Internet Engineering Task Force (IETF)
Request for Comments: 8739
Category: Standards Track
ISSN: 2070-1721

Y. Sheffer
Intuit
D. Lopez
O. Gonzalez de Dios
A. Pastor Perales
Telefonica I+D
T. Fossati
ARM

March 2020

Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME)

Abstract

Public key certificates need to be revoked when they are compromised, that is, when the associated private key is exposed to an unauthorized entity. However, the revocation process is often unreliable. An alternative to revocation is issuing a sequence of certificates, each with a short validity period, and terminating the sequence upon compromise. This memo proposes an Automated Certificate Management Environment (ACME) extension to enable the issuance of Short-Term, Automatically Renewed (STAR) X.509 certificates.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8739.

Copyright Notice

1. Introduction
  1.1. Name Delegation Use Case
  1.2. Terminology
  1.3. Conventions Used in This Document
2. Protocol Flow
  2.1. Bootstrap
  2.2. Auto Renewal
  2.3. Termination
3. Protocol Details
  3.1. ACME Extensions
    3.1.1. Extending the Order Resource
    3.1.2. Canceling an Auto-renewal Order
  3.2. Capability Discovery
  3.3. Fetching the Certificates
  3.4. Negotiating an Unauthenticated GET
  3.5. Computing notBefore and notAfter of STAR Certificates
    3.5.1. Example
4. Operational Considerations
  4.1. The Meaning of "Short Term" and the Impact of Skewed Clocks
  4.2. Impact on Certificate Transparency (CT) Logs
  4.3. HTTP Caching and Dependability
5. IANA Considerations
  5.1. New Registries
  5.2. New Error Types
  5.3. New Fields in Order Objects
  5.4. Fields in the "auto-renewal" Object within an Order Object
  5.5. New Fields in the "meta" Object within a Directory Object
  5.6. Fields in the "auto-renewal" Object within a Directory Metadata Object
  5.7. Cert-Not-Before and Cert-Not-After HTTP Headers
6. Security Considerations
  6.1. No Revocation
  6.2. Denial-of-Service Considerations
  6.3. Privacy Considerations
7. References
  7.1. Normative References
  7.2. Informative References
Acknowledgments
Authors' Addresses

1. Introduction

The ACME protocol [RFC8555] automates the process of issuing a certificate to a named entity (an Identifier Owner or IdO). Typically, but not always, the identifier is a domain name.

If the IdO wishes to obtain a string of short-term certificates originating from the same private key (see [TOPALOVIC] about why using short-lived certificates might be preferable to explicit revocation), she must go through the whole ACME protocol each time a new short-term certificate is needed, e.g., every 2-3 days. If done this way, the process would involve frequent interactions between the registration function of the ACME Certification Authority (CA) and the identity provider infrastructure (e.g., DNS, web servers), therefore making the issuance of short-term certificates exceedingly dependent on the reliability of both.

This document presents an extension of the ACME protocol that optimizes this process by making short-term certificates first-class objects in the ACME ecosystem. Once the Order for a string of short-term certificates is accepted, the CA is responsible for publishing the next certificate at an agreed upon URL before the previous one expires. The IdO can terminate the automatic renewal before the negotiated deadline if needed, e.g., on key compromise.

For a more generic treatment of STAR certificates, readers are referred to [SHORT-TERM-CERTS].

1.1. Name Delegation Use Case

The proposed mechanism can be used as a building block of an efficient name-delegation protocol, for example, one that exists between a Content Distribution Network (CDN) or a cloud provider and its customers [STAR-DELEGATION]. At any time, the service customer (i.e., the IdO) can terminate the delegation by simply instructing the CA to stop the automatic renewal and letting the currently active certificate expire shortly thereafter.

Note that in the name delegation use case, the delegated entity needs to access the auto-renewed certificate without being in possession of the ACME account key that was used for initiating the STAR issuance. This leads to the optional use of unauthenticated GET in this protocol (Section 3.4).

1.2. Terminology

IdO   Identifier Owner, the owner of an identifier, e.g., a domain
        name, a telephone number, etc.
STAR   Short-Term, Automatically Renewed X.509 certificates.

1.3. Conventions Used in This Document

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.

