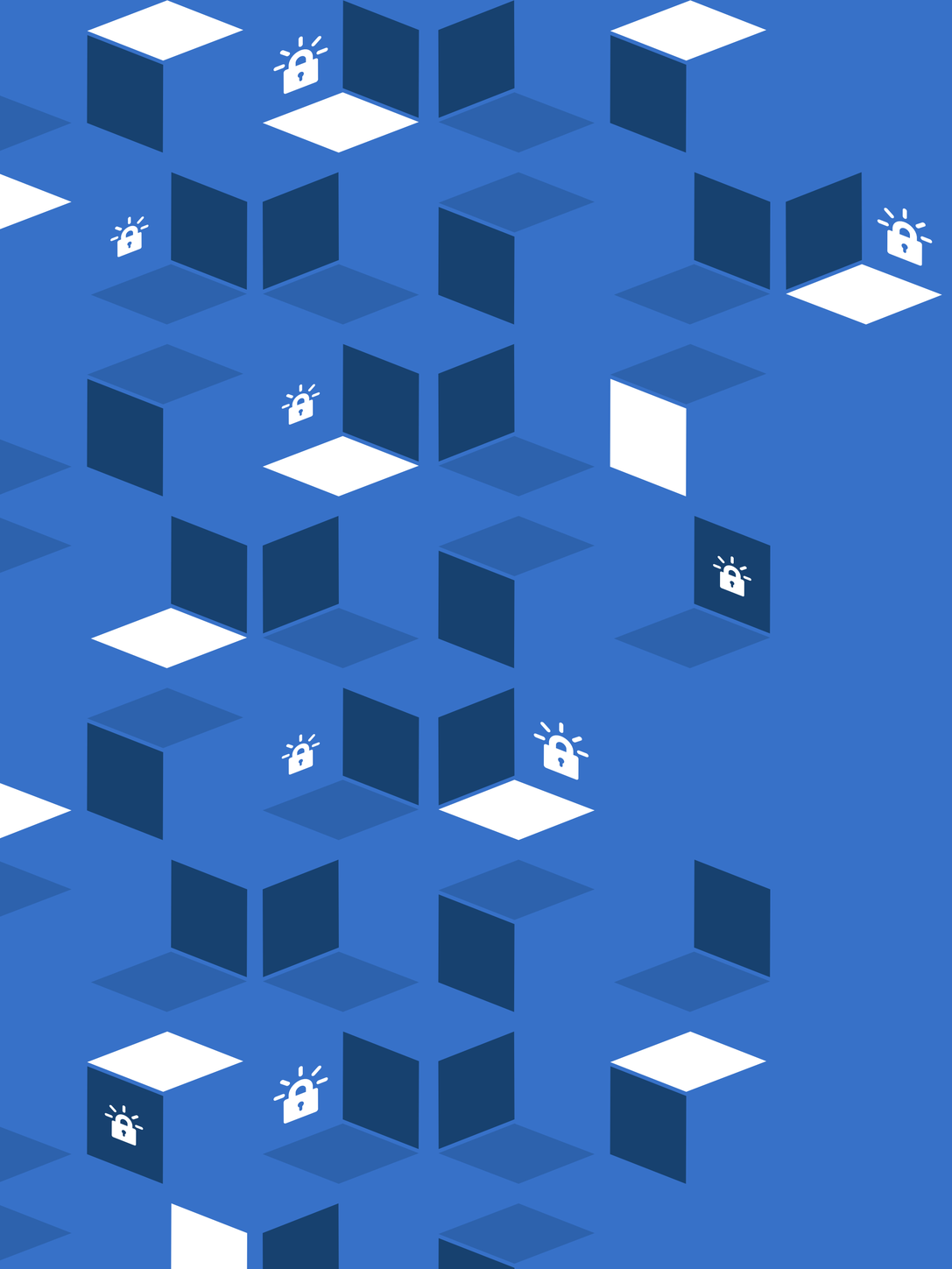


ISRG Internet Security Research Group

FOR A BETTER INTERNET

2020 ANNUAL REPORT

CONTENTS

OUR WORK & THE ROAD AHEAD

A NOTE FROM OUR EXECUTIVE DIRECTOR

ISRG's first project, Let's Encrypt, has been wildly successful. We're now helping to secure more than 225 million websites and the Web is making great progress towards 100% HTTPS. We've put in a lot of hard work and dealt with some challenges along the way, but at a high level the outlook is quite sunny. I'm incredibly proud to share in this report some of what our organization has accomplished in 2020...

While I'm deeply appreciative of being in this position today, I don't let it distract me, or our fantastic Board of Directors, from thinking diligently about the risks on the road ahead. A big part of our job is to look into the future, see threats and challenges, and prepare to face them as best we can. I'm sometimes asked what I view as the biggest threat to our organization and our ability to pursue our mission and my answer is simple: being taken for granted.

When digital security and privacy is your goal, ease of use has to be your focus. When we examine why real world systems aren't secure, it usually isn't because we don't have the technological means to secure them. The problem is almost always that the solutions are not easy enough to use, either for implementers or consumers.

WHEN YOUR STRATEGY AS A NONPROFIT IS TO GET OUT OF THE WAY, TO OFFER SERVICES THAT PEOPLE DON'T NEED TO THINK ABOUT, YOU'RE RUNNING A REAL RISK THAT YOU'LL EVENTUALLY BE TAKEN FOR GRANTED.

HTTPS has been around since the mid-90s but uptake was abysmally slow because SSL/TLS certificates weren't easy to get or manage. Let's Encrypt made getting and managing certificates easy and as a result HTTPS adoption rates shot up. Critically, the answer wasn't to get people to think more about their certificates—we needed to make it possible for people to spend much less time thinking about certificates. Ideally we'd be invisible—server software should just get and manage certificates automatically.

Our next project after Let's Encrypt is going live shortly: ISRG Prio Services. It's a system for collecting digital metrics that allows organizations to collect the information they need without any entity having the ability to access any individual user's data. Much like Let's Encrypt, it protects people without them having to know anything about it.

Despite 2020 being a year of unprecedented, global challenges, ISRG is well positioned for the years ahead. Our current momentum is possible through new major in-kind donations, nearly 90% of our existing sponsors renewing their support for 2020, funding from the Ford Foundation and the Bill & Melinda Gates Foundation, and by welcoming new major sponsors, including AWS, Thales, and Avast.

When your strategy as a nonprofit is to get out of the way, to offer services that people don't need to think about, you're running a real risk that you'll eventually be taken for granted. There is a tension between wanting your work to be invisible and the need for recognition of its value. If people aren't aware of how valuable our services are then we may not get the support we need to continue providing them.

How are we going to mitigate this risk? The most important thing we can do is continue to communicate effectively with people who are in a position to understand our work and support it. The most important things you can do as a supporter include being an advocate for your company sponsoring us, making an individual donation, or going over this annual report with a few people that you think should know more about us.

