Let's Encrypt

Subjects: Others
Contributor: HandWiki Zheng

Let's Encrypt is a certificate authority that provides X.509 certificates for Transport Layer Security (TLS) encryption at no charge. The certificate is valid for 90 days, during which renewal can take place at anytime. The offer is accompanied by an automated process designed to overcome manual creation, validation, signing, installation, and renewal of certificates for secure websites. It launched on April 12, 2016. The project claims to make encrypted connections to World Wide Web servers ubiquitous. By eliminating payment, web server configuration, validation email management and certificate renewal tasks, it is meant to significantly lower the complexity of setting up and maintaining TLS encryption. On a Linux web server, execution of only two commands is sufficient to set up HTTPS encryption and acquire and install certificates. To that end, a software package was included into the official Debian and Ubuntu software repositories. Current initiatives of major browser developers such as Mozilla and Google to deprecate unencrypted HTTP are counting on the availability of Let's Encrypt. The project is acknowledged to have the potential to accomplish encrypted connections as the default case for the entire web. Only domain-validated certificates are being issued, since they can be fully automated. Organization Validation and Extended Validation Certificates are not available. By being as transparent as possible, they hope to both protect their own trustworthiness and guard against attacks and manipulation attempts. For that purpose they regularly publish transparency reports, publicly log all ACME transactions (e.g. by using Certificate Transparency), and use open standards and free software as much as possible. Support of ACME v2 and wildcard certificates was added in March 2018.

Keywords: x.509 ; mozilla ; open standards

1. Involved Parties

Let's Encrypt is a service provided by the Internet Security Research Group (ISRG), a public benefit organization. Major sponsors are the Electronic Frontier Foundation (EFF), the Mozilla Foundation, OVH, Akamai, and Cisco Systems. Other partners include the certificate authority IdenTrust, the University of Michigan (U-M), the Stanford Law School, the Linux Foundation[1] as well as Stephen Kent from Raytheon/BBN Technologies and Alex Polvi from CoreOS.[2]

1.1. Technical Advisory Board

- Rich Salz (Akamai Technologies)
- Joe Hildebrand (Mozilla Corporation)
- Jacob Hoffman-Andrews (Electronic Frontier Foundation)
- J. C. Jones (Mozilla Foundation)
- Russ Housley (Independent)
- Ryan Hurst (Google)
- Stephen Kent (Independent)
- Karen O'Donoghue (Internet Society)

2. Technology

In June 2015, Let's Encrypt announced the generation of their first RSA root certificate, ISRG Root X1.[3] The root certificate was used to sign two intermediate certificates[3], which are also cross-signed by the certificate authority IdenTrust.[4][5] One of the intermediate certificates is used to sign issued certificates, while the other is kept offline as a backup in case of problems with the first intermediate certificate.[3] Because the IdenTrust certificate is preinstalled in major web browsers, Let's Encrypt certificates can normally be validated and are accepted upon installation[6] even before browser vendors include the ISRG root certificate as a trust anchor.

The Let's Encrypt developers planned to generate an ECDSA root certificate as well later in 2015,[3] which was pushed back to early 2016, and again to 2018.[7][8][9]