2. Protocol Flow

The following subsections describe the three main phases of the protocol:

* Bootstrap: the IdO asks an ACME CA to create a short-term, automatically renewed (STAR) certificate (Section 2.1);
* Auto-renewal: the ACME CA periodically reissues the short-term certificate and posts it to the star-certificate URL (Section 2.2);
* Termination: the IdO requests the ACME CA to discontinue the automatic renewal of the certificate (Section 2.3).

2.1. Bootstrap

The IdO, in its role as an ACME client, requests the CA to issue a STAR certificate, i.e., one that:

* Has a short validity, e.g., 24 to 72 hours. Note that the exact definition of "short" depends on the use case;
* Is automatically renewed by the CA for a certain period of time;
* Is downloadable from a (highly available) location.

Other than that, the ACME protocol flows as usual between IdO and CA. In particular, IdO is responsible for satisfying the requested ACME challenges until the CA is willing to issue the requested certificate. Per normal ACME processing, the IdO is given back an Order resource associated with the STAR certificate to be used in subsequent interaction with the CA (e.g., if the certificate needs to be terminated.)

The bootstrap phase ends when the ACME CA updates the Order resource to include the URL for the issued STAR certificate.

2.2. Auto Renewal

The CA issues the initial certificate after the authorization completes successfully. It then automatically reissues the certificate using the same Certificate Signing Request (CSR) (and therefore the same identifier and public key) before the previous one expires and publishes it to the URL that was returned to the IdO at the end of the bootstrap phase. The certificate user, which could be either the IdO itself or a delegated third party as described in [STAR-DELEGATION], obtains the certificate (Section 3.3) and uses it.

The auto-renewal process (Figure 1) goes on until either:

* IdO explicitly terminates the automatic renewal (Section 2.3); or
* Automatic renewal expires.

```
      Certificate             ACME/STAR
      User                    Server
      |     Retrieve cert     |                     [...]
      |---------------------->|                      |
      |                       +------.              /
      |                       |      |             /
      |                       | Automatic renewal :
      |                       |      |             \
      |                       |<-----'              \
      |     Retrieve cert     |                      |
      |---------------------->|           short validity period
      |                       |                      |
      |                       +------.              /
      |                       |      |             /
      |                       | Automatic renewal :
      |                       |      |             \
      |                       |<-----'              \
      |     Retrieve cert     |                      |
      |---------------------->|           short validity period
      |                       |                      |
      |                       +------.              /
      |                       |      |             /
      |                       | Automatic renewal :
      |                       |      |             \
      |                       |<-----'              \
      |                       |                      |
      |         [...]         |                    [...]
```

Figure 1: Auto-renewal

2.3. Termination

The IdO may request early termination of the STAR certificate by sending a cancellation request to the Order resource as described in Section 3.1.2. After the CA receives and verifies the request, it shall:

- Cancel the automatic renewal process for the STAR certificate;
- Change the certificate publication resource to return an error indicating the termination of the issuance;
- Change the status of the Order to "canceled".

Note that it is not necessary to explicitly revoke the short-term certificate.

```
      Certificate                                     ACME/STAR
      User                    IdO                     Server
      |                       |                       |
      |                       |      Cancel Order     |
      |                       +---------------------->|
      |                       |                       +-------.
      |                       |                       |       |
      |                       |                       | End auto-renewal
      |                       |                       | Remove cert link
      |                       |                       | etc.
      |                       |                       |       |
      |                       |         Done          |<------'
      |                       |<----------------------+
      |                       |                       |
      |                                               |
      |              Retrieve cert                    |
      +---------------------------------------------->|
      |              Error: autoRenewalCanceled       |
      |<----------------------------------------------+
      |                                               |
```

Figure 2: Termination

3. Protocol Details

This section describes the protocol details, namely the extensions to the ACME protocol required to issue STAR certificates.

3.1. ACME Extensions

This protocol extends the ACME protocol to allow for automatically renewed Orders.