On behalf of the hundreds of millions of benefiting from Let's Encrypt around the world and our team of 16 people dedicated to this work, thank you for your support.

JOSH AAS
EXECUTIVE DIRECTOR

IN MANY WAYS,

ISRG has come in and made it really easy to have access to encryption, but now that's the expectation. People expect it to be easy and to be there, and there will be a decreasing visibility in to how that works because Let's Encrypt has done such a good job of obviating the need to know how that works.

In many ways that success is also the new challenge. I am happy to work on making sure that ISRG and Let's Encrypt remain viable and that ISRG is ready to tackle some of our next challenges."

DAVID NALLEY
ISRG BOARD OF DIRECTORS
PRINCIPAL, OPEN SOURCE
STRATEGY & MARKETING
AMAZON

WELCOME TO THESE NEW SUPPORTERS

We're proud to call 94 organizations sponsors and funders to ISRG and Let's Encrypt. These are the organizations we've welcomed into the fold this year.

THE INTERNET CALAMITY THAT WASN'T

A STORY OF REMEDIATION AND RESPONSIVENESS

That's what WIRED called our remediation of a bug that we became aware of in early March of this year. The security implications of this bug were relatively limited: Our certificate authority (CA) software, Boulder, checks for CAA records at the same time it validates a subscriber's control of a domain name. In some cases, it is supposed to do this check two times, but...

we learned that it was only checking once. In theory, this could mean that a subscriber could change their CA preference from including Let's Encrypt to excluding us for issuance, but we

WE DETERMINED THERE WERE MORE THAN THREE MILLION NON-COMPLIANT CERTIFICATES, ABOUT 2.6% OF OUR TOTAL ACTIVE CERTIFICATES.

wouldn't know that and issue a certificate anyway because we skipped the second check.

As soon as we discovered the bug, we turned off issuance, fixed it, and resumed our service. This remediation took the team just two hours and 14 minutes. We determined there were more than three million non-compliant certificates, about 2.6% of our total active certificates.

Staff worked tirelessly to identify and communicate with affected subscribers. Issues like this are never pleasant, but bugs are a reality in the software world and we work hard to make sure we're prepared to respond with speed and transparency. In less than 48 hours, our users and large integrators were able to replace over 1.7M certificates. That is an amazing turn around time for such a volume and a testament to automation and coordination. Many readers of this report played a hand in this effort and our gratitude for your work persists. After those initial 48 hours, we tracked the replacement of the remaining certificates over the following weeks until all certificates were replaced before being revoked.

Our focus on automation allowed us, and our subscribers, to make great progress in a short amount of time. We also learned a lot about how we can do even better in the future. ISRG leadership spent much of 2020 analyzing our processes and infrastructure to identify opportunities for a better response the next time a bug emerges. We look forward to sharing the details of this work in the coming months.

“THE INTRICACIES OF INTERNET INFRASTRUCTURE ARE GENERALLY IGNORED UNTIL SOMETHING GOES TERRIBLY WRONG. THIS TIME, THOUGH, IT’S USEFUL TO REFLECT ON WHAT WENT RIGHT. FOR ONCE, THE STORY IS THAT NOTHING BROKE.”

WIRED

ELIMINATING BARRIERS

TWO NEW PRIVACY & SECURITY INITIATIVES

This year, we've taken the initial steps beyond running the world's largest certificate authority, Let's Encrypt, to expand upon our mission of removing barriers to secure communication over the internet. This work has us focused on two projects: building a privacy-respecting system, ISRG Prio Services, for the collection of application metrics, and funding the work to move critical components of the ubiquitous software curl to memory safe code.

INTRODUCING ISRG PRIO SERVICES FOR PRIVACY RESPECTING METRICS COLLECTION

Applications such as web browsers, mobile applications, and websites generate metrics. Normally they would just send all of the metrics back to the application developer, but with Prio, applications split the metrics into two anonymized and encrypted shares and upload each share to different processors that do not share data with each other. This way only minimal information about the original metrics is revealed to either processor. Each processor then aggregates its shares into a partial sum. The partial sums can then be combined into a final aggregation, permitting useful statistics over the whole body of metrics while revealing minimal information about individual users. To learn more about the foundations of Prio, we recommend reading the Prio research paper by Henry Corrigan-Gibbs and Dan Boneh of Stanford University.

We have been researching Prio technology for some time because the privacy provided by this service can deliver significant benefits to the public. Application end-users have little control over the metrics that are collected about their application usage and how that information is used by developers. When applications use systems like ISRG's Prio Services, end-users won't have to just trust that they are safe from an attacker stealing and disclosing their information, or a company selling their personal data, or a government collecting their information for mass surveillance. By offering low-cost and easy-to-use cryptographic privacy protection for user metrics, ISRG will be taking a significant step to protect the general public from privacy violations. It is our hope that privacy respecting metrics collection will become an expectation for application developers. We are excited to offer this service to lead the way.

ISRG will operate Prio data share processors as a service to facilitate a subscriber's private metrics collection system. Our Site Reliability Engineering team maintains our open source data share processor and operates a 24/7 oncall schedule to ensure it functions smoothly.

Subscribers to ISRG's Prio Services are responsible for getting a second data share processor which implements the same protocol as ours, as well as sharing, encrypting, and uploading metrics from their applications to the data share processors and assembling the final aggregation.

We believe we will be the first organization to operate Prio services in a production capacity.

We'd like to thank Dan Boneh and Henry Corrigan-Gibbs for their incredible work developing the Prio idea and system. We'd also like to thank the people at Mozilla Firefox who have begun to experiment with using Prio for Firefox and sharing their experience.

ADDRESSING ONE OF THE BIGGEST THREATS TO INTERNET SECURITY

Memory safety vulnerabilities represent one of the biggest threats to Internet security. As such, we at ISRG are interested in finding ways to make the most heavily relied-upon software on the Internet memory safe. We are working with Daniel Stenberg, author of ubiquitous curl software and WolfSSL, to make critical parts of the curl codebase memory safe.

ISRG is funding Daniel to work on adding support for Hyper as an HTTP back-end for curl. Hyper is a fast and safe HTTP implementation written in Rust.

At the same time, ISRG engineers will add support for Rustls as a TLS back-end for curl. Rustls is a safe implementation of TLS, including certificate verification and the network protocol written in Rust. It has been audited and we suggest reading the conclusions on page 11 of the report if you want to get even more excited about Rustls.

At first the memory-safe HTTP and TLS backends will be opt-in. We will work with Daniel and various partners to make sure they are extensively tested, and if all goes well the plan is for the memory safe back-ends to become the default. By making the most frequently used networking code in curl memory safe by default we'll better protect the billions of people who rely on systems using curl.