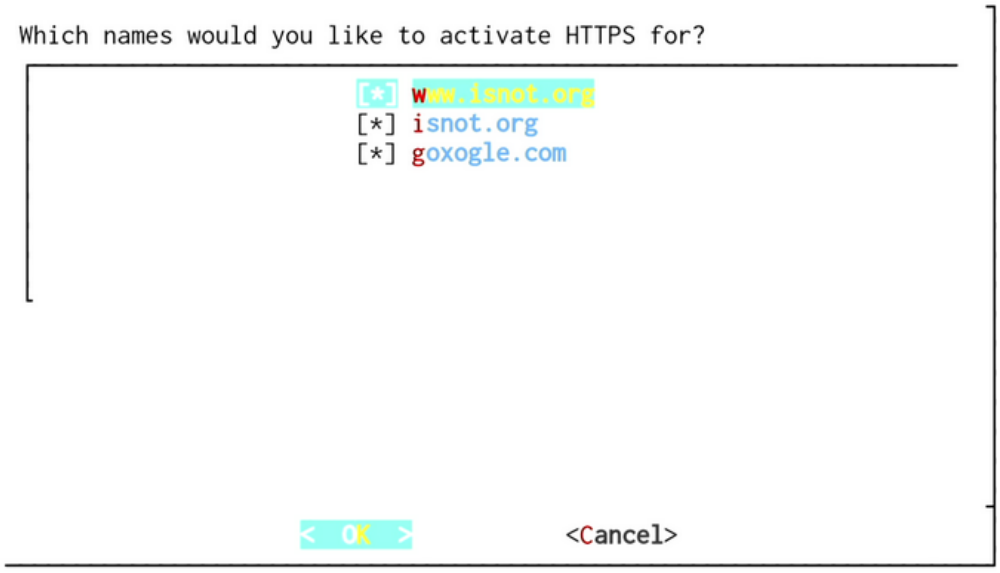
2.1. Protocol

The challenge–response protocol used to automate enrolling with this new certificate authority is called Automated Certificate Management Environment (ACME). It involves various requests to the web server on the domain that is covered by the certificate. Based on whether the resulting responses match the expectations, control of the enrollee over the domain is assured (domain validation). In order to do that, the ACME client software sets up a special TLS server on the server system that gets queried by the ACME certificate authority server with special requests using Server Name Indication (Domain Validation using Server Name Indication, DVSNI).

The validation processes are run multiple times over separate network paths. Checking DNS entries is provisioned to be done from multiple geographically diverse locations to make DNS spoofing attacks harder to do.

ACME interactions are based on exchanging JSON documents over HTTPS connections.[10] A draft specification is available on GitHub,[11] and a version has been submitted to the Internet Engineering Task Force (IETF) as a proposal for an Internet standard.[12]

2.2. Software Implementation



Domain selection dialogue. https://handwiki.org/wiki/index.php?curid=1447148

The certificate authority consists of a piece of software called Boulder, written in Go, that implements the server side of the ACME protocol. It is published as free software with source code under the terms of version 2 of the Mozilla Public License (MPL).[13] It provides a RESTful API that can be accessed over a TLS-encrypted channel.

An Apache-licensed[14] Python certificate management program called *certbot* (formerly *letsencrypt*) gets installed on the client side (the web server of an enrollee). This is used to order the certificate, to conduct the domain validation process, to install the certificate, to configure the HTTPS encryption in the HTTP server, and later to regularly renew the certificate.[2][15] After installation and agreeing to the user license, executing a single command is enough to get a valid certificate installed. Additional options like OCSP stapling or HTTP Strict Transport Security (HSTS) can also be enabled.[10] Automatic setup initially only works with Apache and nginx.

Let's Encrypt issues certificates valid for 90 days. The reason given is that these certificates "limit damage from key compromise and mis-issuance" and encourage automation.[16] The official *certbot* client and most of the third-party clients allow automation of the certificate renewal.

Several third-party client implementations in several languages were created by the community.[17]

3. History

The Let's Encrypt project was started in 2012 by two Mozilla employees, Josh Aas and Eric Rescorla, together with Peter Eckersley at the Electronic Frontier Foundation and J. Alex Halderman at the University of Michigan. Internet Security Research Group, the company behind Let's Encrypt, was incorporated in May 2013.[18]

Let's Encrypt was announced publicly on November 18, 2014.[19]

On January 28, 2015, the ACME protocol was officially submitted to the IETF for standardisation.[20] On April 9, 2015, the ISRG and the Linux Foundation declared their collaboration.[1] The root and intermediate certificates were generated in the beginning of June.[6] On June 16, 2015, the final launch schedule for the service was announced, with the first certificate expected to be issued sometime in the week of July 27, 2015, followed by a limited issuance period to test security and scalability. General availability of the service was originally planned to begin sometime in the week of September 14, 2015.[21] On August 7, 2015, the launch schedule was amended to provide more time for ensuring system security and stability, with the first certificate to be issued in the week of September 7, 2015 followed by general availability in the week of November 16, 2015.[22] The cross-signature from IdenTrust is planned to be available when Let's Encrypt opens for the public.[5]

