Let’s Encrypt contrarié par l’obsolescence du parc Android

À quand l’autonomie pour Let’s Encrypt ? Dans l’absolu, l’autorité de certification à but non lucratif vole déjà de ses propres ailes, sous l’égide d’Internet Security Research Group, société d’intérêt public que financent notamment l’EFF et Mozilla. Mais elle reste dépendante d’IdenTrust.

Ce lien remonte à 2015. Let’s Encrypt commençait alors à émettre son certificat racine ISRG Root X1. En attendant que les éditeurs de navigateurs et de systèmes d’exploitation le mettent en liste blanche, il a fait l’objet d’une signature *via* un certificat tiers. En l’occurrence, celui d’IdenTrust : DST Root X3.

Depuis 2018, ISRG Root X1 figure sur la liste des certificats de confiance dans les principaux OS et navigateurs. Mais il y a une limite à la compatibilité descendante. Notamment sur Android. Les versions antérieures à la 7.1 – sortie en août 2016 – ne prennent pas en charge ISRG Root X1. À moins d’avoir reçu une mise à jour spécifique.

Plus d’un tiers (33,8 %) des appareils Android en circulation seraient dans ce cas. Leurs utilisateurs risquent d’être confrontés à des erreurs lorsqu’ils tenteront de se connecter à des sites qui utilisent ISRG Root X1. Let’s Encrypt se montre de moins en moins optimiste quant à la « modernisation » de ce parc. Mais l’organisation se refuse à nouer un nouveau partenariat avec une autorité de certification tierce. « *Nous engager à prendre en charge les vieilles versions d’Android reviendrait à effectuer indéfiniment* [cette démarche] », résume-t-elle.

Let’s Encrypt joue la montre

Quel palliatif dans ce contexte ? Pour le moment, la connexion avec IdenTrust reste opérationnelle : le certificat DST Root X3 expirera le 30 septembre 2021. Let’s Encrypt souhaite de longue date couper le cordon, mais les motifs sus-exposés ont déjà entraîné plusieurs reports. Il est désormais question du 11 janvier 2021. À cette date, un changement sera effectué sur l’API. Objectif : par défaut, fournir aux sites web des certificats liés directement à ISRG Root X1. Et non plus à DST Root X3.

La transition ne sera cependant pas subite. Les éditeurs pourront choisir de continuer à s’appuyer sur DST Root X3. Ce en exploitant la propriété de relation « alternative » implémentée depuis cet été dans le protocole ACME. Certbot, l’outil de gestion de certificats associé à Let’s Encrypt, la prend en charge depuis sa version 1.6.0, grâce à l’option –preferred-chain.

Cela ne pourra pas durer éternellement, alerte Let’s Encrypt. En tout cas au-delà du 30 septembre 2021 (le partenariat avec IdenTrust, qui doit arriver à échéance le 17 mars 2021, devrait pouvoir être renouvelé jusque-là). Ensuite, il appartiendra aux éditeurs de trancher : abandonner les vieux appareils ? basculer en HTTP non sécurisé ? changer de certificat racine ?… Let’s Encrypt propose une autre solution : demander aux utilisateurs concernés d’installer Firefox Mobile, compatible jusqu’à Android 4.1. La raison : le navigateur n’utilise pas la liste de certificats d’Android. Il a la

sienne… maintenue à jour.

Photo d'illustration © maxkabakov – Fotolia