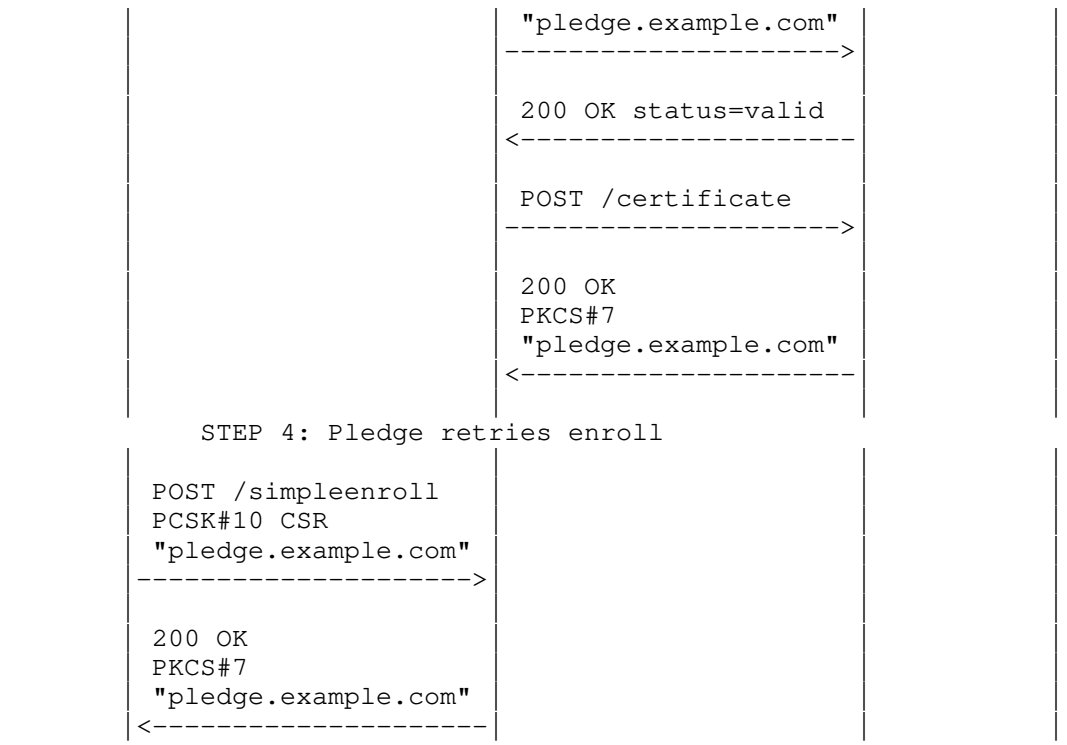
Similar to the EST section above, the client calls EST /csrattrs API before calling the EST /simpleenroll API. This enables the server to indicate what fields the pledge should include in the CSR that the client sends in the /simpleenroll API. Refer to section Section 8.2 for more details.

If the CSR includes an identifier that the EST RA does not control, the RA MUST respond with a 4xx HTTP [RFC9110] error code. Refer to section Section 8.5 for further details on error handling.

The call flow illustrates the RA returning a 202 Retry-After response to the initial EST /simpleenroll API. This may be appropriate if processing of the /simpleenroll request and ACME interactions takes some time to complete.

This example illustrates the use of the ACME ’dns-01’ challenge type.


Pledge
EST RA
ACME Server
MASA
NOTE: Pre-Authorization of "pledge.example.com" is complete
STEP 1: Pledge requests Voucher
POST /requestvoucher
POST /requestvoucher
200 OK Voucher
200 OK Voucher
STEP 2: Pledge enrolls against RA
GET /csrattrs
200 OK
SAN:
"pledge.example.com"
POST /simpleenroll
PCSK#10 CSR
"pledge.example.com"
202 Retry-After
STEP 3: RA places ACME order
POST /newOrder
"pledge.example.com"
201 status=ready
POST /finalize
PKCS#10 CSR