3.1.1. Extending the Order Resource

The Order resource is extended with a new "auto-renewal" object that MUST be present for STAR certificates. The "auto-renewal" object has the following structure:

* start-date (optional, string): The earliest date of validity of the first certificate issued, in [RFC3339] format. When omitted, the start date is as soon as authorization is complete.
* end-date (required, string): The latest date of validity of the last certificate issued, in [RFC3339] format.
* lifetime (required, integer): The maximum validity period of each STAR certificate, an integer that denotes a number of seconds. This is a nominal value that does not include any extra validity time due to server or client adjustment (see below).
* lifetime-adjust (optional, integer): The amount of "left pad" added to each STAR certificate, an integer that denotes a number of seconds. The default is 0. If present, the value of the notBefore field that would otherwise appear in the STAR certificates is pre-dated by the specified number of seconds. See Section 4.1 for why a client might want to use this control, and Section 3.5 for how the effective certificate lifetime is computed. The value reflected by the server, together with the value of the lifetime attribute, can be used by the client as a hint to configure its polling timer.
* allow-certificate-get (optional, boolean): See Section 3.4.

These attributes are included in a POST message when creating the Order as part of the object encoded as "payload". They are returned when the Order has been created. The ACME server MAY adjust them at will according to its local policy (see also Section 3.2).

The optional notBefore and notAfter fields defined in Section 7.1.3 of [RFC8555] MUST NOT be present in a STAR Order. If they are included, the server MUST return an error with status code 400 (Bad Request) and type "malformedRequest".

Section 7.1.6 of [RFC8555] defines the following values for the Order resource's status: "pending", "ready", "processing", "valid", and "invalid". In the case of auto-renewal Orders, the status MUST be "valid" as long as STAR certificates are being issued. This document adds a new status value: "canceled" (see Section 3.1.2).

A STAR certificate is by definition a dynamic resource, i.e., it refers to an entity that varies over time. Instead of overloading the semantics of the "certificate" attribute, this document defines a new attribute, "star-certificate", to be used instead of "certificate".

* star-certificate (optional, string): A URL for the (rolling) STAR certificate that has been issued in response to this Order.

3.1.2. Canceling an Auto-renewal Order

An important property of the auto-renewal Order is that it can be canceled by the IdO with no need for certificate revocation. To cancel the Order, the ACME client sends a POST to the Order URL as shown in Figure 3.

```
  POST /acme/order/ogfr8EcolOT HTTP/1.1
  Host: example.com
  Content-Type: application/jose+json

  {
    "protected": base64url({
      "alg": "ES256",
      "kid": "https://example.com/acme/acct/gw06UNhKfOve",
      "nonce": "Alc00Ap6Rt7GMkEl3L1JX5",
      "url": "https://example.com/acme/order/ogfr8EcolOT"
    }),
    "payload": base64url({
      "status": "canceled"
    }),
    "signature": "g454e3hdBlkT4AEw...nKePnUyZTjGtXZ6H"
  }
```

Figure 3: Canceling an Auto-renewal Order

After a successful cancellation, the server MUST NOT issue any additional certificates for this Order.

When the Order is canceled, the server:

* MUST update the status of the Order resource to "canceled" and MUST set an appropriate "expires" date;
* MUST respond with 403 (Forbidden) to any requests to the star-certificate endpoint. The response SHOULD provide additional information using a problem document [RFC7807] with type "urn:ietf:params:acme:error:autoRenewalCanceled".

Issuing a cancellation for an Order that is not in "valid" state is not allowed. A client MUST NOT send such a request, and a server MUST return an error response with status code 400 (Bad Request) and type "urn:ietf:params:acme:error:autoRenewalCancellationInvalid".

The state machine described in Section 7.1.6 of [RFC8555] is extended as illustrated in Figure 4.

```
    pending --------------+
       |                  |
       | All authz        |
       | "valid"          |
       V                  |
     ready ---------------+
       |                  |
       | Receive          |
       | finalize         |
       | request          |
       V                  |
   processing -----------+
       |                 |
       | First           |
       | certificate     | Error or
       | issued          | Authorization failure
       |                 |
       |                 V
       |              invalid
       V
     valid----------------+
       |                 |
       | STAR            |
       | Certificate     | Natural
       | canceled        | Expiration
       V                 |
    canceled            =|=
```

Figure 4: State Transitions for STAR Order Objects

Explicit certificate revocation using the revokeCert interface (Section 7.6 of [RFC8555]) is not supported for STAR certificates. A server receiving a revocation request for a STAR certificate MUST return an error response with status code 403 (Forbidden) and type "urn:ietf:params:acme:error:autoRenewalRevocationNotSupported".