ISRG IS FUNDING DANIEL STENBERG, AUTHOR OF CURL SOFTWARE, TO MAKE CRITICAL PARTS OF THE CURL CODEBASE MEMORY SAFE

Users who need to continue using the unsafe C back-ends for whatever reason will be able to continue doing so by building curl with the C back-ends enabled.

We'd like to thank Daniel for his willingness to be a leader on this issue. It's not easy to make such significant changes to how wildly successful software is built, but we've come up with a great plan and together we're going to make one of the most critical pieces of networking software in the world significantly more secure. We think this project can serve as a template for how we might secure more critical software, and we're excited to learn along the way.

We'd also like to thank everyone involved in creating Hyper, Rustls, and the libraries they depend on. In particular we'd like to thank Sean McArthur for his work on Hyper, Joseph Birr-Pixton for his work on Rustls, and Brian Smith for his work on Ring (which Rustls uses).

ESTABLISHING A NEW ROOT

MAJOR STEPS FORWARD FOR LET'S ENCRYPT

On Thursday, September 3rd, 2020, Let's Encrypt issued six new certificates: one root, four intermediates, and one cross-sign. These new certificates are part of our larger plan to improve privacy on the web, by making ECDSA end-entity certificates widely available, and by making certificates smaller. Given that we issue 1.5 million certificates every day, what makes these ones special? Why did we issue them? How did we issue them? Let's answer these questions, and in the process take a tour of how Certificate Authorities think and work.

THE BACKSTORY

Every publicly-trusted certificate authority (such as Let's Encrypt) has at least one root certificate which is incorporated into various browser and operating system vendors' (e.g. Mozilla, Google) trusted root stores. This is what allows users who receive a certificate from a website to confirm that the certificate was issued by an organization that their browser trusts. But root certificates, by virtue of their widespread trust and long lives, must have their corresponding private key carefully protected and stored offline, and therefore can't be used to sign things all the time. So every certificate authority (CA) also has some number of "intermediates", certificates which are able to issue additional certificates but are not roots, which they use for day-to-day issuance.

For the last five years, Let's Encrypt has had one root: the ISRG Root X1, which has a 4096-bit RSA key and is valid until 2035.

Over that same time, we've had four intermediates: the Let's Encrypt Authorities X1, X2, X3, and X4. The first two were issued when Let's Encrypt first began operations in 2015, and were valid for 5 years. The latter two were issued about a year later, in 2016, and are also valid for 5 years, expiring about this time next year. All of these intermediates use 2048-bit RSA keys. In addition, all of these intermediates are cross-signed by IdenTrust's DST Root CA X3, another root certificate controlled by a different certificate authority which is trusted by most root stores.

Finally, we also have the ISRG Root OCSP X1 certificate. This one is a little different – it doesn't issue any certificates. Instead, it signs Online Certificate Status Protocol (OCSP) responses that indicate the intermediate certificates have not been revoked. This is important because the only other thing capable of signing such statements is our root itself, and as mentioned above, the root needs to stay offline and safely secured.

THE NEW CERTIFICATES

For starters, we've issued two new 2048-bit RSA intermediates which we're calling R3 and R4. These are both issued by ISRG Root X1, and have 5-year lifetimes. They are also cross-signed by IdenTrust. They're basically direct replacements for our current X3 and X4, which are expiring in a year. We expect to switch our primary issuance pipeline to use R3 later this year, which won't have any real effect on issuance or renewal.

The other new certificates are more interesting. First up, we have the new ISRG Root X2, which has an ECDSA P-384 key instead of RSA, and is valid until 2040. Issued from that, we have two new intermediates, E1 and E2, which are both also ECDSA and are valid for 5 years.

Notably, these ECDSA intermediates are not cross-signed by IdenTrust's DST Root CA X3. Instead, the ISRG Root X2 itself is cross-signed by our existing ISRG Root X1. An astute observer might also notice that we have not issued an OCSP Signing Certificate from ISRG Root X2.

WHY WE ISSUED AN ECDSA ROOT & INTERMEDIATES

There are lots of other articles you can read about the benefits of ECDSA (smaller key sizes for the same level of security; correspondingly faster encryption, decryption, signing, and verification operations; and more). But for us, the big benefit comes from their smaller certificate sizes.

Every connection to a remote domain over https:// requires a TLS handshake. Every TLS handshake requires that the server provide its certificate. Validating that certificate requires a certificate chain (the list of all intermediates up to but not including a trusted root), which is also usually provided by the server. This means that every connection—and a page covered in ads and tracking pixels might have dozens or hundreds—ends up transmitting a large amount of certificate data. And every certificate contains both its own public key and a signature provided by its issuer.

While a 2048-bit RSA public key is about 256 bytes long, an ECDSA P-384 public key is only about 48 bytes. Similarly, the RSA signature will be another 256 bytes, while the ECDSA signature will only be 96 bytes. Factoring in some additional overhead, that's a savings of nearly 400 bytes per certificate. Multiply that by how many certificates are in your chain, and how many connections you get in a day, and the bandwidth savings add up fast.

These savings are a public benefit both for our subscribers – who can be sites for which bandwidth can be a meaningful cost every month – and for end-users, who may have limited or metered connections. Bringing privacy to the whole Web doesn't just mean making certificates available, it means making them efficient, too.

As an aside: since we're concerned about certificate sizes, we've also taken a few other measures to save bytes in our new certificates. We've shortened their Subject Common Names from "Let's Encrypt Authority X3" to just "R3", relying on the previously-redundant Organization Name field to supply the words "Let's Encrypt". We've shortened their Authority Information Access Issuer and CRL Distribution Point URLs, and we've dropped their CPS and OCSP urls entirely. All of this adds up to another approximately 120 bytes of savings without making any substantive change to the useful information in the certificate.

WHY WE CROSS-SIGNED THE ECDSA ROOT

Cross-signing is an important step, bridging the gap between when a new root certificate is issued and when that root is incorporated into various trust stores. We know that it is going to take 5 years or so for our new ISRG Root X2 to be widely trusted itself, so in order for certificates issued by the E1 intermediate to be trusted, there needs to be a cross-sign somewhere in the chain.

We had basically two options: we could cross-sign the new ISRG Root X2 from our existing ISRG Root X1, or we could cross-sign the new E1 and E2 intermediates from ISRG Root X1. Let's examine the pros and cons of each.

Cross-signing the new ISRG Root X2 certificate means that, if a user has ISRG Root X2 in their trust store, then their full certificate chain will be 100% ECDSA, giving them fast validation, as discussed above. And over the next few years, as ISRG Root X2 is incorporated into more and more trust stores, validation of ECDSA end-entity certificates will get faster without users or websites having to change anything. The tradeoff though is that, as long as X2 isn't in trust stores, user agents will have to validate a chain with two intermediates: both E1 and X2 chaining up to the X1 root. This takes more time during certificate validation.

Cross-signing the intermediates directly has the opposite tradeoff. On the one hand, all of our chains will be the same length, with just one intermediate between the subscriber certificate and the widely-trusted ISRG Root X1. But on the other hand, when the ISRG Root X2 does become widely trusted, we'd have to go through another chain switch in order for anyone to gain the benefits of an all-ECDSA chain.

In the end, we decided that providing the option of all-ECDSA chains was more important, and so opted to go with the first option, and cross-sign the ISRG Root X2 itself.

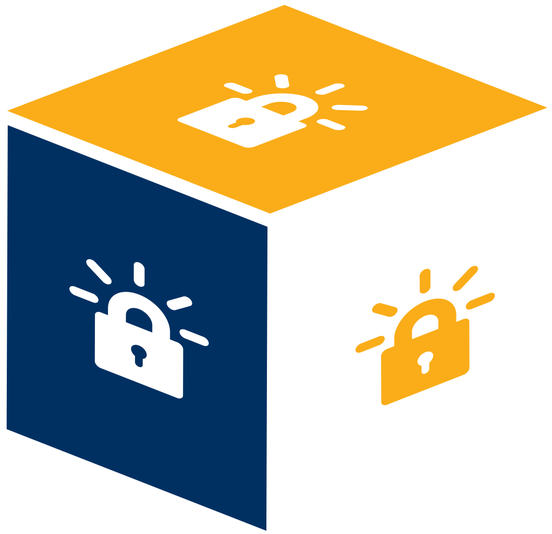
PUTTING IT ALL TOGETHER

Now that we've shared our new certificates look the way they do, there's one last thing we'd like to mention: how we actually went about issuing them.

The creation of new root and intermediate certificates is a big deal, since their contents are so regulated and their private keys have to be so carefully protected. So much so that the act of issuing new ones is called a "ceremony". Let's Encrypt believes strongly in automation, so we wanted our ceremony to require as little human involvement as possible.

Over the last few months we've built a ceremony tool which, given appropriate configuration, can produce all of the desired keys, certificates, and requests for cross-signs. We also built a demo of our ceremony, showing what our configuration files would be, and allowing anyone to run it themselves and examine the resulting output. Our SREs put together a replica network, complete with Hardware Security Modules, and practiced the ceremony multiple times to ensure it would work flawlessly. We shared this demo with our technical advisory board, our community, and various mailing lists, and in the process received valuable feedback that actually influenced some of the decisions we've talked about above! Finally, on September 3rd, our Executive Director met with SREs at a secure datacenter to execute the whole ceremony, and record it for future audits.

And now the ceremony is complete. We've updated our certificates page to include details about all of our new certificates, and are beginning the process of requesting that our new root be incorporated into various trust stores. We'd like to thank IdenTrust for their early and ongoing support of our vision to change security on the Web for the better.



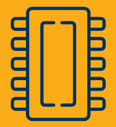
SERVING AT SCALE

THE NEXT GEN DATABASE SERVERS POWERING LET'S ENCRYPT

A database is at the heart of how Let's Encrypt manages certificate issuance. If this database isn't performing well enough, it can cause API errors and timeouts for our subscribers. Database performance is the single most critical factor in our ability to scale while meeting service level objectives. Here's a closer look at how our infrastructure is able to serve the world.

HARDWARE SPECIFICATIONS

The previous generation of database hardware was powerful but it was regularly being pushed to its limits. For the next generation, we wanted to more than double almost every performance metric in the same 2U form factor. In order to pull that off, we needed AMD EPYC chips and Dell's PowerEdge R7525 was ideal. Here are the specifications:

	PREVIOUS GEN	NEXT GEN
	2x Intel Xeon E5-2650 Total 24 cores / 48 threads	2x AMD EPYC 7542 Total 64 cores / 128 threads
	1TB 2400MT/s	2TB 3200MT/s
	24x 3.8TB Samsung PM883 SATA SSD 560/540 MB/s read/write	24x 6.4TB Intel P4610 NVMe SSD 3200/3200 MB/s read/write

WHAT EXACTLY ARE WE DOING WITH THESE SERVERS?

Our certificate authority software, Boulder, uses MySQL-style schemas and queries to manage subscriber accounts and the entire certificate issuance process. It's designed to work with a single MySQL, MariaDB, or Percona database. We currently use MariaDB, with the InnoDB database engine.

We run the CA against a single database in order to minimize complexity. Minimizing complexity has been good for security, reliability, and reducing maintenance burden. We do have a number of replicas of the database active at any given time, and we direct some read operations to replica database servers to reduce load on the primary.

One consequence of this design is that our database machines need to be pretty powerful. Eventually we may need to shard or break the single database into multiple databases, but hardware advancements have allowed us to avoid that so far.

HARDWARE SPECIFICATIONS

By going with AMD EPYC, we were able to get 64 physical CPU cores while keeping clock speeds high: 2.9GHz base with 3.4GHz boost. More importantly, EPYC provides 128 PCIe v4.0 lanes, which allows us to put 24 NVMe drives in a single machine. NVMe is incredibly fast (~5.7x faster than the SATA SSDs in our previous-gen database servers) because it uses PCIe instead of SATA. However, PCIe lanes are typically very limited: modern consumer chips typically have only 16 lanes, and Intel's Xeon chips have 48. By providing 128 PCI lanes per chip (v4.0, no less), AMD EPYC has made it possible to pack large numbers of NVMe drives into a single machine.

OPENZFS & NVMe

NVMe drives are becoming increasingly popular because of their incredible performance. Up until recently, though, it was nearly impossible to get many of them in a single machine because NVMe uses PCIe lanes. Those were very limited: Intel's Xeon processors come with just 48 PCIe v3 lanes, and a number of those are used up by the chipset and add-on cards such as network adapters and GPUs. You can't fit many NVMe drives in the remaining lanes.

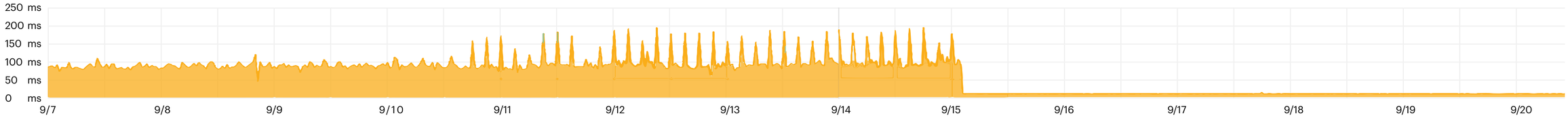
AMD's latest generation of EPYC processors come with 128 PCIe lanes - more than double what Intel offers - and they're PCIe v4. This is enough to pack a 2U server full of NVMe drives (24 in our case).

Once you have a server full of NVMe drives, you have to decide how to manage them. Our previous generation of database servers used hardware RAID in a RAID-10 configuration, but there is no effective hardware RAID for NVMe, so we needed another solution. One option was software RAID (Linux mdraid), but we got several recommendations for OpenZFS and decided to give it a shot. We've been very happy with it.

PERFORMANCE IMPACT

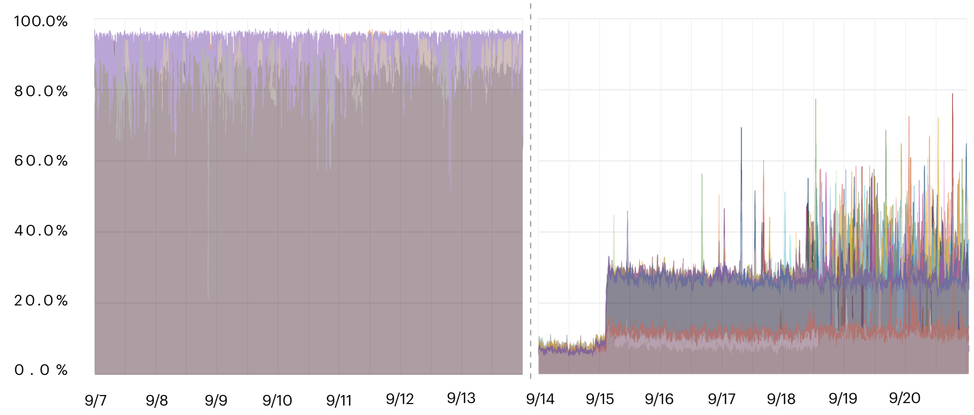
We'll start by looking at our median time to process a request because it best reflects subscribers' experience. Before the upgrade, we turned around the median API request in ~90 ms. The upgrade decimated that metric to ~9 ms!

MEDIAN API REQUEST LATENCY



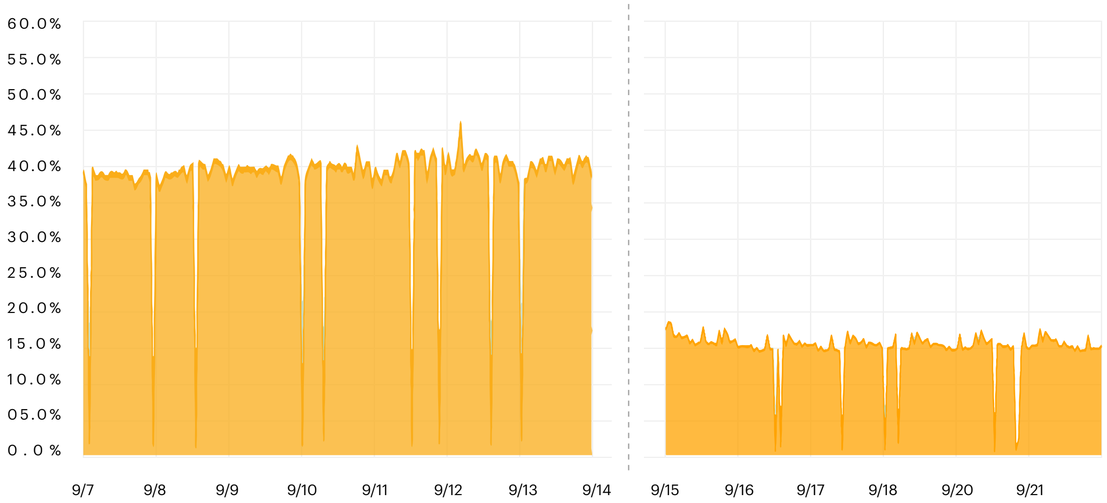
In the week before we upgraded our primary database server, its CPU usage (from /proc/stat) averaged over 90%. The new AMD EPYC CPUs sit at about 25%. You can see in this graph where we promoted the new database server from replica (read-only) to primary (read/write) on September 15.

DATABASE SERVER CPU USAGE



The upgrade greatly reduced our overall database latency. The average query response time (from INFORMATION_SCHEMA) used to be ~0.45ms. Queries now average three times faster, about 0.15ms.

AVERAGE QUERY RESPONSE TIME

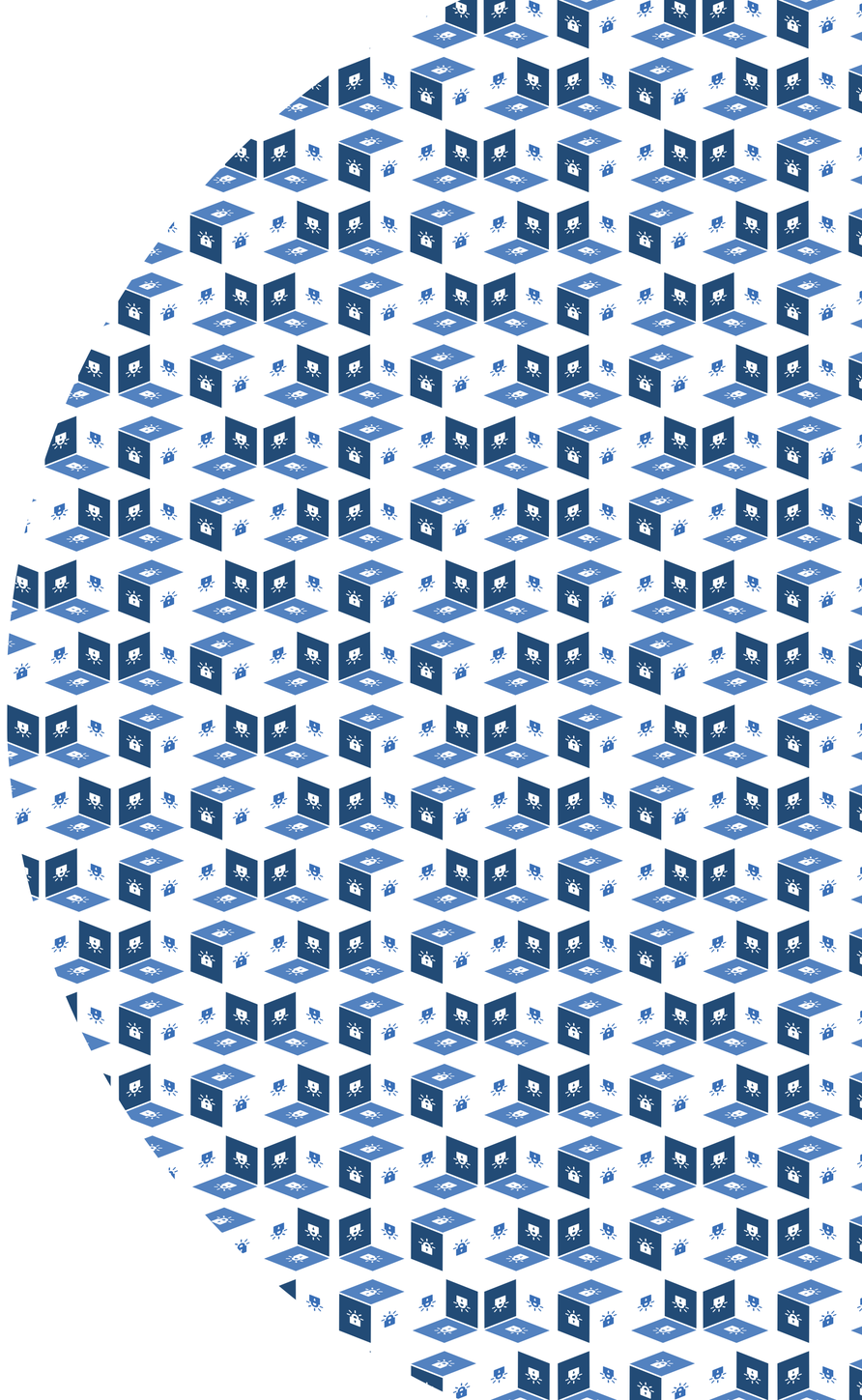


A GLOBAL COMMUNITY

USERS AND SUPPORTERS AROUND THE GLOBE

ISRG is proud to serve hundreds of millions of people around the world. And while we strive for our work to be easy-to-use, we know that our impact is only possible through the support we receive in time and resources from a, comparatively, small group of folks.

“Supporter” is a word we throw around often, but that one word isn’t adequate in explaining just how many ways people make our work possible. From niche technical advice on our community forum, to in-kind donations of equipment, to integrators who manage TLS certificates for sometimes millions of their customers, here’s a closer look at some of the people and organizations who are critical to ISRG and Let’s Encrypt.



A COMMUNITY LEAD BY GENEROUS EXPERTS FOR PEOPLE AROUND THE WORLD

Since 2015, a relatively small group of leaders have made community.letsencrypt.org a robust and vibrant home for questions, ideas, and help for users all around the world.

Building a community that's beneficial is a task in itself. Having it be a resource for reliable technical support is a feat! That feat is achieved, every day, led by hundreds of community members who provide technical support, on average, in just two hours.

This year, there have been nearly 40,000 posts and 19,700,000 page views. These community members are critical to our mission of advancing HTTPS adoption.

With Let's Encrypt being freely available in every country and municipality it can be, it's important that our resources and information be as widely accessible as possible.

Over the last few years, community moderator Tom Delmas has been outstanding in helping contributors from around the world translate letsencrypt.org into thirteen different languages.

These volunteer contributors have made our documentation and support available to speakers of German, French, Spanish, Hebrew, Indonesian, Japanese, Korean, Portuguese Russian, Serbian, Swedish, Vietnamese, and Chinese (PRC).

Our thanks to these community forum leaders for their outstanding (and numerous!) contributions through 2020

_az	JuergenAuer	rg305	stevenzhu
9peppe	mnordhoff	Rip	tdelmas
bruncsak	orangepizza	rmbolger	
griffin	Osiris	sahsanu	
JimPas	petercooperjr	schoen	
jmorahan	Patches	ski192man	

Our thanks to these volunteer contributors for translating letsencrypt.org into thirteen languages.

eumel8	shuuji3	linherest
pfontela	henrychoi7	timtorChen
georgeperez	brwolfgang	zaoqi
LOICEV	goodhousekeeper	DDoSolitary
yarons	filipajdacic	stevenzhu25
chez14	labanskoller	ZeroSimple

WITH US SINCE THE BEGINNING

These organizations joined us in 2015, when Let's Encrypt was just an ambitious idea, and gave us the launchpad to change the web. We are grateful for their dauntless support and leadership in building a better internet.

Akamai
cisco
HOSTPOINT
mozilla
SiteGround
ALA American Library Association
cyon
IdenTrust part of HID Global
OVHcloud
VULTR
AUTOMATTIC
EFF
infomaniak
PlanetHoster
chrome
facebook
Internet Society
shopify

A TRUSTED PARTNER FOR DATTO

Datto is the world's leading provider of cloud-based software and technology solutions purpose-built for delivery by managed service providers (MSPs). They have been a sponsor and user of Let's Encrypt since 2017. Since then they've gone on to grow dramatically. We sat down with Christopher Hoult, Principal Software Engineer, to chat about Datto's work with Let's Encrypt.

LE: Datto joined us in 2018 as a sponsor. What's changed between now and then? How has using Let's Encrypt certificates helped you scale?

CH: The biggest change over the past two years has been that our BCDR business has experienced exceptional growth, with the number of customer devices increasing significantly each year. Let's Encrypt has scaled along with us, allowing us to continue supporting our over 17,000 Managed Service Provider (MSPs) partners to support their customers by providing easy and secure HTTPS access to on-site devices in the field.

Security is incredibly important to us and those we serve, and so being able to use a globally-trusted PKI provider gives us a highly cost-effective mechanism to create the best experience for everyone without compromising on safety, as well as building our products knowing that we're incorporating the firepower of the best experts in the business.

LE: What was the process like for setting up your Let's Encrypt implementation? What made you decide to use Let's Encrypt?

CH: The process for setting up our Let's Encrypt implementation was very straightforward - even though we required the creation of a custom client for our solution, the entire experience of working with Let's Encrypt was smooth, from the quality of the ACME documentation to the wonderful relationship with our contacts at Let's Encrypt. When it came to upgrading from ACMEv1 to v2 in the past year, we were incredibly well looked-after by Let's Encrypt, who ensured we were both aware of the upcoming changes as well as following up with us after we'd put our changes into production. We very much feel like we're part of a team with Let's Encrypt.

The reason we chose Let's Encrypt for our products was because of its programmatic approach to certificate issuance, as well as straightforward renewal process and global trust. Many of our customers deal with hundreds of support issues per day, and anything that slows them down as they either setup new installations or investigate issues reduces their ability to help other clients. Let's Encrypt is essential to us for supplying the kind of smooth customer experience that Datto is known for as part of our mission to keep the MSP world moving.

LE: Have you found that getting a Let's Encrypt cert is fast? Does the speed of getting a cert help you and your customers?

CH: Operating at the scale we do—17,000 customers and growing, and each customer having their own end customers making use of our solutions—it's imperative that their experience is fast and reliable. Let's Encrypt's performance at scale has been particularly impressive, with certificates being issued within seconds using the DNS challenge mechanism. The fact that we can cycle our certificates with confidence means we can continue to provide the seamless experience Datto is known for without cutting any corners on security.

We are grateful for Datto's longtime support, and proud to call them a partner in building a better web.

2020 SPONSORS & FUNDERS

Ninety-four sponsors and funders from more than twenty countries around the world supported us in 2020.

From one-employee shops to thousand-employee companies, we are proud to have support from these organizations who prioritize the importance of investing in a more secure and privacy-respecting Web.

> **EVEN IF AN OPEN SOURCE PROJECT IS USED BY 100% OF WEBSITES ON THE INTERNET, THE HARDER PART, IRONICALLY, IS MAKING ENOUGH MEANING FOR 1,000 PEOPLE: BECOMING VISIBLE AND PRESENT ENOUGH THAT THEY CARE WHAT HAPPENS TO YOU AND YOUR PROJECT, VERSUS ANY OTHER OPPORTUNITY OUT THERE."**

NADIA EGHBAL
WORKING IN PUBLIC

ORGANIZATIONAL UPDATES

NEW FACES, FINANCIALS, AND OUR LEADERSHIP

2020 has been a year of momentum for ISRG. Let's Encrypt is serving reliably, at scale, supported by a robust global community. Our work as a nonprofit organization is emboldened by our longtime support from a core group of funders and inspired by new investments in our work. Here is a closer look at new team members, our revenues in 2020 and our leadership.

ADDITIONS TO ISRG STAFF

My name is Kiel Christofferson, I've been with ISRG for almost three years, and this year I became the manager focused on helping each member of our Site Reliability Engineering (SRE) team grow to meet their goals. We've been fortunate to hire four new people, two SREs and two developers. I'm excited to share a little bit about what I've learned while working with them.

Reflecting on the results of this year's hiring efforts, I remain impressed and very grateful that we find coworkers who are able to bring their considerable experience, their fantastic skills (both well-established and brand-new), and their humility, to elevate the teams they join.

Our first two additions of the year (on the same day!) were Aaron Gable joining the Boulder Development team, and Tim Geoghegan joining the SRE Team.

Aaron Gable previously worked on Chromium developer tools and infrastructure at Google. Right after he started, Aaron very quickly churned through code to help complete a tricky migration. Since then, he's stepped in to pinch-hit as a Team Lead and made it look easy (it's not). My own understanding of particular code paths has been improved by his careful explanations.

Tim Geoghegan previously worked on hardware security at Square and Apple. I've seen Tim take on the giant hurdles of new projects which may have global impact and involve new problem spaces. He summons the drive and dedication one might need to cross the United States on a bicycle (which Tim has also done!).

Next we brought Samantha Frank to the Boulder Dev team. Samantha previously worked on incident reduction and Change Management automation at Amazon. Golang may be relatively new to her, but I notice her striding through improvements to error assertions within every single Boulder component, improving testing ergonomics, and collaborating with SRE team members to evaluate component performance within a changing infrastructure. Samantha is also helping to improve our hiring process.

Most recently we added Amir Omidi to our SRE team. Amir previously worked with the Azure Data team at Microsoft. Amir has ramped-up quickly and is tackling the intricacies of implementing a brand new component for his project with confidence. His thorough research and clean code are helping to build a product that we can capably support long-term.

J.C. Jones will be joining our SRE team at the end of November. In many ways, we are welcoming an old friend: J.C. was one of the original collaborators on the Let's Encrypt project while it was incubated within Mozilla. He has continued to be a valuable member of our community over the years and we are thrilled he will be contributing in a formal capacity again.

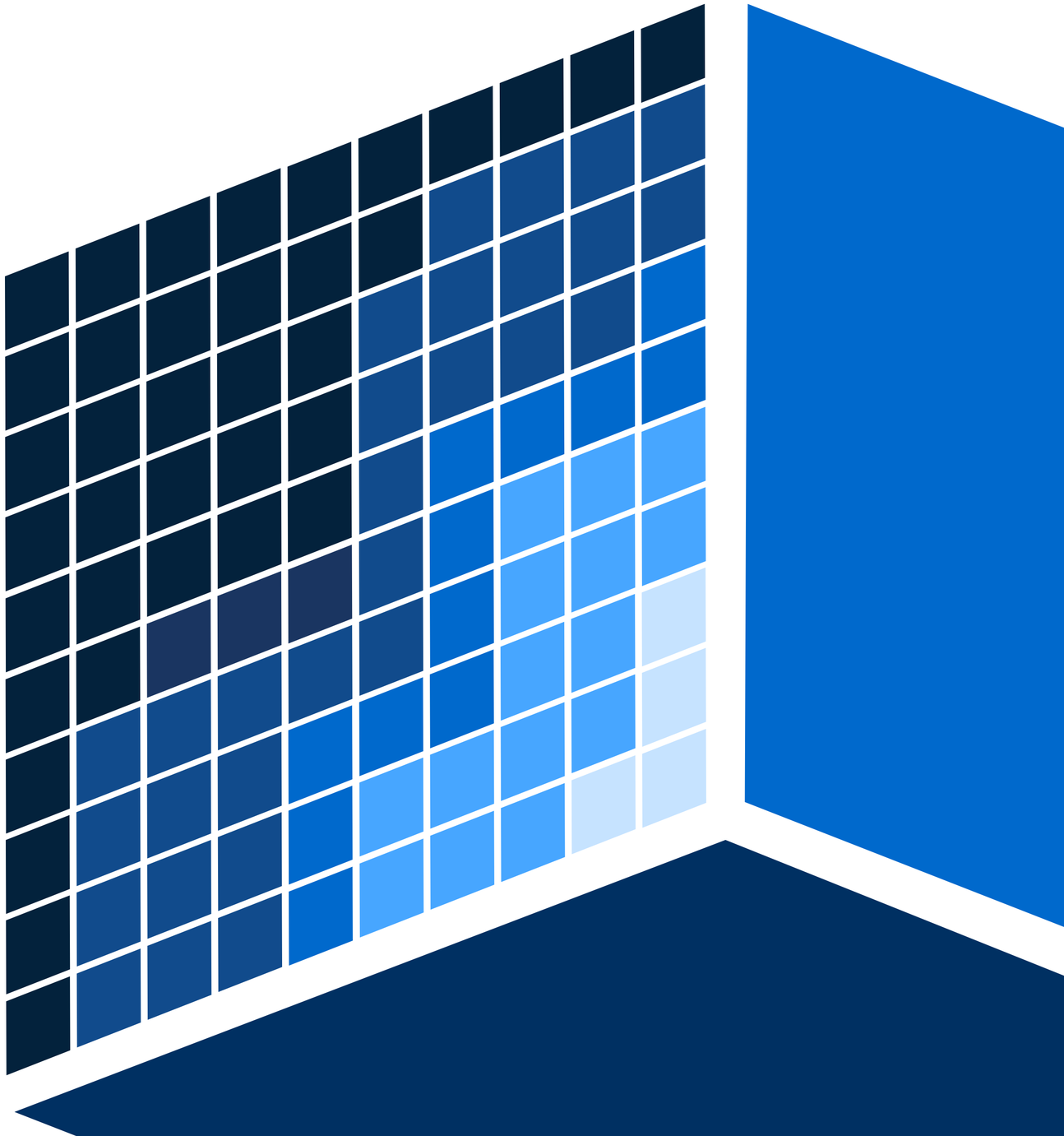
Our new team members meet and exceed the expectations of an organization that works hard to function transparently. They thoughtfully engage with their coworkers and with our partners. They leverage their experience to improve the work we do, yet remain open to learning and to the peculiarities of offering an automated Certificate Authority. I have watched each of them dig into the unfamiliar, the compliance-restricted, the documentation-lacking, the critical communications with external partners, the technical debt, and the loose ends, all to contribute fantastically to a better internet.

KIEL CHRISTOFFERSON
SITE RELIABILITY ENGINEER
TEAM MANAGER

2020 REVENUE BY SOURCE

2020 is on track to being one of ISRG's most successful fundraising years to date. This is made possible by ninety-four sponsors, major national grantmaking organizations, substantial equipment donations, and support from thousands of individuals around the world.

FUNDING SOURCE	PERCENT OF TOTAL
Platinum Sponsorships	37%
Gold Sponsorships	3%
Silver Sponsorships	29%
Corporate Donations	12%
Grants	15%
Individual Donations	4%



2020 BOARD OF DIRECTORS

AANCHAL GUPTA
INDEPENDENT

CHRISTINE RUNNEGAR
INTERNET SOCIETY

DAVID NALLEY
AMAZON WEB SERVICES

JENNIFER GRANICK
AMERICAN CIVIL LIBERTIES UNION

J. ALEX HALDERMAN
UNIVERSITY OF MICHIGAN

JOSH AAS
INTERNET SECURITY RESEARCH GROUP

MAX HUNTER
ELECTRONIC FRONTIER FOUNDATION

PASCAL JAILLON
OVH CLOUD

RICHARD BARNES
CISCO

VICKY CHIN
MOZILLA

TECHNICAL ADVISORY BOARD

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

ONWARDS TO A BETTER INTERNET

SUPPORT OUR WORK

Thanks to our staff, community, users, sponsors, grantmakers, and individual donors, ISRG and its projects are building a better internet for everyone, everywhere.

ISRG Internet Security Research Group

Let's Encrypt

The mission of Internet Security Research Group (ISRG) is to reduce financial, technological, and educational barriers to secure communication over the Internet. ISRG is a California public benefit corporation, recognized by the IRS as a tax-exempt organization under Section 501(c)(3).

For more on our work, visit https://abetterinternet.org

OUR THANKS TO THESE INDIVIDUAL DONORS

This year we received more than 12,000 gifts from 50+ countries around the world. Our thanks to these donors for their support.

@repkam09
Abdessamad Razougui
Aileen M. Baluyut
AJ Jordan
Alex C
Alex C.
Alex Qyoun-ae
Alexis Touet
Algolia
AlgoSecure
alpet
alpha-mouse
ANN JI HAN
Anton
Anton Schegg
Anunay Kulshrestha
Arkadiy Tetelman
basst85 on Twitter
Behr & Tom the Corgis
Ben Sykes
BENEDICTO PEREZ
Bernardo Garcia
bn.dyn-berlin.de
BobbyJo / WarpCoil
Boris Pavlenko
Boyan Zahariev
Brian Duncan
Brisa
Bruno
Bruno Miyamotto
Bt0dotninja
bto
campoint AG
Carl Frederic de Celles
Chris Grindstaff
Chris Wilson
Christoph Noppeney
Christopher
Ciera
Cloud9Dynamics
Dan Zachareas
Dana Ariya
Daniel Spangenberg
DARWIN BAISA
David McKendrick
DavidH
Dean Oakley
Dedicated for Dr APJ
Abdul Kalam
Desia Yamese Clements Lewis
DG6JS
dohq
Dominic
Don Hawkins
Project “Pasos de Jesús”
Drakkar
Durongrit Tripak
eClinPro
efeyopixel.com
Egor Petukhovsky
epidata.dk
Eugene Blundell
Ezra Wolfe
Fabio Neves
Fernando Luccarini
Forrest Hoffman
Foxdebug
Foxel
Gabriel Bautista
Geoffrey R.
Gerald Luke
gitpod.io
GORO
hamurabi delgado
HARUKI SATO
Helpful Digital
Hemant
Henri Hannetel
Hofstadter, Inc
Hotsoft Informática
Humu, Inc.
Ian Norman
Image-charts.com
In honor of our little Wildcat, Tarzan!
In loving memory of Boo, our sweet Boston terrier.
In loving memory of Kitten Koo, Fluffy and Fritz - some amazing childhood kitties.
In memory of A.J. the Budgie Car Alarm
In memory of Chris Laursen
In memory of Dusty
In memory of our beloved cat, Beans
Infinistats Ltd
Ingrid Dominguez
International Documents Canada
IONICA
Isaiah Banks
James Agbormbai
Jean H Neas
Jeff Geerling
Jesus Gaibor
Jesús M.
Jon O’Brien
Jose Gomez
Joseph Catrambone
JP POZZI
Juan Vera
Julia Brunenberg
Julien Marque
Kalvö Koloniby (non-profit)
Kamol Chalermviriya
Karol Augustin
Kerim Güney
kevfrancisco.dev
Kevin Kaland, WizOne Solutions
Kia Lo
Kill the groove
Krishnan Rajendram
Lluis Gras Giné
lmcs from Perú
Lukas Gotter
Lyuboslav Petrov
Malik W Dixon
Manfred Riedl
Marian Hähnlein
Marius Kjærstad
MASAHARU SAKAKI
Matt Brown
Matthew Bobletz
Matthieu Baralle
Mauricio Mercado
michael barker
Michael Downing
MULLER REBEYROL
Marian
NAKA Hirotoshi
Nemo
ngoralski
ngsw
NICRONICS
Nikhil Karkare
Nikola Jocic
nimnaij
Noritaka Horio
OH JONG IN
Oleksandr K
Olivier Mondoloni
Ollie Parsley
OneIT
Oskar Holowaty
Paul Reinheimer
Paulius Gudonis, neqsoft
PEDIPA
Peter Götz, Agile Coach & Trainer
Peter Norell
Phil Pennock
Philippe
Prachetas Prabhu
Pranke GmbH
Private House
Priyanshu Ojha Project
QBIST Inc.
Quentonian Bonaparte
Kitty-Kizzle III
quickytools
RALPH HAHN NET
Ramsés Cruz
Ranking Software
RedisGreen
Regis LEMAIRE
Rene Gielen
Revolution
Ricardo
Richard Renard
rictic
Rnig
Rober Pankrath
Robert Abela from WP White Security
Robin Stafford Group
Roger Goudarzi & Nicola Downes
RoiEX
ROR Branch of B6 Investment LLC
Sam Klugherz
SamePostRu
Samphan Raruenrom
Satish Yadav
Sawl Stone
SD
Sébastien Coutu
Sergey
Sergio IT

Donors listed alphabetically and recognized exactly as submitted.