6. ACME Integration with BRSKI Default Cloud Registrar

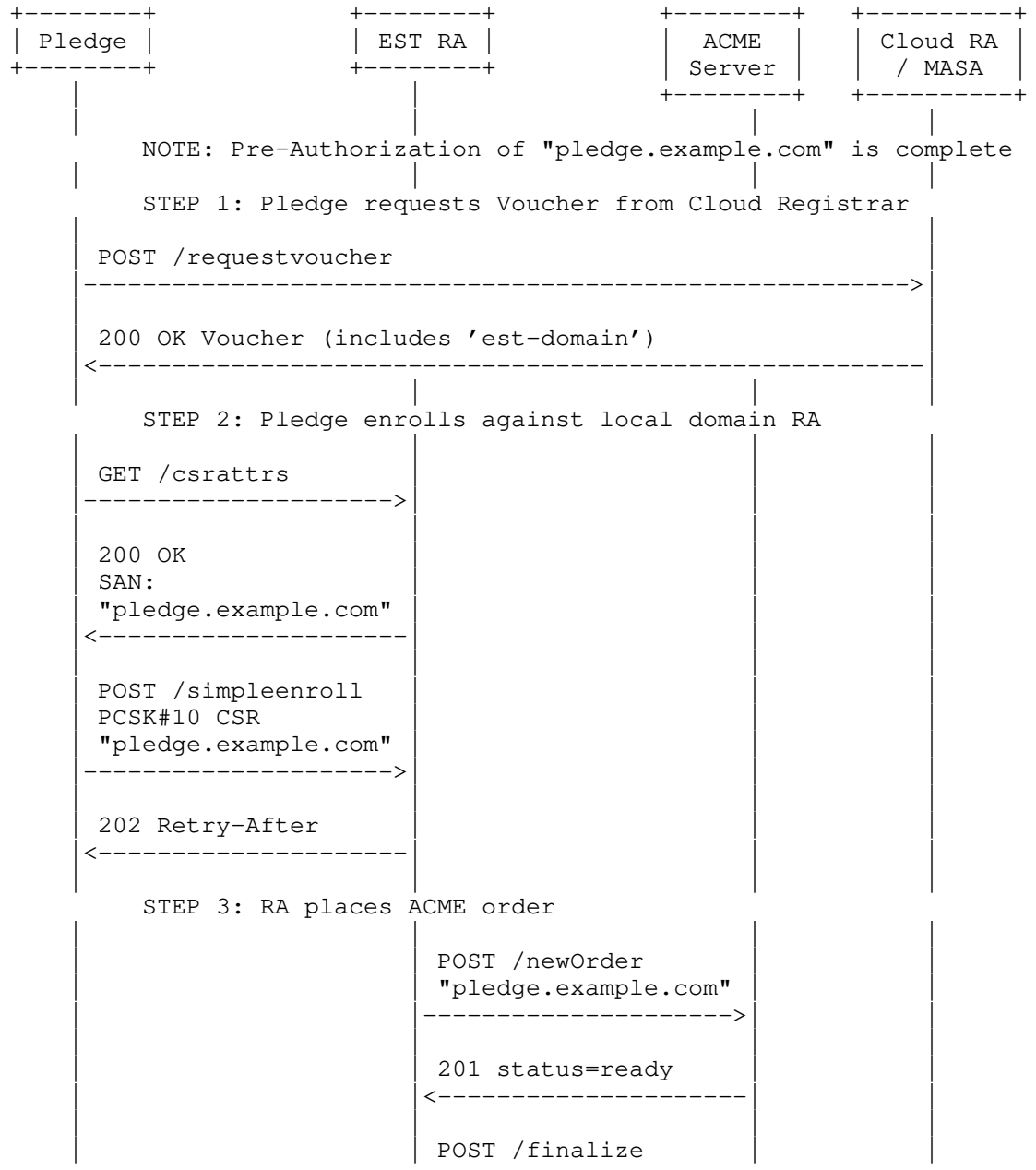
BRSKI Cloud Registrar [I-D.ietf-anima-brski-cloud] specifies the behavior of a BRSKI Cloud Registrar, and how a pledge can interact with a BRSKI Cloud Registrar when bootstrapping. Similar to the local domain registrar BRSKI flow, ACME can be easily integrated with a cloud registrar bootstrap flow.

