RFC 9115 : An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 septembre 2021

Date de publication du RFC : Septembre 2021

https://www.bortzmeyer.org/9115.html

Ce nouveau RFC décrit un profil du protocole ACME d'obtention de certificat, profil qui permet de **déléguer** la demande à un tiers. C'est surtout utile pour le cas où vous sous-traitez l'hébergement de votre site Web (par exemple sur un CDN) : le sous-traitant peut alors demander un certificat, avec sa clé privée à lui, pour un nom de domaine que vous contrôlez et prouver qu'il héberge bien le serveur pour ce nom. Serveurs et clients TLS n'ont pas besoin d'être modifiés (seuls les serveurs et clients ACME le seront), et, bien entendu, le titulaire du nom de domaine garde un complet contrôle et peut, par exemple, révoquer les certificats obtenus par ses sous-traitants.

Ce profil utilise lui-même le profil STAR ("*Short-Term, Automatically Renewed*") décrit dans le RFC 8739 [1] donc faites bien attention à avoir lu le RFC 8739 avant. Le cas typique d'utilisation de ce mécanisme de délégation est le CDN. Un webmestre (l'IdO pour "*Identifier Owner*" car il est titulaire du nom de domaine, mettons `foobar.example`) a un site Web et sous-traite tout ou partie du service à un CDN, appelé ici NDC pour "*Name Delegation Consumer*" (et la ressemblance entre les sigles CDN et NDC est volontaire). Le CDN devra pouvoir répondre aux requêtes HTTPS pour `www.foobar.example` et donc présenter un certificat au nom `www.foobar.example`. Avec ACME, l'IdO peut obtenir un tel certifiat mais il ne souhaite probablement pas transmettre la clé privée correspondante au NDC. La solution de notre RFC est d'utiliser une extension à ACME, permettant la délégation du nom. Le NDC pourra alors obtenir un certificat STAR (de courte durée de vie, donc) pour `www.foobar.example`. Pas besoin de partager une clé privée, ni de transmettre des secrets de longue durée de vie (les délégations sont révocables, et les certificats STAR ne durent pas longtemps, le NDC devra renouveller souvent et ça cessera en cas de révocation). C'est l'utilisation typique de la délégation mais d'autres sont possibles (par

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8739.txt`

exemple avec des certificats ordinaires, non-STAR). Le RFC note que la solution de délégation ne modifie qu'ACME, et pas TLS, et qu'elle marche donc avec les clients et serveurs TLS actuels (contrairement à d'autres propositions qui sont étudiées).

Pour que la délégation fonctionne, l'IdO doit avoir un serveur ACME, auquel le NDC devra se connecter, et s'être mis d'accord avec le NDC sur les paramètres à utiliser. C'est donc une étape relativement nouvelle, l'utilisateur d'ACME typique n'ayant qu'un client ACME, seule l'AC a un serveur. Mais c'est quand même plus simple que de monter une AC. Le serveur ACME chez l'IdO ne signera pas de certificats, il relaiera simplement la requête. Quand le NDC aura besoin d'un certificat, il enverra une demande à l'IdO, qui la vérifiera et, devenant client ACME, l'IdO enverra une demande à l'AC. Si ça marche, l'IdO prévient le NDC, et celui-ci récupérera le certificat chez l'AC (par "*unauthenticated GET*", RFC 8739, section 3.4).

Le protocole ACME gagne un nouveau type d'objet, les délégations, qui indiquent ce qu'on permet au NDC. Comme les autres objets ACME, elles sont représentées en JSON et voici un exemple :

```
{
     "csr-template": {
       "keyTypes": [
         {
           "PublicKeyType": "id-ecPublicKey",
           "namedCurve": "secp256r1",
           "SignatureType": "ecdsa-with-SHA256"
         }
       ],
       "subject": {
         "country": "FR",
         "stateOrProvince": "**",
         "locality": "**"
       },
       "extensions": {
         "subjectAltName": {
           "DNS": [
             "www.foobar.example"
           ]
         },
         "keyUsage": [
           "digitalSignature"
         ],
         "extendedKeyUsage": [
           "serverAuth"
         ]
         }
     }
}
```

(Les champs des extensions comme `keyUsage` sont dans un nouveau registre IANA `<https://www.iana.org/assignments/acme/acme.xml#acme-star-delegation-csr-template-extensions>`; on peut ajouter des champs, selon la politique « spécification nécessaire ».) Ici, le NDC est autorisé à demander des certificats ECDSA pour le nom `www.foobar.example`. Quand le NDC enverra sa requête de certificat à l'IdO, il devra inclure cet objet « délégation », que l'IdO pourra comparer avec ce qu'il a configuré pour ce NDC. Voici un exemple partiel, envoyé lors d'un POST HTTPS au serveur ACME de l'IdO :

```
   {
     "protected": base64url({
       "alg": "ES256",
       "kid": "https://acme.ido.example/acme/acct/evOfKhNU60wg",
```

```
    "nonce": "Alc00Ap6Rt7GMkEl3L1JX5",
    "url": "https://acme.ido.example/acme/new-order"
  }),
  "payload": base64url({
    "identifiers": [
      {
        "type": "dns",
        "value": "www.foobar.example"
      }
    ],
    "delegation":
      "https://acme.ido.example/acme/delegation/gm0wfLYHBen"
  }),
  "signature":    ...
```

(Le nouveau champ `delegation` a été placé dans le registre IANA <https://www.iana.org/assignments/acme/acme.xml#acme-order-object-fields>.) Le NDC enverra ensuite le CSR, et l'IdO relaiera la requête vers le serveur ACME de l'AC (moins l'indication de délégation, qui ne regarde pas l'AC).