On September 14, 2015, Let's Encrypt issued its first certificate, which was for the domain helloworld.letsencrypt.org. On the same day, ISRG submitted its root program applications to Mozilla, Microsoft, Google and Apple.[23]

On October 19, 2015, the intermediate certificates became cross-signed by IdenTrust, causing all certificates issued by Let's Encrypt to be trusted by all major browsers.[4]

On November 12, 2015, Let's Encrypt announced that general availability would be pushed back and that the first public beta would commence on December 3, 2015.[24] The public beta ran from December 3, 2015[25] to April 12, 2016.[26]

3.1. Certificates Issued

Date	Certificates issued
March 8, 2016	**1 million**[27]
April 21, 2016	**2 million**[28]
June 3, 2016	**4 million**[29]
June 22, 2016	**5 million[*]**[30]
September 9, 2016	**10 million**[31]
November 27, 2016	
December 12, 2016	
June 28, 2017	**100 million**[32]
August 6, 2018	**115 million**[33]
September 14, 2018	**380 million**[34]

[*] Of which 3.8 million are unexpired and unrevoked. Their active certificates cover more than 7 million unique domains, in part due to support by large hosting companies.

References

1. Kerner, Sean Michael (April 9, 2015). "Let's Encrypt Becomes Linux Foundation Collaborative Project". QuinStreet Enterprise. //www.eweek.com/security/lets-encrypt-becomes-linux-foundation-collaborative-project.html.
2. Fabian Scherschel (November 19, 2014). "Let's Encrypt: Mozilla und die EFF mischen den CA-Markt auf" (in de). heise.de. //heise.de/-2460155.
3. Aas, Josh (June 4, 2015). "Let's Encrypt Root and Intermediate Certificates". https://letsencrypt.org/2015/06/04/isrg-ca-certs.html.
4. Aas, Josh (October 19, 2015). "Let's Encrypt is Trusted". https://letsencrypt.org/2015/10/19/lets-encrypt-is-trusted.html.
5. Reiko Kaps (June 17, 2015). "SSL-Zertifizierungsstelle Lets Encrypt will Mitte September 2015 öffnen" (in de). heise.de. //heise.de/-2714819.
6. Reiko Kaps (June 5, 2015). "Let's Encrypt: Meilenstein zu kostenlosen SSL-Zertifikaten für alle" (in de). heise.de. //heise.de/-2679600.
7. "Certificates". https://letsencrypt.org/certificates/.