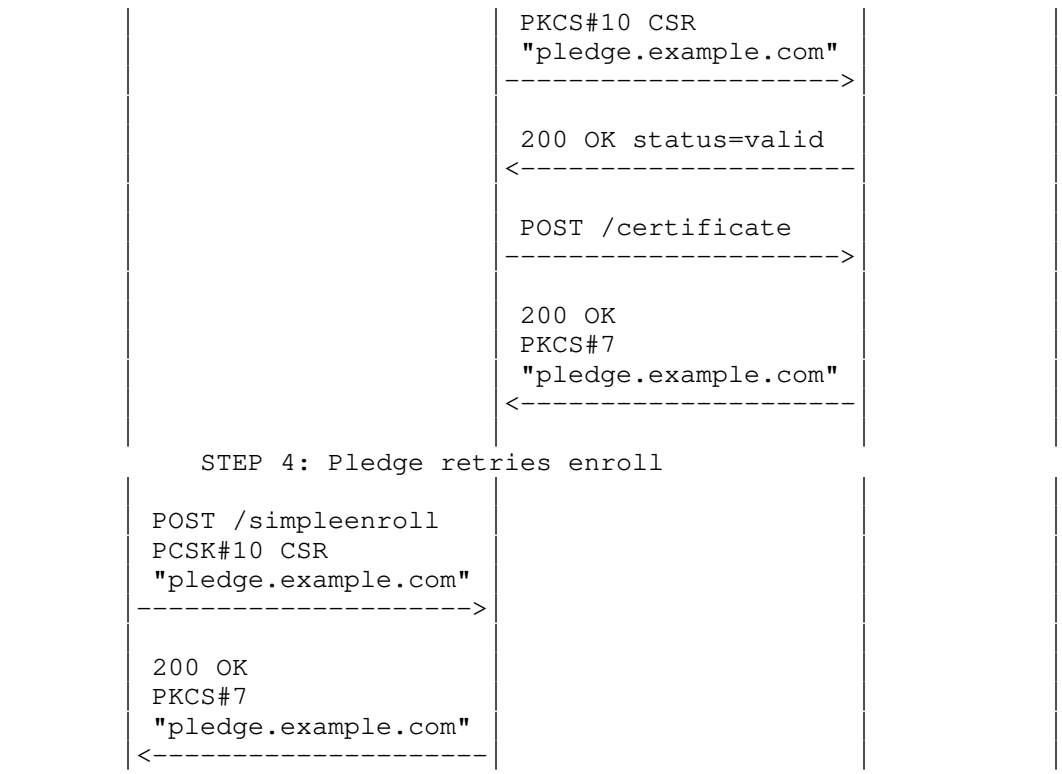
BRSKI cloud registrar is flexible and allows for multiple different local domain discovery and redirect scenarios. The est-domain leaf defined in [I-D.ietf-anima-brski-cloud] allows the specification of a bootstrap EST domain. In this example, the est-domain extension allows the cloud registrar to specify the local domain RA that the pledge should connect to for the purposes of EST enrollment.

For brevity, it assumes that the EST RA has previously proven ownership of the certificate identifier. This ownership proof could have been by fulfilling an authorization challenge against the explicit identifier "pledge.example.com", or by fulfilling an authorization challenge against the parent domain "example.com" leveraging [I-D.ietf-acme-subdomains]. The domain ownership exchanges between the RA, ACME and DNS are not shown.

Similar to the sections above, the client calls EST /csrattrs API before calling the EST /simpleenroll API.

This example illustrates the use of the ACME 'dns-01' challenge type.