3.2. Capability Discovery

In order to support the discovery of STAR capabilities, the "meta" field inside the directory object defined in Section 9.7.6 of [RFC8555] is extended with a new "auto-renewal" object. The "auto-renewal" object MUST be present if the server supports STAR. Its structure is as follows:

* min-lifetime (required, integer): Minimum acceptable value for auto-renewal lifetime, in seconds.
* max-duration (required, integer): Maximum allowed delta between the end-date and start-date attributes of the Order's auto-renewal object.
* allow-certificate-get (optional, boolean): See Section 3.4.

An example directory object advertising STAR support with one-day min-lifetime and one-year max-duration and supporting certificate fetching with an HTTP GET is shown in Figure 5.

```
 {
    "new-nonce": "https://example.com/acme/new-nonce",
    "new-account": "https://example.com/acme/new-account",
    "new-order": "https://example.com/acme/new-order",
    "new-authz": "https://example.com/acme/new-authz",
    "revoke-cert": "https://example.com/acme/revoke-cert",
    "key-change": "https://example.com/acme/key-change",
    "meta": {
      "terms-of-service": "https://example.com/acme/terms/2017-5-30",
      "website": "https://www.example.com/",
      "caa-identities": ["example.com"],
      "auto-renewal": {
        "min-lifetime": 86400,
        "max-duration":  31536000,
        "allow-certificate-get": true
      }
    }
 }
```

Figure 5: Directory Object with STAR Support

3.3. Fetching the Certificates

The certificate is fetched from the star-certificate endpoint with POST-as-GET as per Section 7.4.2 of [RFC8555] unless the client and server have successfully negotiated the "unauthenticated GET" option described in Section 3.4. In such case, the client can simply issue a GET to the star-certificate resource without authenticating itself to the server as illustrated in Figure 6.

```
GET /acme/cert/g7m3ZQeTEqa HTTP/1.1
Host: example.com
Accept: application/pem-certificate-chain

HTTP/1.1 200 OK
Content-Type: application/pem-certificate-chain
Link: <https://example.com/acme/some-directory>;rel="index"
Cert-Not-Before: Thu, 3 Oct 2019 00:00:00 GMT
Cert-Not-After: Thu, 10 Oct 2019 00:00:00 GMT

-----BEGIN CERTIFICATE-----
[End-entity certificate contents]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[Issuer certificate contents]
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
[Other certificate contents]
-----END CERTIFICATE-----
```

Figure 6: Fetching a STAR Certificate with Unauthenticated GET

The server SHOULD include the "Cert-Not-Before" and "Cert-Not-After" HTTP header fields in the response. When they exist, they MUST be equal to the respective fields inside the end-entity certificate. Their format is "HTTP-date" as defined in Section 7.1.1.2 of [RFC7231]. Their purpose is to enable client implementations that do not parse the certificate.

The following are further clarifications regarding usage of these header fields as per Section 8.3.1 of [RFC7231]. All apply to both headers.

* This header field is a single value, not a list.
* The header field is used only in responses to GET, HEAD, and POST-as-GET requests, and only for MIME types that denote public key certificates.
* Header field semantics are independent of context.

* The header field is not hop-by-hop.
* Intermediaries MAY insert or delete the value;
* If an intermediary inserts the value, it MUST ensure that the newly added value matches the corresponding value in the certificate.
* The header field is not appropriate for a Vary field.
* The header field is allowed within message trailers.
* The header field is not appropriate within redirects.
* The header field does not introduce additional security considerations. It discloses in a simpler form information that is already available inside the certificate.

To improve robustness, the next certificate MUST be made available by the ACME CA at the URL indicated by "star-certificate" halfway through the lifetime of the currently active certificate at the latest. It is worth noting that this has an implication in case of cancellation; in fact, from the time the next certificate is made available, the cancellation is not completely effective until the "next" certificate also expires. To avoid the client accidentally entering a broken state, the notBefore of the "next" certificate MUST be set so that the certificate is already valid when it is published at the "star-certificate" URL. Note that the server might need to increase the auto-renewal lifetime-adjust value to satisfy the latter requirement. For a detailed description of the renewal scheduling logic, see Section 3.5. For further rationale on the need for adjusting the certificate validity, see Section 4.1.

The server MUST NOT issue any certificates for this Order with notAfter after the auto-renewal end-date.

For expired Orders, the server MUST respond with 403 (Forbidden) to any requests to the star-certificate endpoint. The response SHOULD provide additional information using a problem document [RFC7807] with type "urn:ietf:params:acme:error:autoRenewalExpired". Note that the Order resource's state remains "valid", as per the base protocol.

3.4. Negotiating an Unauthenticated GET

In order to enable the name delegation workflow defined in [STAR-DELEGATION] and to increase the reliability of the STAR ecosystem (see Section 4.3 for details), this document defines a mechanism that allows a server to advertise support for accessing star-certificate resources via unauthenticated GET (in addition to POST-as-GET), and a client to enable this service with per-Order granularity.

Specifically, a server states its availability to grant unauthenticated access to a client's Order star-certificate by setting the allow-certificate-get attribute to "true" in the auto-renewal object of the meta field inside the directory object:

* allow-certificate-get (optional, boolean): If this field is present and set to "true", the server allows GET (and HEAD) requests to star-certificate URLs.

A client states its desire to access the issued star-certificate via unauthenticated GET by adding an allow-certificate-get attribute to the auto-renewal object of the payload of its newOrder request and setting it to "true".

* allow-certificate-get (optional, boolean): If this field is present and set to "true", the client requests the server to allow unauthenticated GET (and HEAD) to the star-certificate associated with this Order.

If the server accepts the request, it MUST reflect the attribute setting in the resulting order object.

Note that even when the use of unauthenticated GET has been agreed upon, the server MUST also allow POST-as-GET requests to the star-certificate resource.

3.5. Computing notBefore and notAfter of STAR Certificates

We define "nominal renewal date" as the point in time when a new short-term certificate for a given STAR Order is due. Its cadence is a multiple of the Order's auto-renewal lifetime that starts with the issuance of the first short-term certificate and is upper-bounded by the Order's auto-renewal end-date (Figure 7).

```
    T       - STAR Order's auto-renewal lifetime
    end     - STAR Order's auto-renewal end-date
    nrd[i] - nominal renewal date of the i-th STAR certificate
```

```
                 .- T -.   .- T -.   .- T -.   .__.
                /       \ /       \ /       \ /  end
    -----------o---------o---------o---------o----X-------> t
              nrd[0]    nrd[1]    nrd[2]    nrd[3]
```

Figure 7: Nominal Renewal Date

The rules to determine the notBefore and notAfter values of the i-th STAR certificate are as follows:

```
    notAfter  = min(nrd[i] + T, end)
    notBefore = nrd[i] - max(adjust_client, adjust_server)
```

Where "adjust_client" is the minimum value between the auto-renewal lifetime-adjust value ("la"), optionally supplied by the client, and the auto-renewal lifetime of each short-term certificate ("T"); "adjust_server" is the amount of padding added by the ACME server to make sure that all certificates being published are valid at the time of publication. The server padding is a fraction (f) of T (i.e., f * T with .5 <= f < 1; see Section 3.3):

```
    adjust_client = min(T, la)
    adjust_server = f * T
```

Note that the ACME server MUST NOT set the notBefore of the first STAR certificate to a date prior to the auto-renewal start-date.

3.5.1. Example

Given a server that intends to publish the next STAR certificate halfway through the lifetime of the previous one, and a STAR Order with the following attributes:

```
     "auto-renewal": {
       "start-date": "2019-01-10T00:00:00Z",
       "end-date": "2019-01-20T00:00:00Z",
       "lifetime": 345600,          // 4 days
       "lifetime-adjust": 259200    // 3 days
     }
```

The amount of time that needs to be subtracted from each nominal renewal date is 3 days, i.e., max(min(345600, 259200), 345600 * .5).

The notBefore and notAfter of each short-term certificate are:

notBefore	notAfter
2019-01-10T00:00:00Z	2019-01-14T00:00:00Z
2019-01-11T00:00:00Z	2019-01-18T00:00:00Z
2019-01-15T00:00:00Z	2019-01-20T00:00:00Z

Table 1

The value of the notBefore is also the time at which the client should expect the new certificate to be available from the star-certificate endpoint.

4. Operational Considerations

4.1. The Meaning of "Short Term" and the Impact of Skewed Clocks

"Short Term" is a relative concept; therefore, trying to define a cutoff point that works in all cases would be a useless exercise. In practice, the expected lifetime of a STAR certificate will be counted in minutes, hours, or days, depending on different factors: the underlying requirements for revocation, how much clock synchronization is expected among relying parties and the issuing CA, etc.

Nevertheless, this section attempts to provide reasonable suggestions for the Web use case, informed by current operational and research experience.

Acer et al. [ACER] find that one of the main causes of "HTTPS error" warnings in browsers is misconfigured client clocks. In particular, they observe that roughly 95% of the "severe" clock skews -- the 6.7% of clock-related breakage reports that account for clients that are more than 24 hours behind -- happen to be within 6-7 days.

In order to avoid these spurious warnings about a not yet valid server certificate, site owners could use the auto-renewal lifetime-adjust attribute to control the effective lifetime of their Web-facing certificates. The exact number depends on the percentage of the "clock-skewed" population that the site owner expects to protect -- 5 days cover 97.3%, 7 days cover 99.6% -- as well as the nominal auto-renewal lifetime of the STAR Order. Note that exact choice is also likely to depend on the kinds of client that are prevalent for a given site or app -- for example, Android and Mac OS clients are known to behave better than Windows clients. These considerations are clearly out of scope of this document.

In terms of security, STAR certificates and certificates with the Online Certificate Status Protocol (OCSP) "must-staple" flag asserted [RFC7633] can be considered roughly equivalent if the STAR certificate's and the OCSP response's lifetimes are the same. (Here, "must-staple" refers to a certificate carrying a TLS feature extension with the "status_request" extension identifier [RFC6066].) Given OCSP responses can be cached, on average, for 4 days [STARK], it is RECOMMENDED that a STAR certificate that is used on the Web has an "effective" lifetime (excluding any adjustment to account for clock skews) no longer than 4 days.

4.2. Impact on Certificate Transparency (CT) Logs

Even in the highly unlikely case STAR becomes the only certificate issuance model, discussion with the IETF TRANS Working Group and implementers of Certificate Transparency (CT) logs suggests that existing CT Log server implementations are capable of sustaining the resulting 100-fold increase in ingestion rate. Additionally, such a future higher load could be managed with a variety of techniques (e.g., sharding by modulo of certificate hash, using "smart" load-balancing CT proxies, etc.). With regards to the increase in the log size, current CT log growth is already being managed with schemes like Chrome's Log Policy [OBRIEN], which allow Operators to define their log life cycle, as well as allowing the CAs, User Agents, Monitors, and any other interested entities to build in support for that life cycle ahead of time.

4.3. HTTP Caching and Dependability

When using authenticated POST-as-GET, the HTTPS endpoint from where the STAR certificate is fetched can't be easily replicated by an on-path HTTP cache. Reducing the caching properties of the protocol makes STAR clients increasingly dependent on the ACME server availability. This might be problematic given the relatively high rate of client-server interactions in a STAR ecosystem, especially when multiple endpoints (e.g., a high number of CDN edge nodes) end up requesting the same certificate. Clients and servers should consider using the mechanism described in Section 3.4 to mitigate the risk.

When using unauthenticated GET to fetch the STAR certificate, the server SHALL use the appropriate cache directives to set the freshness lifetime of the response (Section 5.2 of [RFC7234]) such that on-path caches will consider it stale before or at the time its effective lifetime is due to expire.

5. IANA Considerations

5.1. New Registries

Per this document, IANA has created the following new registries:

* ACME Order Auto-Renewal Fields (Section 5.4)
* ACME Directory Metadata Auto-Renewal Fields (Section 5.6)

These registries are administered under a Specification Required policy [RFC8126].

5.2. New Error Types

Per this document, IANA has added the following entries to the "ACME Error Types" registry:

Type	Description	Reference
autoRenewalCanceled	The short-term certificate is no longer available because the auto-renewal Order has been explicitly canceled by the IdO	RFC 8739
autoRenewalExpired	The short-term certificate is no longer available because the auto-renewal Order has expired	RFC 8739
autoRenewalCancellationInvalid	A request to cancel an auto-renewal Order that is not in state "valid" has been received	RFC 8739
autoRenewalRevocationNotSupported	A request to revoke an auto-renewal Order has been received	RFC 8739

Table 2

5.3. New Fields in Order Objects

Per this document, IANA has added the following entries to the "ACME Order Object Fields" registry:

Field Name	Field Type	Configurable	Reference
auto-renewal	object	true	RFC 8739
star-certificate	string	false	RFC 8739

Table 3

5.4. Fields in the "auto-renewal" Object within an Order Object

The "ACME Order Auto-Renewal Fields" registry lists field names that are defined for use in the JSON object included in the "auto-renewal" field of an ACME order object.

Template:

* Field name: The string to be used as a field name in the JSON object
* Field type: The type of value to be provided, e.g., string, boolean, array of string
* Configurable: Boolean indicating whether the server should accept values provided by the client
* Reference: Where this field is defined

Initial contents: The fields and descriptions defined in Section 3.1.1.

Field Name	Field Type	Configurable	Reference
start-date	string	true	RFC 8739
end-date	string	true	RFC 8739
lifetime	integer	true	RFC 8739
lifetime-adjust	integer	true	RFC 8739
allow-certificate-get	boolean	true	RFC 8739

Table 4

5.5. New Fields in the "meta" Object within a Directory Object

Per this document, IANA has added the following entry to the "ACME

Directory Metadata Fields":

Field Name	Field Type	Reference
auto-renewal	object	RFC 8739

Table 5

5.6. Fields in the "auto-renewal" Object within a Directory Metadata Object

The "ACME Directory Metadata Auto-Renewal Fields" registry lists field names that are defined for use in the JSON object included in the "auto-renewal" field of an ACME directory "meta" object.

Template:

* Field name: The string to be used as a field name in the JSON object
* Field type: The type of value to be provided, e.g., string, boolean, array of string
* Reference: Where this field is defined

Initial contents: The fields and descriptions defined in Section 3.2.

Field Name	Field Type	Reference
min-lifetime	integer	RFC 8739
max-duration	integer	RFC 8739
allow-certificate-get	boolean	RFC 8739

Table 6

5.7. Cert-Not-Before and Cert-Not-After HTTP Headers

The "Message Headers" registry has been updated with the following additional values:

Header Field Name	Protocol	Status	Reference
Cert-Not-Before	http	standard	RFC 8739, Section 3.3
Cert-Not-After	http	standard	RFC 8739, Section 3.3

Table 7

6. Security Considerations

6.1. No Revocation

STAR certificates eliminate an important security feature of PKI, which is the ability to revoke certificates. Revocation allows the administrator to limit the damage done by a rogue node or an adversary who has control of the private key. With STAR certificates, expiration replaces revocation so there is potential for lack of timeliness in the revocation taking effect. To that end, see also the discussion on clock skew in Section 4.1.

It should be noted that revocation also has timeliness issues because both Certificate Revocation Lists (CRLs) and OCSP responses have nextUpdate fields that tell relying parties (RPs) how long they should trust this revocation data. These fields are typically set to hours, days, or even weeks in the future. Any revocation that happens before the time in nextUpdate goes unnoticed by the RP.

One situation where the lack of explicit revocation could create a security risk to the IdO is when the Order is created with a start-date of some appreciable amount of time in the future. Recall that when authorizations have been fulfilled, the Order moves to the "valid" state and the star-certificate endpoint is populated with the first cert (Figure 4). So, if an attacker manages to get hold of the private key as well as the first (post-dated) certificate, there is a time window in the future when they will be able to successfully impersonate the IdO. Note that cancellation is pointless in this case. In order to mitigate the described threat, it is RECOMMENDED that IdO place their Orders at a time that is close to the Order's start-date.

More discussion of the security of STAR certificates is available in [TOPALOVIC].

6.2. Denial-of-Service Considerations

STAR adds a new attack vector that increases the threat of denial-of-service attacks, caused by the change to the CA's behavior. Each STAR request amplifies the resource demands upon the CA, where one Order produces not one but potentially dozens or hundreds of certificates, depending on the auto-renewal "lifetime" parameter. An attacker can use this property to aggressively reduce the auto-renewal "lifetime" (e.g., 1 second) jointly with other ACME attack vectors identified in Section 10 of [RFC8555]. Other collateral impact is related to the certificate endpoint resource where the client can retrieve the certificates periodically. If this resource is external to the CA (e.g., a hosted web server), the previous attack will be reflected to that resource.

Mitigation recommendations from ACME still apply, but some of them need to be adjusted. For example, applying rate limiting to the initial request, due to the nature of the auto-renewal behavior, cannot solve the above problem. The CA server needs complementary mitigation, and specifically, it SHOULD enforce a minimum value on auto-renewal "lifetime". Alternatively, the CA can set a rate limit for internal certificate generation processes. Note that this limit has to take account of already scheduled renewal issuances as well as new incoming requests.

6.3. Privacy Considerations

In order to avoid correlation of certificates by account, if unauthenticated GET is negotiated (Section 3.4), the recommendation in Section 10.5 of [RFC8555] regarding the choice of URL structure applies, i.e., servers SHOULD choose URLs of certificate resources in a non-guessable way, for example, using capability URLs [W3C.CAPABILITY-URLS].

7. References

7.1. Normative References

[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>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <https://www.rfc-editor.org/info/rfc7234>.

[RFC7807] Nottingham, M. and E. Wilde, "Problem Details for HTTP APIs", RFC 7807, DOI 10.17487/RFC7807, March 2016, <https://www.rfc-editor.org/info/rfc7807>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

7.2. Informative References

[ACER] Acer, M.E., Stark, E., Felt, A.P., Fahl, S., Bhargava, R., Dev, B., Braithwaite, M., Sleevi, R., and P. Tabriz, "Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors", DOI 10.1145/3133956.3134007, October 2017, <https://acmccs.github.io/papers/p1407-acerA.pdf>.

[OBRIEN] O'Brien, D. and R. Sleevi, "Chromium Certificate Transparency Policy", April 2017, <https://github.com/chromium/ct-policy>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <https://www.rfc-editor.org/info/rfc6066>.

[RFC7633] Hallam-Baker, P., "X.509v3 Transport Layer Security (TLS) Feature Extension", RFC 7633, DOI 10.17487/RFC7633, October 2015, <https://www.rfc-editor.org/info/rfc7633>.

[SHORT-TERM-CERTS] Nir, Y., Fossati, T., Sheffer, Y., and T. Eckert, "Considerations For Using Short Term Certificates", Work in Progress, Internet-Draft, draft-nir-saag-star-01, 5 March 2018, <https://tools.ietf.org/html/draft-nir-saag-star-01>.

[STAR-DELEGATION] Sheffer, Y., Lopez, D., Pastor, A., and T. Fossati, "An ACME Profile for Generating Delegated STAR Certificates", Work in Progress, Internet-Draft, draft-ietf-acme-star-delegation-03, 8 March 2020, <https://tools.ietf.org/html/draft-ietf-acme-star-delegation-03>.

[STARK] Stark, E., Huang, L.S., Israni, D., Jackson, C., and D. Boneh, "The case for prefetching and prevalidating TLS server certificates", February 2012, <https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-prefetch.html>.

[TOPALOVIC] Topalovic, E., Saeta, B., Huang, L.S., Jackson, C., and D. Boneh, "Towards Short-Lived Certificates", 2012, <https://www.ieee-security.org/TC/W2SP/2012/papers/w2sp12-final9.pdf>.

[W3C.CAPABILITY-URLS] Tennison, J., "Good Practices for Capability URLs", W3C First Public Working Draft, Latest version available at <https://www.w3.org/TR/capability-urls/>, February 2014, <https://www.w3.org/TR/2014/WD-capability-urls-20140218>.

Acknowledgments

This work is partially supported by the European Commission under Horizon 2020 grant agreement no. 688421 Measurement and Architecture for a Middleboxed Internet (MAMI). This support does not imply endorsement.

Thanks to Ben Kaduk, Richard Barnes, Roman Danyliw, Jon Peterson, Eric Rescorla, Ryan Sleevi, Sean Turner, Alexey Melnikov, Adam Roach, Martin Thomson, and Mehmet Ersue for helpful comments and discussions that have shaped this document.

Authors' Addresses

Yaron Sheffer
Intuit

Email: yaronf.ietf@gmail.com

Diego Lopez
Telefonica I+D

Email: diego.r.lopez@telefonica.com

Oscar Gonzalez de Dios
Telefonica I+D

Email: oscar.gonzalezdedios@telefonica.com

Antonio Agustin Pastor Perales
Telefonica I+D

Email: antonio.pastorperales@telefonica.com

Thomas Fossati
ARM

Email: thomas.fossati@arm.com