Let's Encrypt

FOR A BETTER INTERNET

2019 ANNUAL REPORT

LETTER FROM THE EXECUTIVE DIRECTOR

DEAR COMMUNITY AND SUPPORTERS,

Let’s Encrypt is dedicated to creating a more secure and privacy-respecting Web by issuing the digital certificates needed for sites to secure their network traffic. In 2019, we helped to secure an additional 34 million websites, bringing the total number of sites we service to 187 million. While doing so we made major investments in the security, reliability, and ease-of-use of our services.

We talk a lot about numbers at Let’s Encrypt because we measure so many things as part of our work, but my view of the organization is fundamentally human, so I’d like to highlight the work our leadership team has been doing this year.

Andrew Gabbitas leads our Site Reliability Engineering team, making sure our service is secure, reliable, and operated efficiently. Over the past year, Andrew has been focused on scaling to meet subscriber growth expectations and helping his team learn to perform even deeper automation of our infrastructure. Andrew’s team is obsessed with automation because automated systems are both more efficient and reliable. Automation is how we make sure the dollars entrusted to us by our donors go as far as possible.

Jacob Hoffman-Andrews leads our software engineering team, which is responsible for writing and maintaining our core certificate authority (CA) software. Jacob's team understands just about every nuance of how CA compliance and policy interacts with the real world and the complicated realities of the Web. They translate that knowledge into the software that powers the world's largest CA with an excellent security and compliance track record. This year they helped standardized the ACME certificate issuance and management protocol in IETF so that the entire ecosystem of CAs and certificate subscribers can benefit from a secure and reliable protocol.

"MY VIEW OF THE ORGANIZATION IS FUNDAMENTALLY HUMAN, SO I'D LIKE TO HIGHLIGHT THE WORK OUR LEADERSHIP TEAM HAS BEEN DOING THIS YEAR."

Sarah Gran leads our communications and fundraising team, which is responsible for how we engage with the Web community and funders. We need to make people aware of us as a resource and inspire them to give back if they're able. We also communicate to provide transparency. Our organization is trusted to perform critical security work for the Web, and people deserve to know why they should trust us.

Sarah's team has a knack for asking great questions so they can understand what our community and funders care about, and so they can communicate clearly and accurately about what we do. Over the past year, the response to our engagement efforts has been phenomenal. So far we've met most of our fundraising goals and our community translated our website into 11 additional languages!

Four years after we issued our first certificates, the percentage of encrypted page loads has grown from 39% to over 80%, globally. It's nearing 90% in the United States. I've tried to comprehend how much data about peoples' lives this has protected, and tried even harder to comprehend what that means in human or privacy terms. It's simply beyond my ability.

I'm incredibly proud to share in this report some of what our organization has accomplished in 2019. We couldn't have done it without amazing staff, community members, users, sponsors, grantmakers, and individual donors, all of whom I'd like to thank wholeheartedly.