7. ACME Integration with TEAP

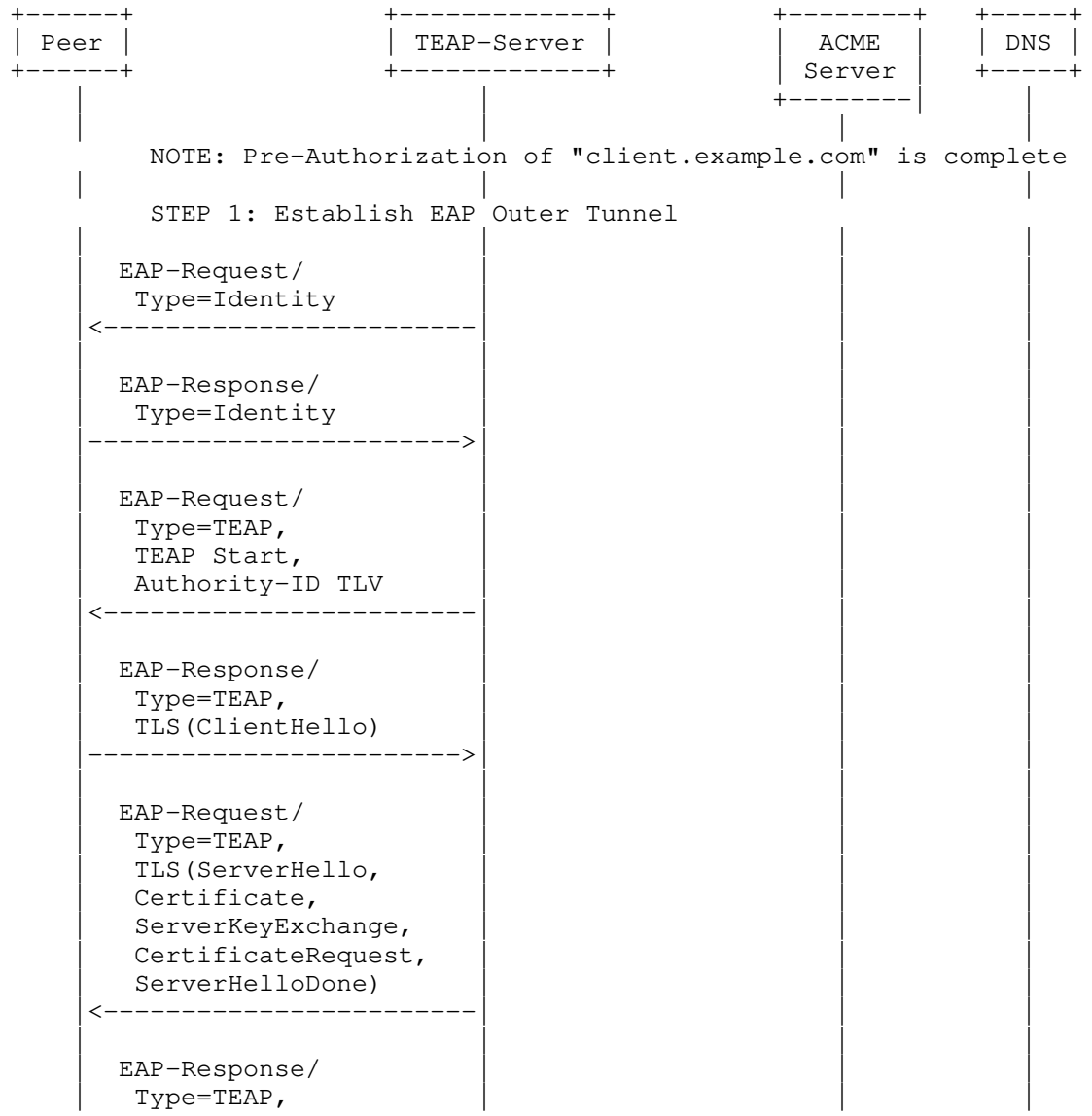
TEAP [RFC7170] defines a tunnel-based EAP method that enables secure communication between a peer and a server by using TLS to establish a mutually authenticated tunnel. TEAP enables certificate provisioning within the tunnel. TEAP [RFC7170] does not define how the TEAP server communicates with the CA.