Quand on utilise un CDN, il est fréquent qu'on doive configurer un alias dans le DNS pour pointer vers un nom indiqué par l'opérateur du CDN. Voici par exemple celui de l'Élysée :

```
% dig CNAME www.elysee.fr
...
;; ANSWER SECTION:
www.elysee.fr. 3600 IN CNAME 3cifmt6.x.incapdns.net.
...
```

L'extension au protocole ACME spécifiée dans notre RFC permet au NDC d'indiquer cet alias dans sa requête, l'IdO peut alors l'inclure dans sa zone DNS.

Tous les serveurs ACME ne seront pas forcément capables de gérer des délégations, il faudra donc l'indiquer dans les capacités du serveur, avec le champ `delegation-enabled` (mis dans le registre IANA <https://www.iana.org/assignments/acme/acme.xml#acme-directory-metadata-fields>).

Comme indiqué plus haut, l'IdO peut arrêter la délégation quand il veut, par exemple parce qu'il change de CDN. Cet arrêt se fait par une interruption explicite de la demande STAR (RFC 8739, section 3.1.2). Si les certificats ne sont pas des STAR, le mécanisme à utiliser est la révocation normale des certificats.

Après cet examen du protocole, la section 3 de notre RFC décrit le comportement de l'AC. Il n'y a pas grand'chose à faire pour l'AC (le protocole est entre le NDC et l'IdO) à part à être capable d'accepter des récupérations non authentifiées de certificats (car le NDC n'a pas de compte à l'AC).

On a parlé plus haut du CSR. Il doit se conformer à un certain gabarit, décidé par l'IdO. Ce gabarit est évidemment au format JSON, comme le reste d'ACME. La syntaxe exacte est décrite avec le langage CDDL (RFC 8610) et figure dans l'annexe A ou bien, si vous préférez, avec le langage JSON Schema, utilisé dans l'annexe B. Voici l'exemple de gabarit du RFC :

```
{
   "keyTypes": [
     {
       "PublicKeyType": "rsaEncryption",
       "PublicKeyLength": 2048,
       "SignatureType": "sha256WithRSAEncryption"
     },
     {
       "PublicKeyType": "id-ecPublicKey",
       "namedCurve": "secp256r1",
       "SignatureType": "ecdsa-with-SHA256"
     }
   ],
   "subject": {
     "country": "CA",
     "stateOrProvince": "**",
     "locality": "**"
   },
   "extensions": {
     "subjectAltName": {
       "DNS": [
         "abc.ido.example"
       ]
     },
     "keyUsage": [
       "digitalSignature"
     ],
     "extendedKeyUsage": [
       "serverAuth",
       "clientAuth"
     ]
   }
 }
```

Dans cet exemple, l'IdO impose au NDC un certificat RSA ou ECDSA et rend impérative (c'est le sens des deux astérisques) l'indication de la province et de la ville. L'IdO doit évidemment vérifier que le CSRT reçu se conforme bien à ce gabarit.

Le RFC présente (en section 5) quelques autres cas d'utilisation de cette délégation. Par exemple, un IdO peut déléguer à plusieurs CDN, afin d'éviter que la panne d'un CDN <https://www.bortzmeyer.org/panne-fastly-presentation.html> n'arrête tout. Avec la délégation, ça se fait tout seul, chacun des CDN est authentifié, et demande séparément son certificat.

Autre cas rigolo, celui où le CDN délègue une partie du service à un CDN plus petit. Le modèle de délégation ACME peut s'y adapter (le petit CDN demande un certificat au gros, qui relaie à l'IdO…), si les différentes parties sont d'accord.

Enfin, la section 7 du RFC revient sur les propriétés de sécurité de ces délégations. En gros, il faut avoir confiance en celui à qui on délègue car, pendant la durée de la délégation, il pourra faire ce qu'il veut avec le nom qu'on lui a délégué, y compris demander d'autres certificats en utilisant sa délégation du nom de domaine. Il existe quelques mesures techniques que l'IdO peut déployer pour empêcher le NDC de faire trop de bêtises. C'est le cas par exemple des enregistrements DNS CAA (RFC 8659) qui peuvent limiter le nombre d'AC autorisées (voir aussi le RFC 8657).

Je ne connais pas encore d'opérateur de CDN qui mette en œuvre cette solution.