Josh

JOSH AAS
EXECUTIVE DIRECTOR

LET'S ENCRYPT IS A

FREE

AUTOMATED

OPEN

NONPROFIT

CERTIFICATE AUTHORITY

BROUGHT TO THE WORLD BY

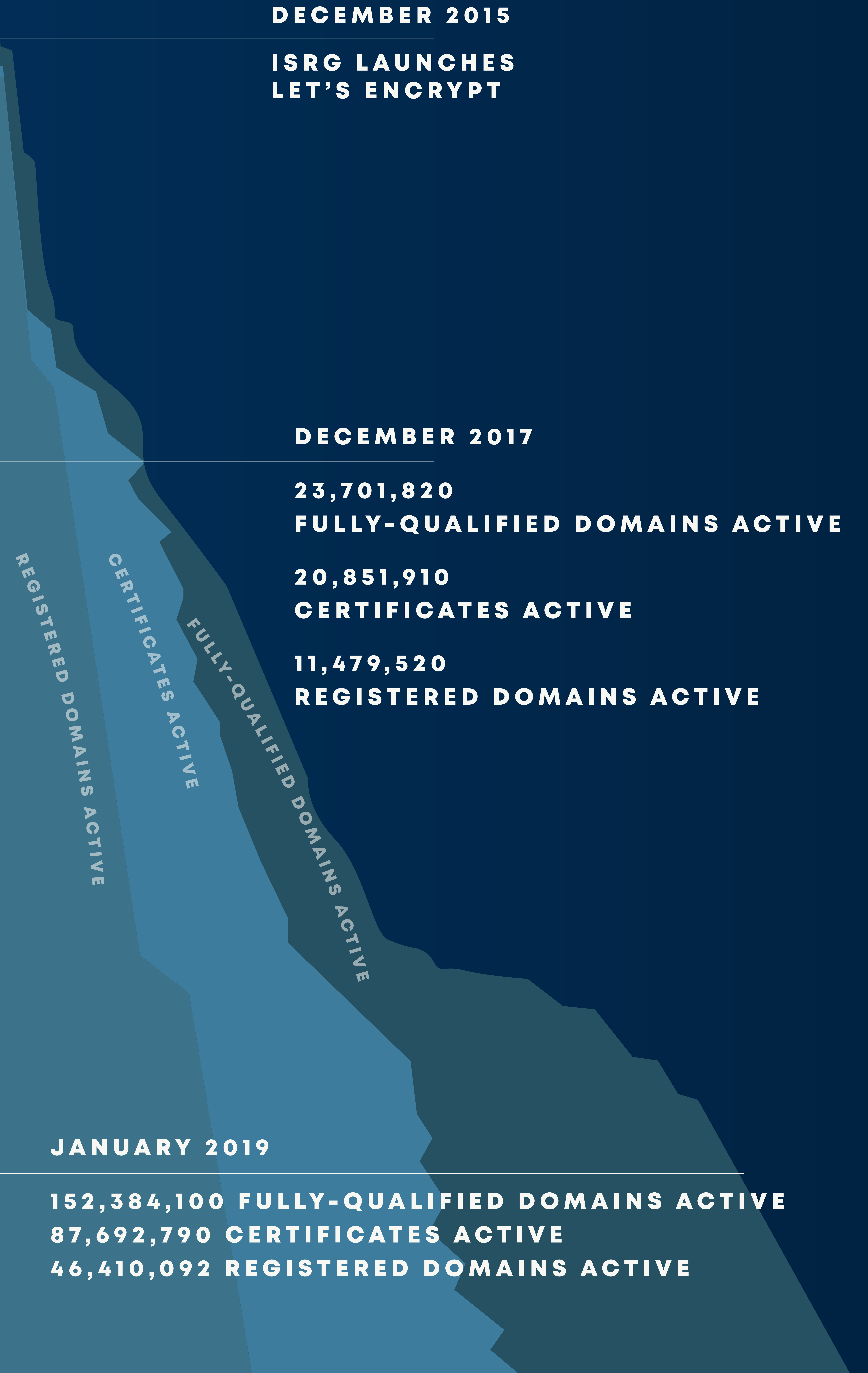
INTERNET SECURITY RESEARCH GROUP

In just four years, global HTTPS page loads have grown from 39% to more than 80% in 2019.

■ REGISTERED DOMAINS ACTIVE

■ CERTIFICATES ACTIVE

■ FULLY-QUALIFIED DOMAINS ACTIVE



DECEMBER 2015

ISRG LAUNCHES
LET'S ENCRYPT

DECEMBER 2017

23,701,820
FULLY-QUALIFIED DOMAINS ACTIVE

20,851,910
CERTIFICATES ACTIVE

11,479,520
REGISTERED DOMAINS ACTIVE

JANUARY 2019

152,384,100 FULLY-QUALIFIED DOMAINS ACTIVE
87,692,790 CERTIFICATES ACTIVE
46,410,092 REGISTERED DOMAINS ACTIVE

OUR GLOBAL COMMUNITY

Millions of companies, nonprofits, and public sector entities use Let's Encrypt certificates to create a secure connection with Web users all across the world.

WIKIMEDIA FOUNDATION: ESSENTIAL INFRASTRUCTURE FOR FREE KNOWLEDGE

The Wikimedia Foundation is the nonprofit that operates one of the world's most popular websites, Wikipedia. Through Wikipedia and other Wikimedia projects, the organization helps provide the essential infrastructure for free knowledge. Part of that infrastructure is looked after by Valentín Gutierrez, Traffic Security Engineer, who began using Let's Encrypt two years ago. "We chose Let's Encrypt because of automation, security, and the incredible support community. When we encounter any issue or question, the community responds within hours. We've seen growth in our use of Let's Encrypt certificates in that time, and look forward to expanding our work with Let's Encrypt in 2020," said Gutierrez.

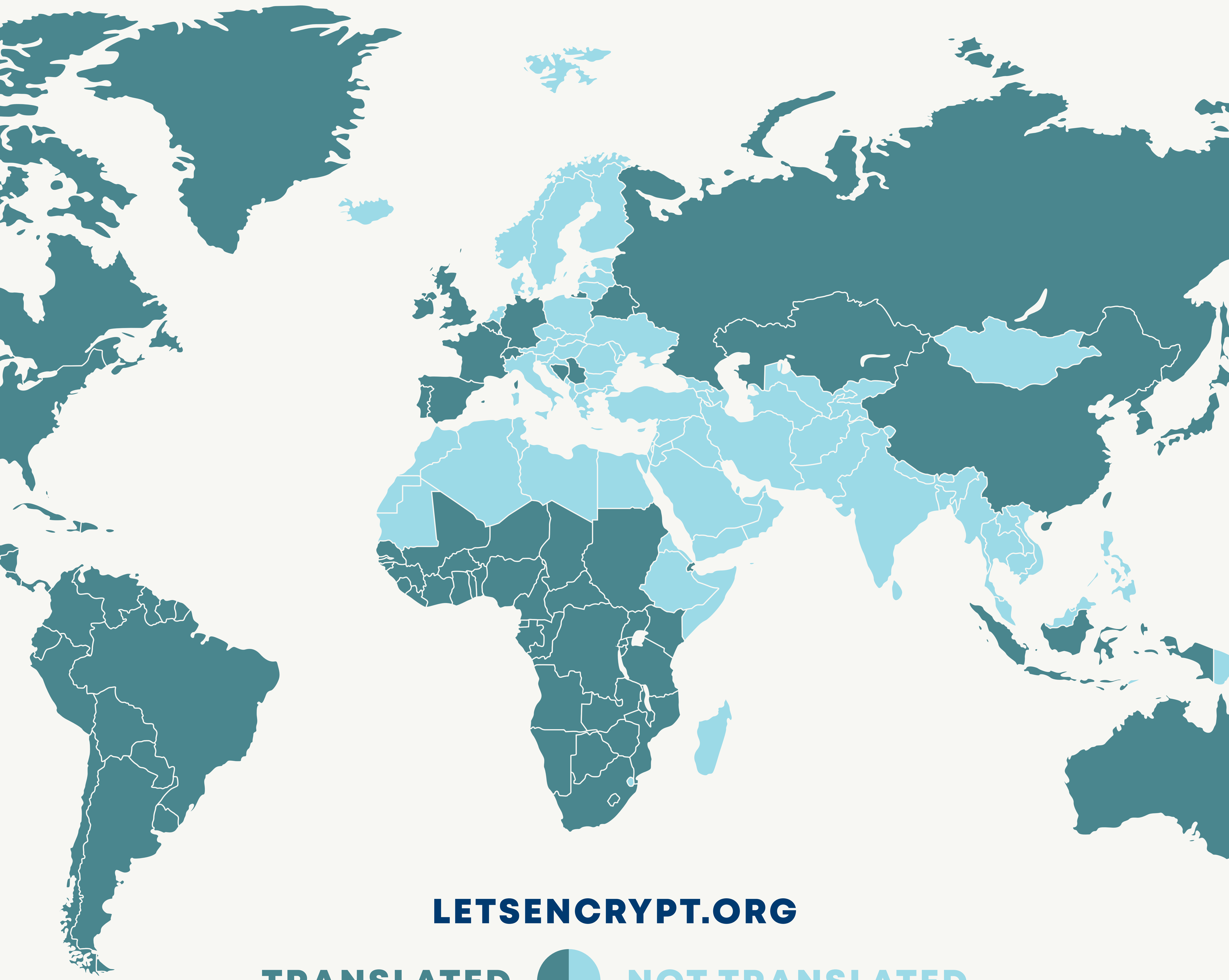
THE BAVARIAN GOVERNMENT: SECURING THE PEOPLE