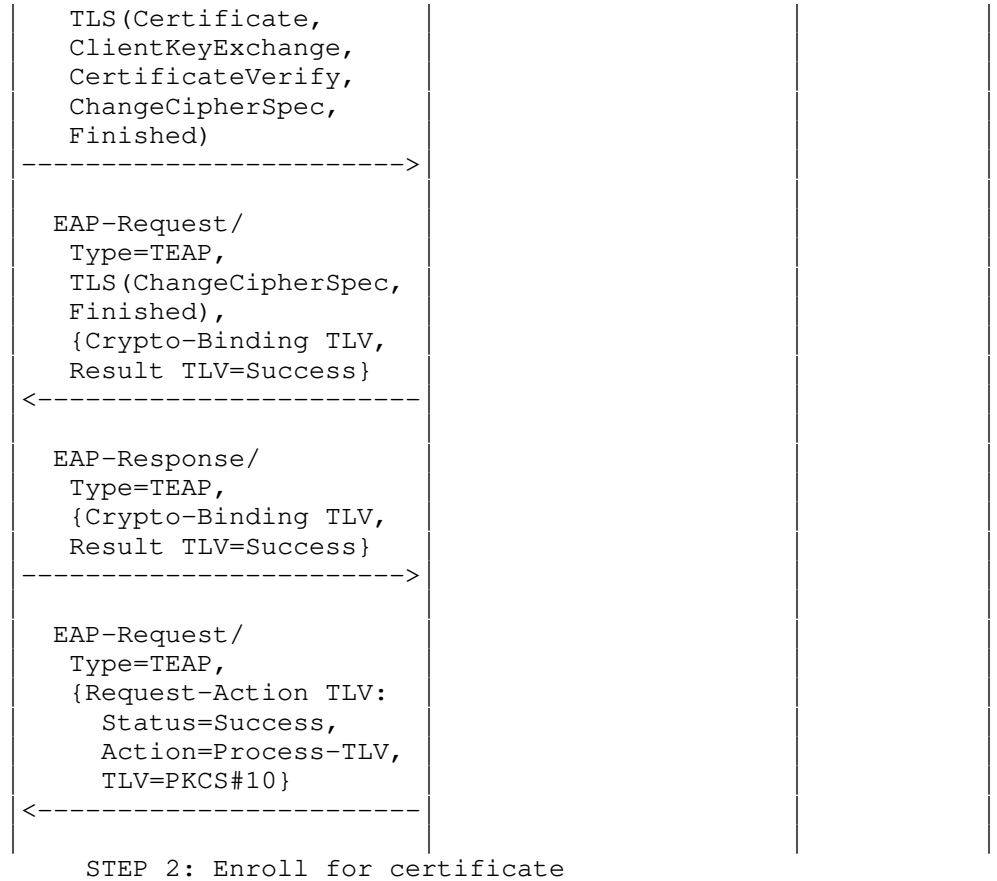
This section outlines how ACME could be used for communication between the TEAP server and the CA. The example call flow leverages [I-D.ietf-acme-subdomains] and shows the TEAP server proving ownership of a parent domain, with individual client certificates being subdomains under that parent domain.

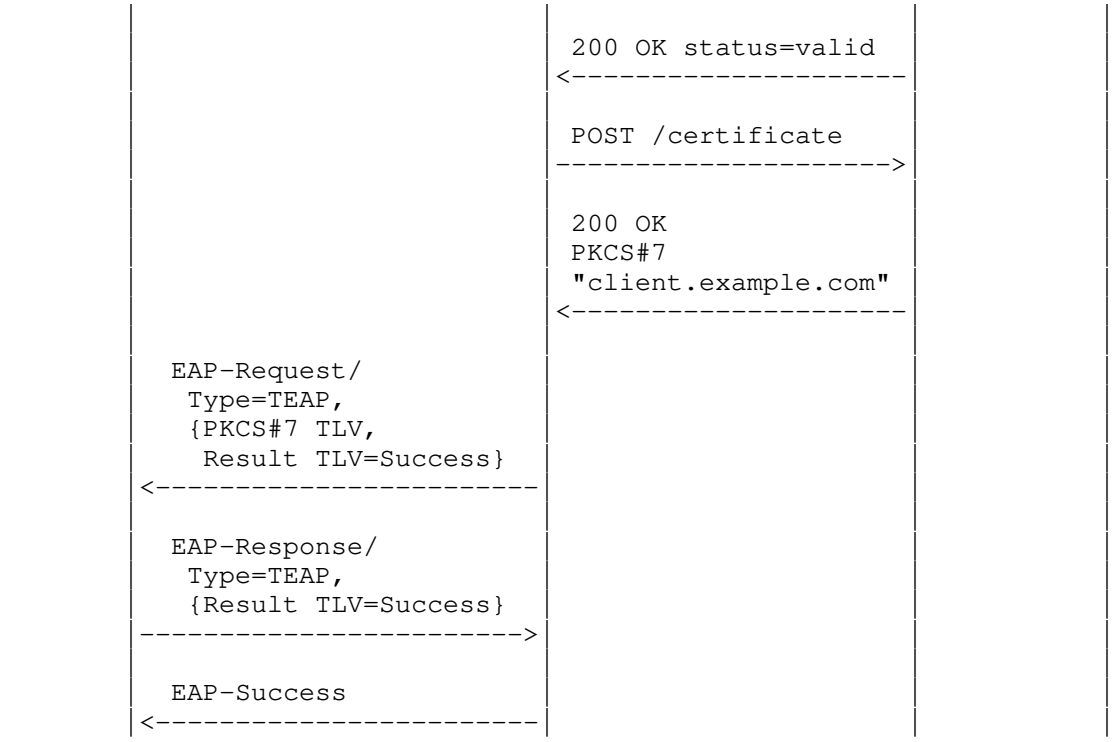
For brevity, it assumes that the TEAP server has previously proven ownership of the certificate identifier. This ownership proof could have been by fulfilling an authorization challenge against the explicit identifier "client.example.com", or by fulfilling an authorization challenge against the parent domain "example.com" leveraging [I-D.ietf-acme-subdomains]. The domain ownership exchanges between the TEAP server, ACME and DNS are not shown.

