RFC 9848 : Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 mars 2026

Date de publication du RFC : Mars 2026

https://www.bortzmeyer.org/9848.html

Le protocole ECH ("*Encrypted Client Hello*", normalisé dans le RFC 9849 [1]) permet de chiffrer la salutation TLS (le ClientHello), notamment le nom du serveur auquel on se connecte. Mais pour cela, il faut la clé publique du serveur. Un des moyens de la récupérer est dans le DNS, comme normalisé dans notre RFC 9848.

C'est qu'ECH pose un problème de cercle vicieux : le serveur TLS (RFC 9846) a besoin du nom demandé par le client pour choisir le bon certificat, donc la bonne clé or, si on veut chiffrer ce nom, il nous faut bien une clé. ECH (RFC 9849) résout le problème en disant que le client TLS va récupérer une clé publique distincte de celle contenue dans le certificat, quelque part. Où ça ? Le RFC 9849 ne le dit pas, mais plusieurs solutions existent, dont notre nouveau RFC qui propose de récupérer cette clé dans le DNS.

Il s'appuie sur les enregistrements SVCB du RFC 9460. Ces enregistrements permettent d'indiquer un grand nombre de paramètres, sous une forme nom=valeur (les « SvcParams »). Les enregistrements HTTPS sont une des formes des SVCB et c'est en général eux qui seront utilisés pour ECH :

```
% dig defo.ie HTTPS
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44251
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
defo.ie.  1750 IN HTTPS 1 . ipv4hint=213.108.108.101 ech=AMD+DQA8ngAgACCBNprc0M4mwJt8Z+q6DtisBc3nQQUwLcEvepAUv27
...
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9849.txt

Que voit-on ? Que `defo.ie` a bien un enregistrement de type HTTPS (dont je rappelle qu'il est une spécialisation du SVCB), qui contient un paramètre ECH (la clé publique et quelques autres informations, mais je ne connais pas de moyen simple d'afficher ces informations).

La section 3 est l'essentiel du RFC. Elle définit le paramètre (« SvcParam ») `ech`, dont la valeur est la clé publique ECH du serveur TLS. Plus précisement, sa valeur est une « ECHConfigList », concept créé par le RFC 9849 (cf. sa section 4), et qui décrit tous les paramètres utiles pour faire de l'ECH. Ce paramètre a été ajouté au registre IANA des SvcParams <`https://www.iana.org/assignments/dns-svcb/dns-svcb.xml#dns-svcparamkeys`> (section 9 de notre RFC).

Si vous voulez fabriquer vous-même un tel enregistrement, la documentation d'Apache donne des explications <`https://httpd.apache.org/docs/trunk/en/mod/mod_ssl.html#sslechkeydir`> (mais il faudra des versions très récentes des logiciels et probablement compilées par vous-même avec les bonnes options).

La section 4 du RFC décrit les conditions d'un déploiement efficace, côté serveur. Si on publie un enregistrement SVCB incluant du `ech`, il faut évidemment s'assurer que le serveur TLS gère ECH. (Un exemple d'outil qui fait ce genre de vérification est echspec <`https://github.com/thekuwayama/echspec`>.) La section 5 du RFC fait la même chose, mais côté serveur ; elle discute notamment des questions de latence puisqu'un client TLS ne peut pas paralléliser la récupération de l'enregistrement DNS avec l'établissement de la session TLS, celle-ci dépendant de ce qu'on trouvera dans l'enregistrement SVCB.

Il existe un autre moyen d'influencer la session TLS, c'est le champ HTTP `Alt-Svc:` du RFC 7838. Comme le note la section 6, `Alt-Svc:` ne peut pas actuellement indiquer de paramètres ECH donc pas de risque de contradiction entre les deux moyens d'obtenir des paramètres TLS sur ce point. En revanche, le serveur doit veiller à ce qu'il publie des enregistrements SVCB avec ECH pour tous les noms qui seraient mentionnés dans le `Alt-Svc:`.

Et puis, bien sûr (section 8), rappelez-vous que ECH servant à dissimuler le nom du serveur demandé, il ne servirait plus à grand'chose si la requête DNS pour ce nom (et le type HTTPS ou SVCB) était en clair et/ou envoyée à des serveurs qui ne sont pas dignes de confiance. Le RFC recommande donc des connexions DNS chiffrées et authentifiées, avec un résolveur de confiance.