Let's Encrypt

Jason Kerssens 11320796, Matthijs Bartelink 11322802,
Mike Mourcous 11222077, Florens Douwes 11254483,
Albert de Boer 11251867

15 oktober 2017

1 Let's Encrypt

1.1 Certificaatautoriteit

Let's Encrypt is een certificaatautoriteit gelanceerd op 12 april 2016.[1] Een certificaatauthoriteit is in de cryptografie een entiteit die digitale certificaten verleent. Om voor sites een veilige TLS (https) connectie op te zetten, moet een certificaatauthoriteit zo een certificaat verlenen. Als een site een TLS connectie aanbiedt, kan het verkeer tussen de browser en de server niet afgeluisterd worden.

1.2 Oprichting

Let's Encrypt was opgericht in 2014, omdat het verkrijgen van een TLS certificaat lastig was om op te zetten. Er zijn kosten, veel configuratie was nodig en het was lastig om te updaten. [2] Let's Encrypt wou TLS certificaten gratis maken en ook een makkelijke installatie bieden.

Let's Encrypt is een service aangeboden door de Internet Security Research Group. [3] Sponsors van Let's Encrypt zijn onder andere Mozilla, Akamai, Cisco, EFF, OVH en Chrome. [4]
Let's encrypt is ondersteund door alle moderne browsers. Let's Encrypt maakt gebruik van een al lang bestaande root authority, wat betekend dat er geen software updates nodig zijn voordat Let's Encrypt ondersteund wordt door browsers. [7]

1.3 Groei

Sinds de lancering is het gebruik van Let's Encrypt enorm gegroeid. Op 28 juni had Let's Encrypt aangekondigd dat het 100 miljoenste certificaat was uitgegeven. Het doel van Let's Encrypt is om het World Wide Web 100% https te maken. Toen Let's encrypt was aangekondigd werden minder dan 40% van alle pagina's geladen met HTTPS. In 19 maanden na de lancering is dit 18% omhoog gegaan naar 58%[5].

1.4 Werking

Om de installatie van Let's Encrypt zo makkelijk mogelijk te maken heeft Let's Encrypt de certificaatverificatie automatisch gemaakt. Deze automatische methode van certificaatuitlening heet Automatic Certificate Management Environment ofwel ACME. ACME is een standaard door de The Internet Engineering Task Force (IETF) [9].
De ACME standaard is door vele programma's geïmplementeerd [10]. De meest gebruikte implementatie is de certbot implementatie. Deze implementatie is officieel ondersteund door Let's Encrypt.

De uitgifte van een certificaat wordt in twee delen gedaan. De ACME implementatie genereert een nieuw sleutelpaar en bewijst dat het de controle heeft over het domein waarvoor er

een certificaat wordt uitgegeven. Om dat te bewijzen kan er een DNS aanpassing worden gedaan (alleen de eigenaar van het domein kan dat doen), of een http document op een bepaald pad online zetten met een geheime sleutel (ook alleen de eigenaar van het domein kan dit doen). Daarna verifieert Let's Encrypt op één van de twee methodes of het domein onder de controle valt. Hierna is de ACME implementatie geautoriseerd om een certificaat aan te vragen. De ACME implementatie vraagt een certificaat aan met de standaard Certificate Signing Request [11]. Als alles correct is, dan installeert de ACME implementatie het certificaat in de webserver. Het domein is meteen klaar voor HTTPS verbindingen.
Het vernieuwen van het certificaat verloopt op dezelfde manier, voordat het certificaat afloopt kan er een nieuw certificaat aangevraagd worden.

1.5 Toekomst

Let's Encrypt heeft aangegeven om wildcard domains te ondersteunen in januari 2018. [14] Met een wildcard certificaat worden alle subdomeinen van een domein (`*.example.com`) geautoriseerd. Dit maakt het configureren makkelijker, omdat niet alle subdomeinen handmatig opgegeven moeten worden. Ondersteuning hiervoor is een van de laatste dingen die het gebruik van Let's Encrypt konden tegenhouden.

Zowel Google als Mozilla hebben aangegeven HTTP verkeer af te willen raden. Dit konden ze alleen doen wanneer de installatie van HTTPS makkelijk en gratis was, wat Let's Encrypt heeft gerealiseerd. [12] [13]

Referenties

[1] https://letsencrypt.org/2016/04/12/leaving-beta-new-sponsors.html

[2] https://letsencrypt.org/2014/11/18/announcing-lets-encrypt.html

[3] https://letsencrypt.org/isrg/

[4] https://letsencrypt.org/sponsors/

[5] https://letsencrypt.org/2017/06/28/hundred-million-certs.html

[6] https://letsencrypt.org/docs/faq/

[7] https://letsencrypt.org/docs/certificate-compatibility/

[8] https://letsencrypt.org/how-it-works/

[9] https://ietf-wg-acme.github.io/acme/draft-ietf-acme-acme.html

[10] https://letsencrypt.org/docs/client-options/

[11] https://tools.ietf.org/html/rfc2986

[12] https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/

[13] https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure

[14] https://letsencrypt.org/2017/07/06/wildcard-certificates-coming-jan-2018.html