After establishing the outer TLS tunnel, the TEAP server instructs the client to enroll for a certificate by sending a PKCS#10 TLV in the body of a Request-Action TLV. The client then replies with a PKCS#10 TLV that contains its CSR. The TEAP server interacts with the ACME server for certificate issuance and returns the certificate in a PKCS#7 TLV as per TEAP [RFC7170].

This example illustrates the use of the ACME 'dns-01' challenge type.




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=Success,
Action=Process-TLV,
TLV=PKCS#10}
STEP 2: Enroll for certificate
EAP-Response/
Type=TEAP,
{PKCS#10 TLV:
"client.example.com"}
POST /newOrder
"client.example.com"
201 status=ready
POST /finalize
PKCS#10 CSR
"client.example.com"



8. ACME Integration Considerations

8.1. Service Operators

The goal of these integrations is enabling issuance of certificates with identifiers in a given domain by an ACME server to a client. The operator of the EST RA or TEAP server must be able to fulfil ACME challenges that prove domain ownership for issuance of certificates with identifiers in that domain. The ACME server is not necessarily operated by the organization that controls the domain.

If the client sends a certificate enrollment request for an identifier in a domain that the EST RA or TEAP server does not have operational control over, the server MUST reject the request with a suitable error immediately, and MUST NOT send a certificate enrollment request to the ACME server. See Section 8.5 for more information on error handling.

8.2. CSR Attributes

In all EST and BRSKI integrations, the client MUST send a CSR Attributes request to the EST server prior to sending a certificate enrollment request. This enables the server to indicate to the client what attributes, and what attribute values, it expects the client to include in the subsequent CSR request. For example, the server could instruct the peer what Subject Alternative Name entries to include in its CSR.

EST [RFC7030] is not clear on how the CSR Attributes response should be structured, and in particular is not clear on how a server can instruct a client to include specific attribute values in its CSR. [I-D.ietf-lamps-rfc7030-csrattrs] clarifies how a server can use CSR Attributes response to specify specific values for attributes that the client should include in its CSR.

Servers MUST use this mechanism to tell the client what identifiers to include in CSR request. ACME [RFC8555] allows the identifier to be included in either CSR Subject or Subject Alternative Name fields, however [I-D.ietf-uta-rfc6125bis] states that Subject Alternative Name field MUST be used. This document aligns with [I-D.ietf-uta-rfc6125bis] and Subject Alternate Name field MUST be used. The identifier MUST be a subdomain of a domain that the server has control over and can fulfill ACME challenges against. The leftmost part of the identifier MAY be a field that the client presented to the server in an IEEE 802.1AR [IDevID].

Servers MAY use this field to instruct the client to include other attributes such as specific policy OIDs. Refer to EST [RFC7030] Section 2.6 for further details.

8.3. Certificate Chains and Trust Anchors

ACME [RFC8555] Section 9.1 states that ACME servers may return a certificate chain to an ACME client where an end entity certificate is followed by certificates that certify it. The trust anchor certificate SHOULD be omitted from the chain as it is assumed that the trust anchor is already known by the ACME client i.e. the EST or TEAP server.

8.3.1. EST /cacerts

EST [RFC7030] Section 4.2.3 states that the /simpleenroll response contains "only the certificate that was issued". EST [RFC7030] Section 4.1.3 states that the /cacerts response "MUST include any additional certificates the client would need to build a chain from an EST CA-issued certificate to the current EST CA TA".

Therefore, the EST server MUST return only the ACME end entity certificate in the /simpleenroll response. The EST server MUST return the remainder of the chain returned by the ACME server to the EST server in the /cacerts response to the client, appending the trust anchor root CA if necessary.