The IT service center of the Bavarian Government, part of the Agency for Digitisation, High-Speed Internet, and Surveying (LDBV), is responsible for offering IT services across a variety of important local government departments. LDBV began using Let's Encrypt in 2019 to provide TLS certificates to secure the provisioning of about 1,500 applications, such as those for geographic surveying and property registration. "The main reason for our use of Let's Encrypt certificates was the increasing work required to renew 1,500 certificates for 2,800 DNS names every year. Since we now use Let's Encrypt certificates, these efforts are negligible," said Michael Doucha, Senior Systems Administrator.

IBM: PRIORITIZING HIGH VOLUME & LOW LATENCY

IBM's Cloud Certificate Manager is a secured repository for storing certificates and their associated private keys, and helps users manage certificate life cycles. More services like this are being developed as we see TLS adoption rise. The team developing this product decided to use Let's Encrypt as the first integrated certificate provider because high volume and low latency were top priorities. Customers are quickly getting a TLS certificate, and are alerted via Slack or a Webhook, enabling a CI/CD pipeline that has security built in.

HELP US REACH EVERYONE, EVERYWHERE



LETSENCRYPT.ORG

TRANSLATED ◐ NOT TRANSLATED

IN AT LEAST ONE OFFICIAL LANGUAGE OF THIS COUNTRY

> “LANGUAGE SHOULDN’T BE A BARRIER TO UNDERSTANDING HOW CERTIFICATE AUTHORITIES SUCH AS LET’S ENCRYPT WORK. WHEN I SAW I COULD HELP TO TRIGGER THE TRANSLATION, I DIDN’T HESITATE. NOW I’M THRILLED TO SEE SO MANY PEOPLE HELPING TO TRANSLATE, SO EVERYBODY CAN LEARN HOW TO USE LET’S ENCRYPT, AND I HOPE TO SEE MORE NEW LANGUAGES ARRIVING!”

TOM DELMAS
LET’S ENCRYPT
COMMUNITY LEADER

DO YOU KNOW HINDI, MALAY, OR ARABIC? THESE THREE LANGUAGES ARE TOP PRIORITIES. GET STARTED ON GITHUB TO HELP US IN THIS WORK.

OPEN SOURCE CONTRIBUTIONS IMPACT MILLIONS OF USERS

RICHARD “SHRED” KÖRBER

Richard “Shred” Körber has been interested in computers and coding since he was six years old. “I made my first programming steps on a Sinclair ZX-81 and ZX-Spectrum,” said Körber. “Later, I moved on to Linux, and learned about the advantages of open source software.” Körber has been working on open source projects since the 1990s when he was a part of the Commodore Amiga hacker and demo scene.

“I NEVER HAD THE FEELING OF BEING JUST A NERD WHO WANTS TO TAKE PART IN SERIOUS BUSINESS.”

Since then, Körber has authored over 30 open source projects, including a widely used ACME client. “I love the idea of open source software. Everyone can get involved in a software project and take part in improving it,” said Körber. “Writing my own open source software, and contributing to other open source projects, is my way to give back to the community.”

When Let’s Encrypt began issuing certificates in 2015, he saw the need for a

Java client for ACME. “When Let’s Encrypt started, the only available client was the official Let’s Encrypt client [now CertBot]. However, the way it worked didn’t really fit my needs, so I couldn’t use it. Thanks to the open ACME protocol, I could finish a first internal proof-of-concept implementation within a few days,” he said. “Then after publishing the source code on GitHub, I quickly got positive feedback and help from other developers. It seems that acme4j has filled a gap,” said Körber. It’s now used by organizations all over the world to help issue certificates.

Körber has been active in the Let’s Encrypt community since 2015, sharing his knowledge of a more secure Web with people around the world. “I have always felt like I am a welcome part of the Let’s Encrypt community” stated Körber, “When I asked for help, I always got help. When I had a comment or found a bug, I have always been taken seriously. I never had the feeling of being just a nerd who wants to take part in serious business.”

We certainly are thankful to have Körber in our community and maintaining acme4j. Because of his dedication to open source, people around the globe have a more privacy-respecting Web experience.

OUR COMMUNITY FORUM IN 2019

The welcoming and helpful community that exists on https://community.letsencrypt.org has helped millions of sites use HTTPS. From first-timer questions to interesting edge cases, the members of our community are quick and respectful in getting people the help they need.