8. Aas, Josh (August 13, 2015). "Elliptic Curve Cryptography (ECC) Support". Archived from the original on December 12, 2015. https://web.archive.org/web/20151212235713/https://community.letsencrypt.org/t/elliptic-curve-cryptography-ecc-support/34.
9. "Certificates". https://letsencrypt.org/certificates/.
10. Brook, Chris (November 18, 2014). "EFF, Others Plan to Make Encrypting the Web Easier in 2015". //threatpost.com/eff-others-plan-to-make-encrypting-the-web-easier-in-2015/109451.
11. "Draft ACME specification". https://github.com/ietf-wg-acme/acme/.
12. Barnes, Richard; Eckersley, Peter; Schoen, Seth; Halderman, Alex; Kasten, James (January 28, 2015). "Automatic Certificate Management Environment (ACME) draft-barnes-acme-01". Network Working Group. https://tools.ietf.org/html/draft-barnes-acme-01.
13. letsencrypt. "boulder/LICENSE.txt at master · letsencrypt/boulder · GitHub". Github.com. https://github.com/letsencrypt/boulder/blob/master/LICENSE.txt. Retrieved January 6, 2016.
14. letsencrypt (November 23, 2015). "letsencrypt/LICENSE.txt at master · letsencrypt/letsencrypt · GitHub". Github.com. https://github.com/letsencrypt/letsencrypt/blob/master/LICENSE.txt. Retrieved January 6, 2016.
15. Sanders, James (November 25, 2014). "Let's Encrypt initiative to provide free encryption certificates". CBS Interactive. //www.techrepublic.com/article/lets-encrypt-initiative-to-provide-free-encryption-certificates/.
16. Aas, Josh (November 9, 2015). "Why ninety-day lifetimes for certificates?". https://letsencrypt.org/2015/11/09/why-90-days.html.
17. "Let’s Encrypt - Documentation". https://letsencrypt.org/docs/client-options/.
18. Aas, Josh (November 18, 2014). "Let’s Encrypt | Boom Swagger Boom". Boomswaggerboom.wordpress.com. https://boomswaggerboom.wordpress.com/2014/11/18/lets-encrypt/. Retrieved January 6, 2016.
19. Joseph Tsidulko (November 18, 2014). "Let's Encrypt, A Free And Automated Certificate Authority, Comes Out Of Stealth Mode" (in en). crn.com. http://www.crn.com/news/cloud/300074840/lets-encrypt-a-free-and-automated-certificate-authority-comes-out-of-stealth-mode.htm.
20. History for draft-barnes-acme //datatracker.ietf.org/doc/draft-barnes-acme/history/
21. Josh Aas (June 16, 2015). "Let's Encrypt Launch Schedule". Let's Encrypt. https://letsencrypt.org/2015/06/16/lets-encrypt-launch-schedule.html. Retrieved June 19, 2015.
22. "Updated Let's Encrypt Launch Schedule". August 7, 2015. https://letsencrypt.org/2015/08/07/updated-lets-encrypt-launch-schedule.html.
23. Michael Mimoso. "First Let’s Encrypt Free Certificate Goes Live". Threatpost.com, Kaspersky Labs. https://threatpost.com/first-lets-encrypt-free-certificate-goes-live/114675/. Retrieved September 16, 2015.
24. "Public Beta: December 3, 2015". November 12, 2015. https://letsencrypt.org/2015/11/12/public-beta-timing.html.
25. "Entering Public Beta - Let's Encrypt - Free SSL/TLS Certificates". Let's Encrypt. December 3, 2015. https://letsencrypt.org/2015/12/03/entering-public-beta.html. Retrieved January 6, 2016.
26. "Let's Encrypt Leaves Beta". Archived from the original on April 15, 2016. https://web.archive.org/web/20160415173611/http://www.linuxfoundation.org/news-media/announcements/2016/04/let-s-encrypt-leaves-beta. Retrieved 17 April 2016.
27. Aas, Josh (March 8, 2016). "Our Millionth Certificate - Let's Encrypt - Free SSL/TLS Certificates". https://letsencrypt.org/2016/03/08/our-millionth-cert.html.
28. "Let's Encrypt Reaches 2,000,000 Certificates". 2016-04-22. https://www.eff.org/deeplinks/2016/04/lets-encrypt-reaches-2000000-certificates.
29. "Let's Encrypt Stats". June 5, 2016. https://letsencrypt.org/stats/.
30. "Progress Towards 100% HTTPS, June 2016". June 24, 2016. https://letsencrypt.org/2016/06/22/https-progress-june-2016.html.
31. Let's Encrypt [@letsencrypt] (September 9, 2016). "We’ve now issued more than 10 million certificates.". https://twitter.com/letsencrypt/status/774313572255932416.
32. "Milestone: 100 Million Certificates Issued - Let's Encrypt - Free SSL/TLS Certificates" (in en). https://letsencrypt.org/2017/06/28/hundred-million-certs.html.
33. "Let's Encrypt Root Trusted By All Major Root Programs" (in en). https://letsencrypt.org/2018/08/06/trusted-by-all-major-root-programs.html.

34. "Let's Encrypt on Twitter" (in en). Twitter. https://twitter.com/letsencrypt/status/1040650167647559680.