8.3.2. TEAP PKCS#7 TLV

TEAP [RFC7170] Section 4.2.16 allows for download of a PKCS#7 [RFC2315] certificate chain in response to a TEAP PKCS#10 [RFC2986] TLV request. TEAP also allows for download of multiple PKCS#7 certificates in response to a TEAP Trusted-Server-Root TLV request.

The TEAP server MUST return the full ACME client certificate chain in the PKCS#7 response to the PKCS#10 TLV request. The TEAP server MUST return the ACME server trust anchor in a PKCS#7 response to a Trusted-Server-Root TLV request. As outlined in Section 8.4, the TEAP server SHOULD also return the trust anchor that was used for issuing its own identity certificate, if different from the ACME server trust anchor.

8.4. id-kp-cmcRA

BRSKI [RFC8995] mandates that the id-kp-cmcRA extended key usage OID is set in the Registrar (or EST RA) end entity certificate that the Registrar uses when signing voucher request messages sent to the MASA. Public ACME servers may not be willing to issue end entity certificates that have the id-kp-cmcRA extended key usage OID set. In these scenarios, the EST RA may be used by the pledge to get issued certificates by a public ACME server, but the EST RA itself will need an end entity certificate that has been issued by a different CA (e.g. an operator deployed private CA) and that has the id-kp-cmcRA OID set.

8.5. Error Handling

ACME [RFC8555] Section 6.7 defines multiple errors that may be returned by an ACME server to an ACME client. TEAP [RFC7170] Section 4.2.6 defines multiple errors that may be returned by a TEAP server to a client in an Error TLV. EST [RFC7030] Section 4.2.3 defines how an EST server may return an error encoded in a CMC [RFC5272] response, or may return a human readable error in the response body.

If a client sends a certificate enrollment request to an EST RA for an identifier that the RA does not control, the RA MUST respond with a suitable 4xx HTTP [RFC9110] error code, and MUST NOT send an enrollment request to the ACME server. The RA MAY include a CMCFailInfo [RFC5272] error code of badIdentity.

If a client sends a certificate enrollment request to a TEAP server for an identifier that the TEAP server does not control, the TEAP server MUST respond with an Error TLV with error code 1024 Bad Identity In Certificate Signing Request, and MUST NOT send an enrollment request to the ACME server.

If the EST RA or TEAP server sends an enrollment request to the ACME server and receives an error response from the ACME server, the following mapping from ACME errors to CMC [RFC5272] Section 6.1.4 CMCFailInfo and TEAP [RFC7170] Section 4.2.6 error codes is RECOMMENDED.

ACME	CMCFailInfo	TEAP Error Code
badCSR	badRequest	1025 Bad CSR
caa	badRequest	1025 Bad CSR
rejectedIdentifier	badIdentity	1024 Bad Identity In CSR
all other errors	internalCAError	1026 Internal CA Error

Table 1

9. IANA Considerations

This document does not make any requests to IANA.

10. Security Considerations

This draft is informational and makes no changes to the referenced specifications. All security considerations from these referenced documents are applicable here:

* EST [RFC7030]

* BRSKI [RFC8995]

* BRSKI Default Cloud Registrar [I-D.ietf-anima-brski-cloud]

* TEAP [RFC7170]

Additionally, all Security Considerations in ACME in the following areas are equally applicable to ACME Integrations.

It is expected that the integration mechanisms proposed here will primarily use the 'dns-01' challenge documented in [RFC8555] Section 8.4. The security considerations in [RFC8555] says:

The DNS is a common point of vulnerability for all of these challenges. An entity that can provision false DNS records for a domain can attack the DNS challenge directly and can provision false A/AAAA records to direct the ACME server to send its HTTP validation query to a remote server of the attacker's choosing.

It is expected that the TEAP-EAP server/EST Registrar will perform DNS dynamic updates. This can be done in a variety of ways, including use of [RFC3007] Dynamic updates (with [RFC2136]), secured with either SIG(0) [RFC2931], or TSIG keys. Other proprietary APIs and interactions are also common, secured by some local credential.

A concern is the disclosure of the credential used to update the DNS records. If an attacker gains access to the credential, they can provision their own certificates into the name space of the entity.

For many uses, this may allow the attacker to get access to some enterprise resource. When used to provision, for instance, a (SIP) phone system this would permit an attacker to impersonate a legitimate phone. Not only does this allow for redirection of phone calls, but possibly also toll fraud.