13,158,487

PAGE VIEWS

31,106

POSTS

13,264

LIKES

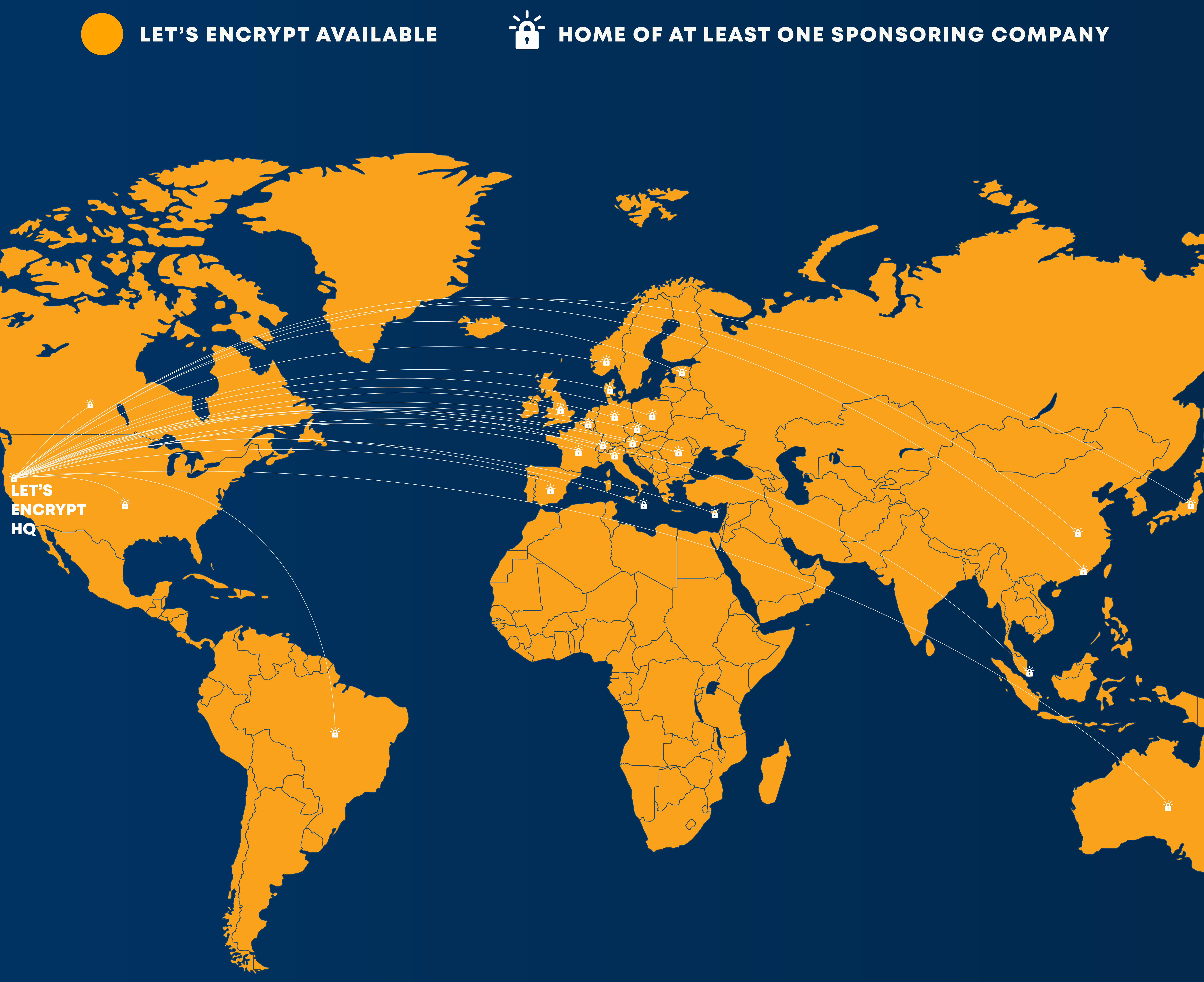
3,774

NEW USERS HELPED

1.8h

AVERAGE RESPONSE TIME

SERVING 187 MILLION WEBSITES

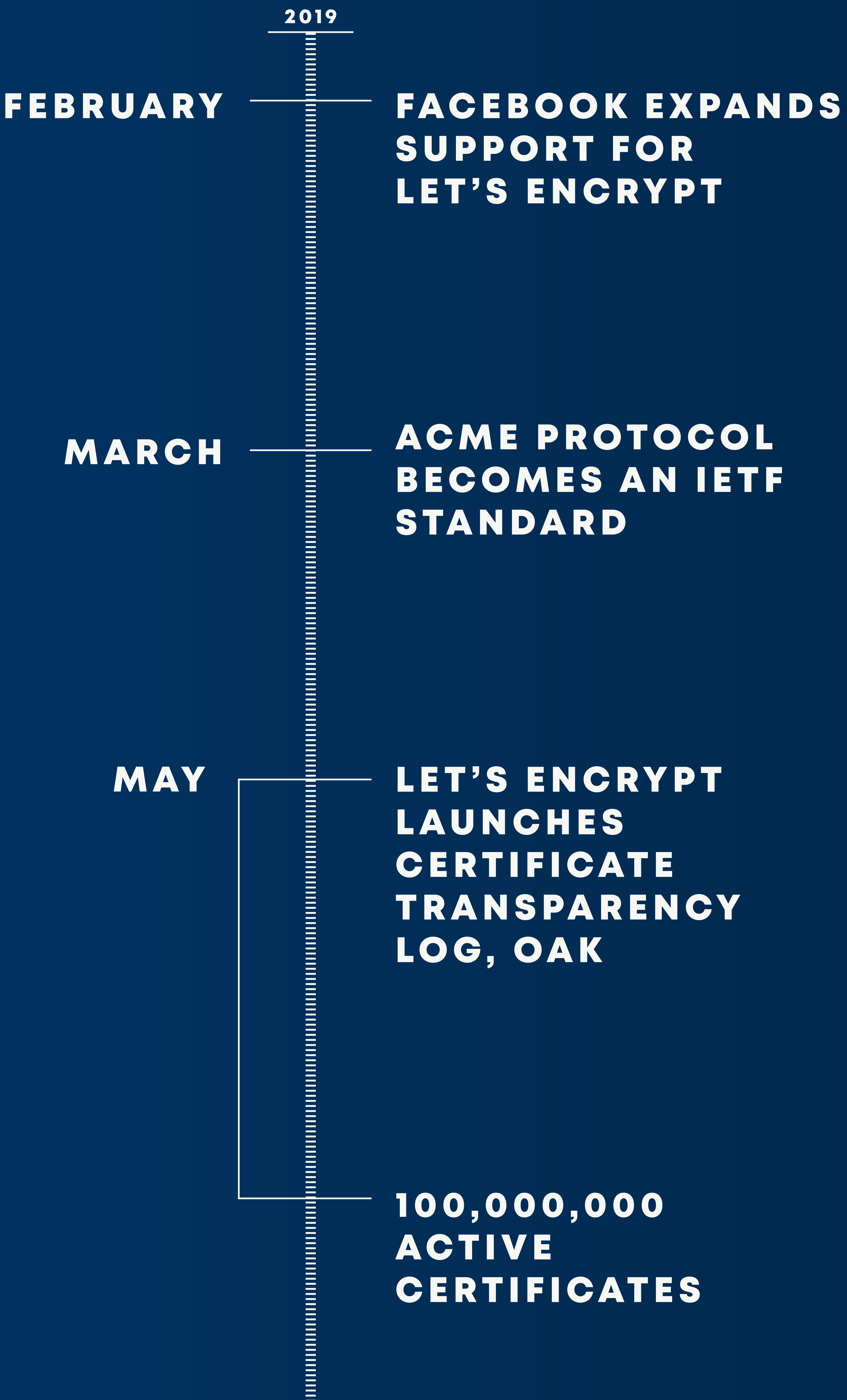

● LET'S ENCRYPT AVAILABLE
🔒 HOME OF AT LEAST ONE SPONSORING COMPANY
LET'S ENCRYPT HQ

In 2019, global HTTPS usage hit 80% of Web page loads for the first time in the history of the Internet.

50% of our sponsors are US-based, 50% are based outside the US.

A YEAR OF MILESTONES

2019 saw multiple key developments take place, from launching our Certificate Transparency Log, Oak, in May to reaching a milestone of 100 million active certificates the very same month.



2019

FEBRUARY — FACEBOOK EXPANDS SUPPORT FOR LET'S ENCRYPT

MARCH — ACME PROTOCOL BECOMES AN IETF STANDARD

MAY — LET'S ENCRYPT LAUNCHES CERTIFICATE TRANSPARENCY LOG, OAK

100,000,000 ACTIVE CERTIFICATES

JUNE	NEW RECORD: 1.7M CERTIFICATES ISSUED IN ONE DAY
SEPTEMBER	GLOBAL HTTPS 80% OF WEB PAGE LOADS
OCTOBER	CT LOG ACCEPTED BY CHROMIUM
EARLY 2020	**ONE BILLION** CERTIFICATES ISSUED

AUTOMATION AT WORK: TWO PERSPECTIVES

MEET ROLAND

Before the conception of Let’s Encrypt, HTTPS was considered to have a relatively high barrier to entry. In part this was due to the cost, but there was also significant complexity with both procuring and installing a TLS certificate.

In 2015, Electronic Frontier Foundation (EFF) did an experiment that showed that it would take an experienced systems administrator anywhere between one and three hours to get a certificate for a website and install it on a webserver. Given each complex process that was required each time a new certificate was needed, website owners would often leave renewals to the last moment, often resulting in expired or misconfigured certificates and HTTPS warning fatigue for users.
When I started working on the Let’s Encrypt project in 2015, the prospect of using software and automation to hide this complexity was intriguing. Over the course of four years, I worked with a community of developers to create and standardize the Automated Certificate Management Environment (ACME) protocol.

ACME not only moved the complexity of getting certificates away from users and into the realm of software, it enabled certificate retrieval, installation, and renewal to be easily automated behind the scenes. Instead of a user needing to remember to complete a complex process, they can set up one of many available clients which handles the process transparently for them. This has led not only to considerably more people feeling confident enabling HTTPS for their websites, but also a significant reduction in the prevalence of expired and misconfigured certificates.

We are slowly moving towards complete automation that is nearly completely hidden from the user. For instance, Apache has built-in ACME clients which simply require a user to indicate they want to enable HTTPS. Soon, hopefully, most users will simply be able to flip a switch and enable HTTPS, a far cry from the days of spending hours on a hit-or-miss process which may or may not result in success.

ROLAND
DEVELOPER

AUTOMATION AT WORK: TWO PERSPECTIVES

MEET JILLIAN

I work at Let’s Encrypt as a Site Reliability Engineer (SRE). My responsibility is to help maintain and improve the infrastructure that runs Let’s Encrypt. This includes everything from upgrading hardware, releasing new versions, responding to incidents, and improving automation throughout the whole environment. It’s a considerable amount of work for a six person team but is made possible through our commitment to automation that saves time, prevents human error, provides space for people to focus on other projects, and allows tasks get done in a consistent and auditable way.

I started working at Let’s Encrypt in fall of 2015. Back then, our team was much smaller and preparing for the Let’s Encrypt public beta before our launch. We knew that automation would be a fundamental part of how we maintained and grew our infrastructure. Initially, we started with basic automation using Saltstack to configure new hosts and quickly deploy updated versions of the Boulder software. Our goal was always to have more automation inline with the current DevOps trend of “automate your job away.”

In 2018, our team transitioned from a DevOps to an SRE practice, and it enabled us to look at our infrastructure with an even greater focus on automation. Our expanded software engineering skills allowed us to create new tools and workflows. We now work more closely with the developer team and it opens up different conversations about small places where we can automate and how we can do it.

For example, I worked on a project to export data directly from the database so it could be processed for graphs on the Let’s Encrypt stats page. I had paired programming sessions with a developer to get to an automated solution faster. The result was a small program that saves time by automatically exporting and processing the data so SREs don’t have to run and wait for queries to complete and can work on other projects.

I came away from this project with a sense that while automating everything is daunting, the pieces are not hard. Our audit requirements will always mean some human review in certain places. We won’t automate our jobs away but we can reduce places where manual work bogs us down so we can instead focus on improving our service.

JILLIAN
SITE RELIABILITY ENGINEER

MEET OAK, OUR CERTIFICATE TRANSPARENCY LOG

This May, we announced the Let’s Encrypt Certificate Transparency (CT) Log, called Oak.

We began work on this project in 2017, when we realized we were going to be significant contributors to the certificate ecosystem. Ensuring the reliability of CT is paramount, since the submission of every certificate to at least two logs is a requirement by Chromium.

Our team collaborated with people from other CAs, log operators, cloud providers, and community members to develop a log that is specifically built with Internet scale in mind while adhering to uptime requirements.

We’d like to thank Sectigo and AWS for providing support to offset a large portion of the cost of running this log.

CT SPONSORED IN PART BY:

SECTIGO aws

WHY CERTIFICATE TRANSPARENCY IS USEFUL TO EVERYONE

Your computer trusts certain certificate authorities. Make sure they are doing what they are supposed to be and nothing more.

See all of the certificates issued for your domains. Know if something was issued without your knowledge or consent.

Allow your OS and browser to reject certificates that aren't publicly logged. Certificates that someone is trying to hide are probably bad news.

HONORING THE FOUNDATION CELEBRATING THE FUTURE

The work of Let's Encrypt is built upon decades of innovation in cryptography and security that reach back to the early days of the Web.

In 2019, we had multiple opportunities to be with some of these leaders who laid the foundation for a better Internet via our work at Let's Encrypt.

In May, Josh Aas attended the Marconi Society Awards and gave a toast celebrating Taher Elgamal and Paul Kocher, the creators of the SSL protocol. Above, Let's Encrypt at the 2019 Marconi Society Awards Dinner. From left to right: Sigrid Cerf; Josh Aas; Whit Diffie; Vint Cerf; Jennifer Granick, ISRG Board Member; Dorothie Hellman; Marty Hellman.

In August, Let's Encrypt was recognized by O'Reilly with the Most Impact Award at the Open Source Awards. We are proud to be recognized as leaders of our field, and grateful for the leaders who laid the foundation.

Below, Let's Encrypt staff Sarah and Jillian accepting the 2019 O'Reilly Open Source Award for Most Impact.

FOR FOUNDING PARTNER CISCO, SPONSORSHIP MEANS IMPACT AT A GLOBAL SCALE

ALISSA COOPER
CISCO FELLOW
PLATINUM SPONSOR

Security is a core part of everything we do at Cisco. As a founding partner of Let’s Encrypt, we have been pleased to see the organization make such a large impact in a short period of time. We are also happy to have been a part of this growth. We have leveraged Let’s Encrypt certificates in several of our products to enable secure services to scale seamlessly and to help make our products secure by default.

“LET’S ENCRYPT HAS HELPED BUILD CONFIDENCE THAT OUR CONTRIBUTIONS ARE HAVING A HIGH IMPACT.”

ISRG’s streamlined, careful approach to running Let’s Encrypt has helped build confidence that our contributions are having

a high impact. It is impressive that Let’s Encrypt can run one of the world’s largest CAs, with industry-leading security practices, while sticking to a budget that makes a sponsorship-based model possible.

We have also been very pleased to see the impact that Let’s Encrypt has had on open standards. ISRG’s leadership in the IETF ACME working group and its work with CA peers and other stakeholders have helped improve the security of the whole Web PKI and all the services that rely on it.

We look forward to continuing to partner with ISRG to make security an intrinsic part of the Internet and we invite others who share this goal to join us.

ALISSA COOPER
CISCO FELLOW

“LET’S ENCRYPT’S VISION FOR MAKING THE INTERNET MORE SECURE AND HTTPS ADOPTION EASIER IS ONE THAT WE BELIEVE CAN’T GO UNAPPRECIATED.”

BEN DOWLING
IPINFO FOUNDER
SILVER SPONSOR

OUR SPONSORS

PLATINUM

moz://a · CISCO · EFF · OVHcloud

chrome · Internet Society · facebook

GOLD

IdenTrust part of HID Global · FORD FOUNDATION

SILVER

Akamai · AUTOMATTIC · ALA American Library Association · shopify · cyon

infomaniak · HOSTPOINT · SiteGround · sucuri · VULTR

PlanetHoster · 云片 YunPian.com · fastly · 3CX · SQUARESPACE

HawkHost · thebestvpn · JIMDO · VTEX · UptimeRobot

DigitalOcean · zendesk · netlify · HOSTPAPA · PANTHEON Website Management Platform · dnsimple

時雨堂 · Discourse · driving-tests.org · SAKURA internet · DuoCircle

ise · privateinternetaccess always use protection · brave · ServerPilot · domainnameshop · easy website, easy hosting easyname

UNRAID · KEENETIC · Rainway · HAPROXY · datto · AXIOM

Livesport · ProPrivacy · nazwa.pl · clever cloud · render · ipinfo.io

ipinfo.io · GreenGeeks WEB HOSTING · Red Hat · NABU CASA · IBM · GitHub

umbraco · THE BEST RUN SAP · verizon digital media services · mongoDB · HOSTING REVIEW · HEROKU

SNIPE-IT OPEN SOURCE ASSET MANAGEMENT · TOP10VPN · WiX.com · Engine Forex · ZEIT · codeinwp

smallstep

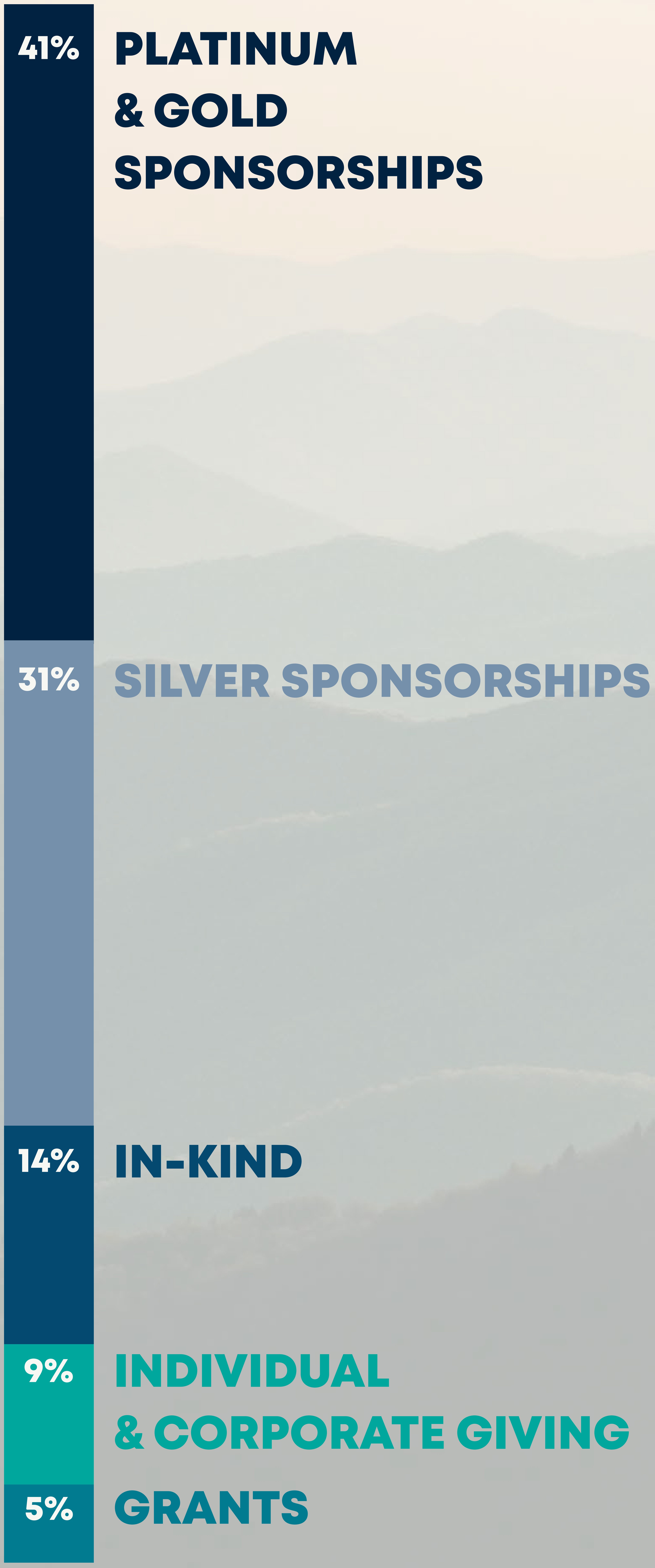
OUR FUNDING

ISRG, the organization behind Let’s Encrypt, is committed to thoughtful and efficient financial stewardship, operating on an annual budget of $3.6 million.

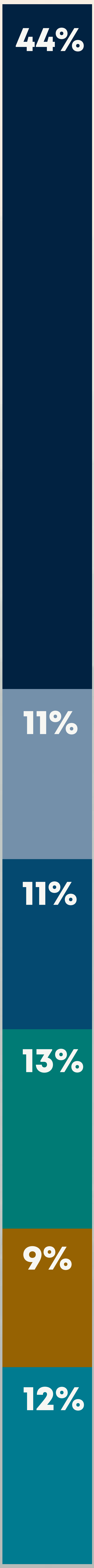
We have received successful audits each year from an independent auditing firm and work hard to ensure our impact scales while our expenses remain reasonable. We are deeply thankful to everyone who contributed in 2019 to make this Internet-scale change possible.

Percentages below are representative of 2019 data through September 30, 2019.

FUNDING SOURCES



EXPENSE BY ACTIVITY



CA INFRASTRUCTURE MAINTENANCE & IMPROVEMENT
Staff, IT Infrastructure, Security & Compliance Audits

CA SOFTWARE MAINTENANCE & IMPROVEMENT Staff, Hosting

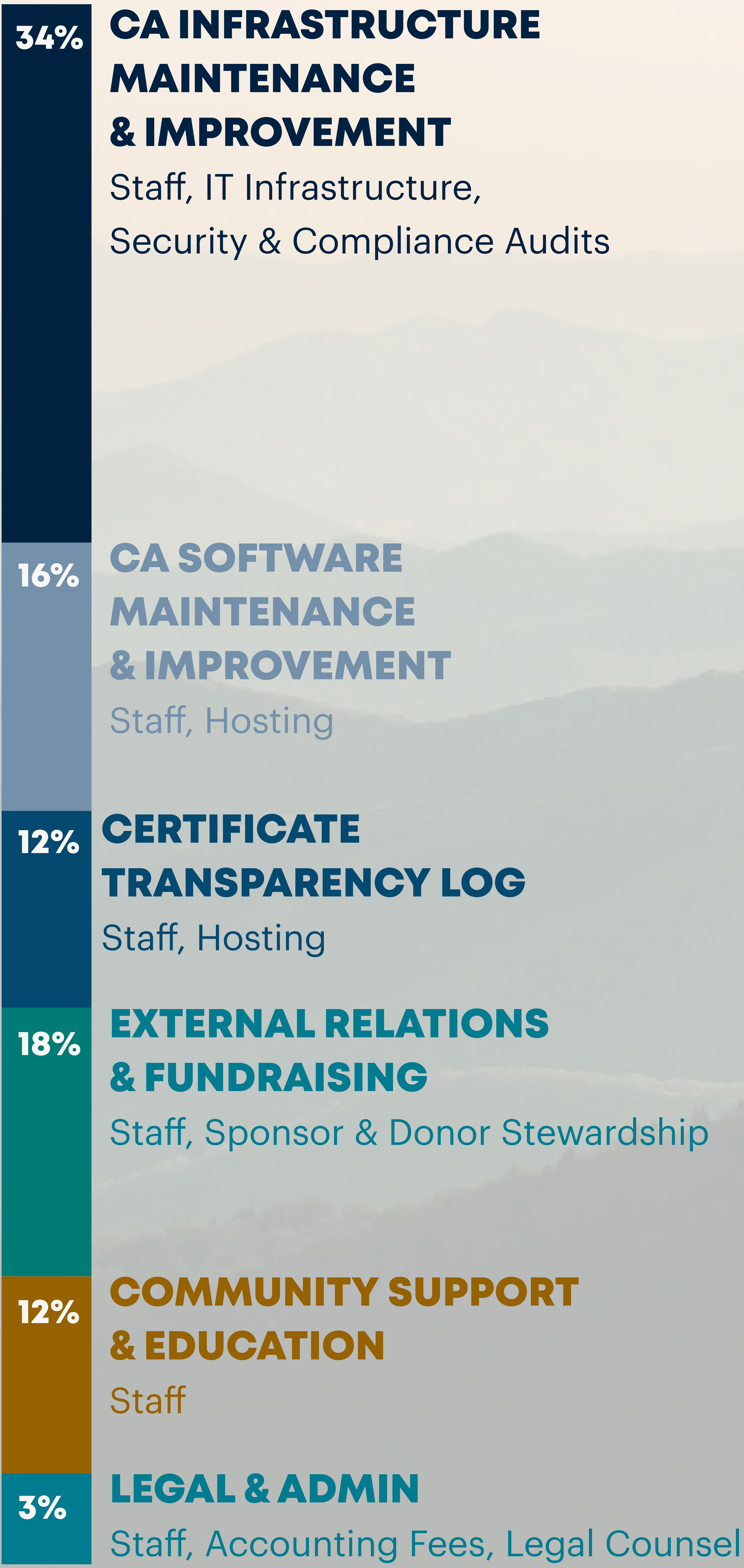
CERTIFICATE TRANSPARENCY LOG
Staff, Hosting

EXTERNAL RELATIONS & FUNDRAISING
Staff, Sponsor & Donor Stewardship

COMMUNITY SUPPORT & EDUCATION
Staff

LEGAL & ADMIN
Staff, Accounting Fees, Legal Counsel

% OF STAFF TIME



34% **CA INFRASTRUCTURE MAINTENANCE & IMPROVEMENT**
Staff, IT Infrastructure, Security & Compliance Audits

16% **CA SOFTWARE MAINTENANCE & IMPROVEMENT**
Staff, Hosting

12% **CERTIFICATE TRANSPARENCY LOG**
Staff, Hosting

18% **EXTERNAL RELATIONS & FUNDRAISING**
Staff, Sponsor & Donor Stewardship

12% **COMMUNITY SUPPORT & EDUCATION**
Staff

3% **LEGAL & ADMIN**
Staff, Accounting Fees, Legal Counsel

BOARD OF DIRECTORS

This great group of people serve as the governing body of ISRG. Our board formally meets quarterly, though they provide insight throughout the year as needs arise for our organization.

AANCHAL GUPTA
FACEBOOK

ALEX POLVI
RED HAT

CHRISTINE RUNNEGAR
INTERNET SOCIETY

JENNIFER GRANICK
AMERICAN CIVIL LIBERTIES UNION

J. ALEX HALDERMAN
UNIVERSITY OF MICHIGAN

JOSH AAS
ISRG

LAURA THOMSON
MOZILLA

MAX HUNTER
ELECTRONIC FRONTIER FOUNDATION

PASCAL JAILLON
OVH CLOUD

RICHARD BARNES
CISCO

Organizations listed for identification purposes only.

TECHNICAL ADVISORY BOARD

The Technical Advisory Board partners directly with Let's Encrypt leadership, staff, and each other to help inform important technical decisions for our organization. We value the breadth and depth of this group's expertise as we build a better Web!

Rich Salz (Akamai)
Joe Hildebrand (Mozilla)
Jacob Hoffman-Andrews (EFF)
Yueting Lee (Facebook)
J.C. Jones (Mozilla)
Russ Housley (Independent)
Ryan Hurst (Google)
Stephen Kent (Independent)
Karen O'Donoghue (Internet Society)
Ivan Ristic (Independent)

WE'RE BUILDING A BETTER INTERNET

Thanks to an incredible group of staff, community members, users, sponsors, grantmakers, and individual donors, Let's Encrypt is building a better Internet so that everyone, everywhere can benefit from a more secure and privacy-respecting Web.

SUPPORT OUR WORK

THANKS TO THESE PHOTOGRAPHERS

Photos by Annie Spratt, Antoine Rault, Eric Weber, Ivana Cajina, Paul Earle, Ruslan Bardash, and Tim van Cleef on Unsplash.

ISRG Internet Security Research Group

Let's Encrypt