Panne du site Web de la Poste, et la révocation des certificats

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 juillet 2020. Dernière mise à jour le 24 juillet 2020

https://www.bortzmeyer.org/poste-revocation.html

Ce matin, les visiteurs du site Web de La Poste ont la désagréable surprise de voir leur navigateur afficher une alerte de sécurité qui les empêche d'aller sur le site . Pourquoi ? C'est un problème assez rare, une révocation du certificat.

Voyons d'abord les symptômes vus par l'utilisateur ou l'utilisatrice normale :

Le certificat a donc été révoqué, ce qui veut dire que l'organisme qui l'a émis, l'Autorité de Certification, a signé un message disant que ce certificat ne devait plus être utilisé (cela peut être, par exemple, car la clé privée correspondante a été compromise).

Et voyons maintenant les détails techniques. D'abord, quel est le numéro de série du certificat ?

```
% gnutls-cli www.laposte.fr
... - subject 'CN=laposte.fr,serialNumber=35600000000048,O=La Poste
   S.A.,street=Quai André
   citroën\,7-11,L=Paris,ST=Île-de-France,C=FR,postalCode=75015,
   businessCategory=Business
   Entity,jurisdictionOfIncorporationLocalityName=Paris,
   jurisdictionOfIncorporationStateOrProvinceName=Île-de-France,
   jurisdictionOfIncorporationCountryName=FR', issuer 'CN=CA de
   Certificados SSL EV,OU=BZ Ziurtagiri publikoa - Certificado publico
   EV,O=IZENPE S.A.,C=ES',
   serial 0x279dad0bbf3d7a5e5b63f8aae70fa366,
   RSA key 4096 bits, signed using RSA-SHA256, activated '2018-08-03 06:39:37 UTC', expires '2020-08-03 06:39:31
    ...
```

(J'aime bien les informations en basque mises par l'AC, Izenpe <https://www.izenpe.com/>.) OK, le certificat final est 279dad0bbf3d7a5e5b63f8aae70fa366 (c'est bien celui qui est révoqué, autrement, il aurait également fallu tester les autres certificats de la chaîne). Cherchons-le dans les journaux "*Certificate Transparency*" (normalisés par le RFC 6962 [1]). On les trouve en , ce qui permet de voir qu'il est en effet révoqué :

Le service `crt.sh` ne nous donne pas la raison de la révocation. Regardons donc la CRL :

```
% openssl s_client -connect www.laposte.fr:443 -showcerts | openssl x509 -text
    ...
    X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.izenpe.com/cgi-bin/crlsslev2
     ...

% wget http://crl.izenpe.com/cgi-bin/crlsslev2

% openssl crl -inform DER -text -noout -in crlsslev2
...
    Serial Number: 279DAD0BBF3D7A5E5B63F8AAE70FA366
        Revocation Date: Jul 22 07:35:53 2020 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Unspecified
```

Et nous avons désormais la révocation de ce certificat 279DAD0BBF3D7A5E5B63F8AAE70FA366 , sa date (il y a plus de vingt-quatre heures, mais notez que la CRL n'est pas forcément publiée immédiatement après l'opération de révocation) et la raison (enfin, si on peut dire).

Sinon, dans un cas comme cela, il peut être prudent de vérifier que le problème n'est pas local et qu'il ne s'agit pas, par exemple, d'un détournement vers un serveur pirate. On va donc utiliser cent sondes RIPE Atlas <https://atlas.ripe.net/> en France pour demander le certificat :

```
 % blaeu-cert --requested 100 --country FR --serial -4 www.laposte.fr
99 probes reported
[279dad0bbf3d7a5e5b63f8aae70fa366] : 99 occurrences
Test #26427062 done at 2020-07-23T08:50:57Z
```

OK, toutes les sondes voient le même numéro de série donc ce n'est sans doute pas un détournement local.

Suite de l'affaire : vers 1100 UTC, le 23 juillet, le certificat révoqué a enfin été remplacé, par un Let's Encrypt. On peut le voir dans le journal <https://crt.sh/?id=3128845569>. Un autre certificat, fait par Global Sign <https://crt.sh/?id=3128983609>, a été émis et a remplacé le Let's Encrypt quelques heures après. Notez qu'il ne s'agit que du site Web public, `www.laposte.fr`. Le 24 juillet au matin, le service `api.laposte.fr` (API du système de suivi de colis) avait toujours un certificat révoqué de l'ancienne AC <https://crt.sh/?id=1454179120&opt=ocsp>.

Sinon, il y a cet article du Monde Informatique <https://www.lemondeinformatique.fr/actualites/lire-lapostefr-indisponible-suite-a-un-probleme-de-certificat-ssl-79818.html>, qui n'apprend rien de plus, et un autre du Figaro <https://www.lefigaro.fr/secteur/high-tech/le-site-internet-de-la-poste-indisponible-pendant-plusieurs-heures-20200723> où la Poste raconte que l'ancien certificat a été révoqué avant l'installation du nouveau.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6962.txt`