Operators should consider restricting the integration server such that it can only update the DNS records for a specific zone or zones where ACME is required for client certificate enrollment automation. For example, if all IoT devices in an organization enroll using EST against an EST RA, and all IoT devices will be issued certificates in a subdomain under iot.example.com, then the integration server could be issued a credential that only allows updating of DNS records in a zone that includes domains in the iot.example.com namespace, but does not allow updating of DNS records under any other example.com DNS namespace.

When performing challenge fulfilment via writing files to HTTP webservers, write access should only be granted to a specific set of servers, and only to a specific set of directories for storage of challenge files.

10.1. Denial of Service against ACME infrastructure

The intermediate node (the TEAP-EAP server, or the EST Registrar) should cache the resulting certificates such that if the communication with the pledge is lost, subsequent attempts to enroll will result in the cache certificate being returned.

As many public ACME servers have per-day, per-IP and per-subjectAltName limits, it is prudent not to request identical certificates too often. When the limits are hit, it is often a sign of operator or installer error: Multiple configuration resets occurring within a short period of time.

Many private CA relationships use [RFC8555] as their enrollment protocol, and in those cases, there may be very different limits. But, rate limiting and caching still has some value in protecting external infrastructure.

The cache should be indexed by the complete contents of the Certificate Signing Request, and should not persist beyond the notAfter date in the certificate.

This means that if the private/public keypair changes on the pledge, then a new certificate will be issued. If the requested SubjectAltName changes, then a new certificate will be requested.

In a case where a device is simply factory reset, and enrolls again, then the same certificate can be returned.

10.2. TLS Channel Bindings

EST [RFC7030], Section 3.5 and TEAP [RFC7170], Section 3.8.2 specify mechanisms to bind the PKCS#10 CSR request with the TLS tunnel used to transport the CSR request by using the tls-unique value from the TLS subsystem. It is RECOMMENDED that implementations use these tls-unique channel binding mechanisms.

11. References

11.1. Normative References

[I-D.ietf-acme-subdomains]
Friel, O., Barnes, R., Hollebeek, T., and M. Richardson, "Automated Certificate Management Environment (ACME) for Subdomains", Work in Progress, Internet-Draft, draft-ietf-acme-subdomains-07, 1 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-subdomains-07>.

[I-D.ietf-anima-brski-cloud]
Friel, O., Shekh-Yusef, R., and M. Richardson, "BRSKI Cloud Registrar", Work in Progress, Internet-Draft, draft-ietf-anima-brski-cloud-06, 17 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-cloud-06>.

[I-D.ietf-lamps-rfc7030-csrattrs]
Richardson, M., Friel, O., von Oheimb, D., and D. Harkins, "Clarification of RFC7030 CSR Attributes definition", Work in Progress, Internet-Draft, draft-ietf-lamps-rfc7030-csrattrs-02, 8 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-rfc7030-csrattrs-02>.

[I-D.ietf-uta-rfc6125bis]
Salz, R., "Update to Verifying TLS Server Identities with X.509 Certificates", Work in Progress, Internet-Draft, draft-ietf-uta-rfc6125bis, 1 April 2021, <https://datatracker.ietf.org/doc/draft-ietf-uta-rfc6125bis/>.

[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>.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, DOI 10.17487/RFC5272, June 2008, <https://www.rfc-editor.org/info/rfc5272>.

[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>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/info/rfc9110>.

11.2. Informative References

[IDevID] IEEE, "IEEE Standard for Local and metropolitan area networks - Secure Device Identity", n.d., <https://1.ieee802.org/security/802-1ar>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, DOI 10.17487/RFC2315, March 1998, <https://www.rfc-editor.org/info/rfc2315>.

[RFC2931] Eastlake 3rd, D., "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, DOI 10.17487/RFC2931, September 2000, <https://www.rfc-editor.org/info/rfc2931>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, DOI 10.17487/RFC3007, November 2000, <https://www.rfc-editor.org/info/rfc3007>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", RFC 8366, DOI 10.17487/RFC8366, May 2018, <https://www.rfc-editor.org/info/rfc8366>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

Authors' Addresses

Owen Friel
Cisco
Email: ofriel@cisco.com

Richard Barnes
Cisco
Email: rlb@ipv.sx

Rifaat Shekh-Yusef
Ernst & Young
Email: rifaat.s.ietf@gmail.com

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca