ISRG Internet Security Research Group

Building a better Internet

2024 ANNUAL REPORT

https://abetterinternet.org

Contents

JOSH AAS
EXECUTIVE DIRECTOR

Nearly 10 years of Let's Encrypt

A NOTE FROM OUR EXECUTIVE DIRECTOR

The past year at ISRG has been a great one and I couldn't be more proud of our staff, community, funders, and other partners that made it happen. Let's Encrypt continues to thrive, serving more websites around the world than ever before with excellent security and stability. Our understanding of what it will take to make more privacy-preserving metrics more mainstream via our Divvi Up project is evolving in important ways.

Prossimo has made important investments in making software critical infrastructure safer, from TLS and DNS to the Linux kernel.

Next year is the 10th anniversary of the launch of Let's Encrypt. Internally things have changed dramatically from what they looked like ten years ago, but outwardly our service hasn't changed much since launch. That's because the vision we had for how best to do our job remains as powerful today as it ever was: free 90-day TLS certificates via an automated API. Pretty much as many as you need. More than 500,000,000 websites benefit from this offering today, and the vast majority of the web is encrypted.

Our longstanding offering won't fundamentally change next year, but we are going to introduce a new offering that's a big shift from anything we've done before - short-lived certificates. Specifically, certificates with a lifetime of six days. This is a big upgrade for the security of the TLS ecosystem because it minimizes exposure time during a key compromise event.

Because we've done so much to encourage automation over the past decade, most of our subscribers aren't going to have to do much in order to switch to shorter lived certificates. We, on the other hand, are going to have to think about the possibility that we will need to issue 20x as many certificates as we do now. It's not inconceivable that at some point in our next decade we may need to be prepared to issue 100,000,000 certificates per day.

That sounds sort of nuts to me today, but issuing 5,000,000 certificates per day would have sounded crazy to me ten years ago. Here's the thing though, and this is what I love about the combination of our staff, partners, and funders - whatever it is we need to do to doggedly pursue our mission, we're going to get it done. It was hard to build Let's Encrypt. It was difficult to scale it to serve half a billion websites. Getting our Divvi Up service up and running from scratch in three months to service exposure notification applications was not easy. Our Prossimo project was a primary contributor to the creation of a TLS library that provides memory safety while outperforming its peers - a heavy lift.

Charitable contributions from people like you and organizations around the world make this stuff possible. Since 2015, tens of thousands of people have donated. They've made a case for corporate sponsorship, given through their DAFs, or set up recurring donations, sometimes to give $3 a month. That's all added up to millions of dollars that we've used to change the Internet for nearly everyone using it. I hope you'll join these people and help lay the foundation for another great decade.

JOSH AAS

EXECUTIVE DIRECTOR

Encryption for Everybody

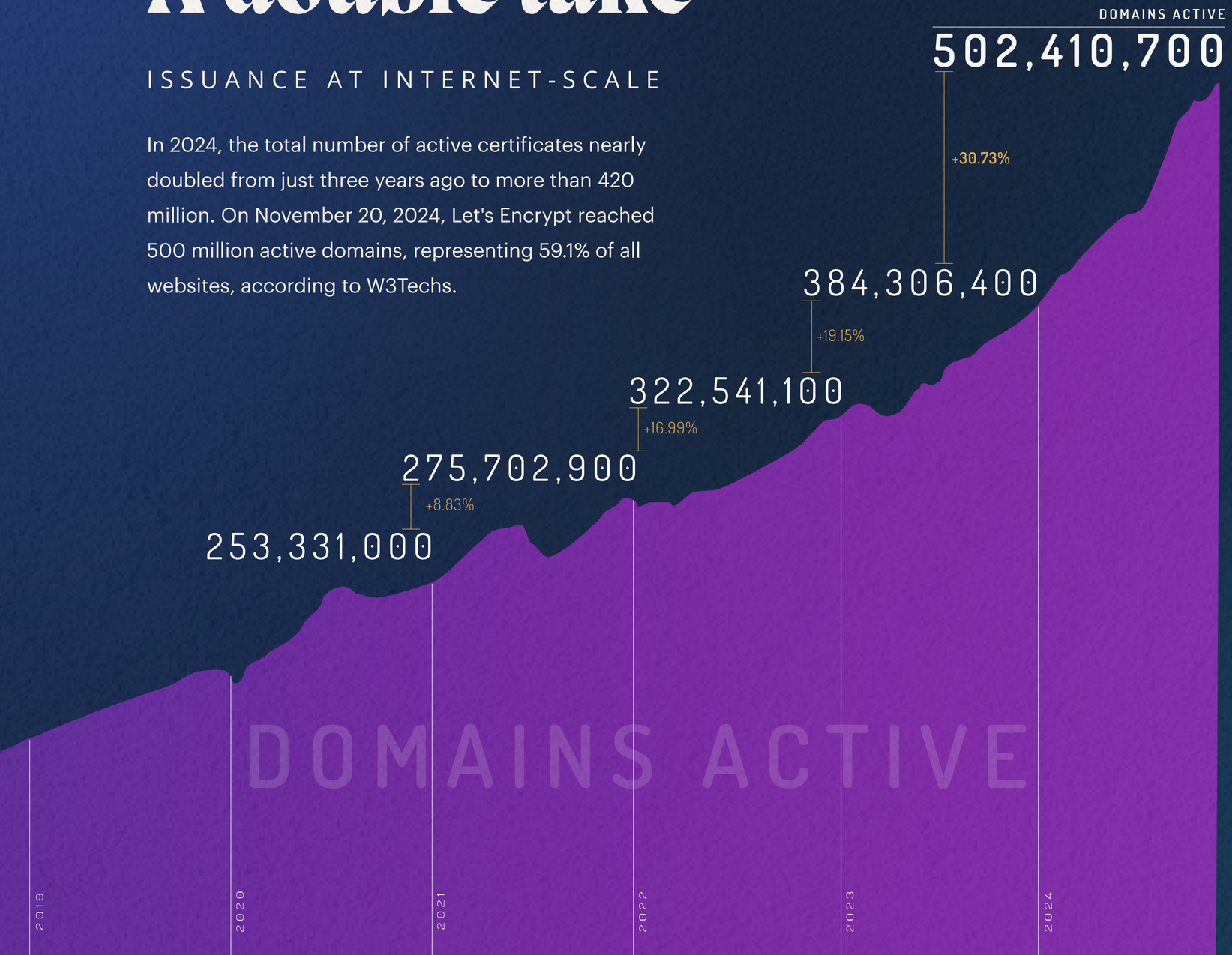
SERVING 500 MILLION DOMAINS

Nine years since we issued our first certificate, this year saw Let's Encrypt continue to reliably serve hundreds of millions of websites, meaning nearly all of the 5+ billion users of the Internet experienced a more secure and privacy-respecting web thanks to widespread HTTPS page loads.

A double take

ISSUANCE AT INTERNET-SCALE

In 2024, the total number of active certificates nearly doubled from just three years ago to more than 420 million. On November 20, 2024, Let's Encrypt reached 500 million active domains, representing 59.1% of all websites, according to W3Techs.

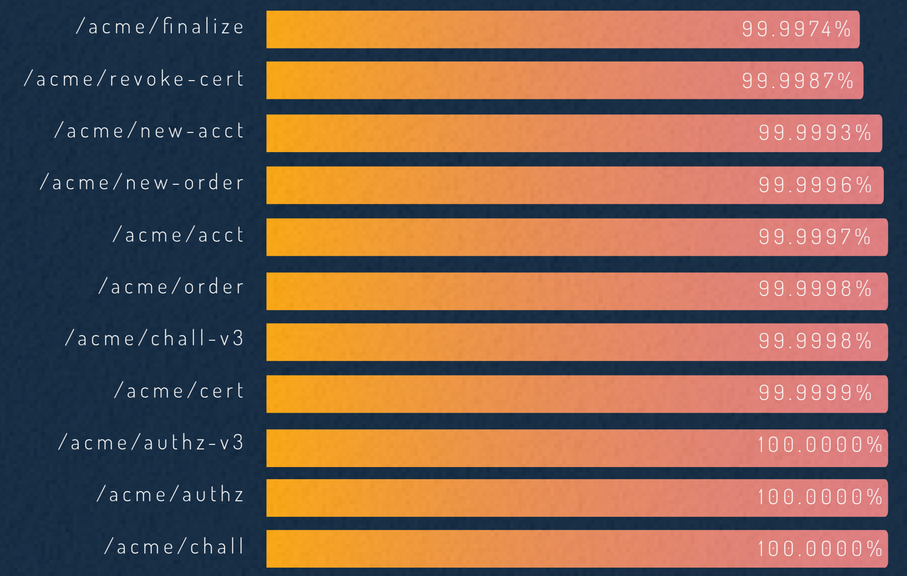


CERTIFICATES ACTIVE, YOY

NUMBER OF CERTIFICATES ISSUED, ALL TIME

5,794,252,821

LET'S ENCRYPT SERVICE LEVEL INDICATORS



Let's Encrypt has internal Service Level Objectives (SLOs) that guide our assessment of our infrastructure's performance and health. We observe the corresponding Service Level Indicators (SLIs) on a 90-day rolling basis. These SLIs reflect the uptime across our API endpoints during a recent analysis of 30 days. SLOs and SLIs inform engineering decisions like planned maintenance or timing of new features. Since the purpose of these is to serve as internal guidance, they do not constitute a promise or guarantee to external parties about the Let's Encrypt service.

It's time to adopt ARI

ADOPTING AUTOMATED RENEWAL INFO (ARI)

ARI enables seamless, automated renewals, allowing Let’s Encrypt to signal to ACME clients when a certificate needs to be renewed—both under normal circumstances and in urgent cases where revocation is necessary. This innovation ensures that service disruptions due to unexpected revocation events are minimized, improving both security and reliability across the web.

> **To foster wider adoption, we're excited to announce a new compelling incentive: certificate renewals that utilize ARI will now be exempt from all rate limits."**

SAMANTHA FRANK
SENIOR SOFTWARE ENGINEER
LET'S ENCRYPT

Without ARI, a sudden revocation might necessitate manual intervention, relying on emails or engineers scrambling to initiate renewals. ARI eliminates these concerns, enabling fully automated renewals—even in extenuating circumstances—without burdening subscribers or risking downtime. As of this year, ARI also offers subscribers the ability to bypass rate limits for certificate renewals, provided renewals occur within the ARI-suggested timeframe.

Beyond making renewals more efficient, ARI sets the stage for Let's Encrypt's future plans, including shorter certificate lifetimes. Subscribers can now be prepared to renew at optimal times, further enhancing the agility and security of their services.

The widespread adoption of ARI is critical to ensuring the web remains resilient and secure. By adopting ARI, subscribers not only gain automation, but also contribute to a more robust certificate ecosystem. With ARI now live in production, we encourage more ACME clients to implement support for this feature and help shape the future of the TLS certificate lifecycle.

Encryption Ecosystem

INNOVATION & COLLABORATION

Let's Encrypt is able to serve more than 500 million domains thanks to a global collaboration of people. From chipping in to help individuals on our community forum to developing a new method for certificate transparency logs, people power this encryption ecosystem.

Sunlight, a new way for certificate transparency

Let's Encrypt built Sunlight in partnership with Filippo Valsorda, who led the design and implementation work. We focused on scalability and efficiency to meet the demands of modern web PKI.

The key motivation behind Sunlight is to overcome the limitations of traditional CT logs, which struggle with the enormous volume of certificates. Let’s Encrypt, for example, issues nearly 5 million certificates daily, which places immense strain on our existing log system. By rethinking the database architecture, Sunlight reduces operational costs and enhances performance by using "tiles"—static files that can be stored and cached more efficiently than dynamic CT APIs.

Sunlight’s innovative tile-based system streamlines both the reading and writing processes. It eliminates complex leader election in the write path, using a simpler, single-node writer, while batching certificates to avoid the latency issues caused by merge delays. This reduces potential failures and simplifies operations.

Now fully operational, Sunlight stands as a robust, scalable solution, improving the CT ecosystem’s reliability and performance.

> **Let's Encrypt's impact over the past ten years went well beyond the hundreds of millions of websites they directly helped secure: they led the industry in deploying automation and contributed to the progress of technical solutions like Certificate Transparency. ISRG is now going beyond the PKI in helping secure the Internet, addressing the main cause of security vulnerabilities: memory safety. As ever, ISRG's efforts under the Prossimo project are efficiently well-targeted to have an impact on the field at large."**
>
> **FILIPPO VALSORDA**
> CRYPTOGRAPHY ENGINEER
> THE GO PROJECT

Thanks to our partners around the world

We are grateful to our donors, sponsors, and funders, whose support makes Let's Encrypt possible. However, we don't talk enough about our technical partners, without whom Let's Encrypt's success may not have been possible.

An example is the collaboration fostered via the Internet Engineering Task Force (IETF). The IETF helps establish a forum for people to collaborate towards setting open standards. It has been instrumental in the development and adoption of critical security standards like the ACME protocol as well as ACME Renewal Information (ARI). Over the last ten years, our Let's Encrypt engineers have participated in and led working groups, and helped draft standards that strengthen Internet security on a global scale.

Our collaboration with Princeton University's Center for Information Technology Policy (CITP) team has likewise been pivotal. Our work with Princeton has focused on defending against Border Gateway Protocol (BGP) attacks on domain control validation via Multi-Perspective Issuance Corroboration (MPIC). This work was made possible by funding from the Open Technology Fund (OTF).

We'd also like to thank IdenTrust for their years of collaboration. They played an important role in helping Let's Encrypt get to where we are today by cross-signing our certificates back in the very beginning, enabling us to be widely trusted by all major browsers.

And thanks to our global community of experts

Over the last ten years, a relatively small group of leaders have made community.letsencrypt.org a robust and vibrant home for questions, ideas, and help for users all over the world.

This year, there have been nearly 29,000 posts, with an average of nearly 4 million page views per month. And while our Let's Encrypt engineers post regularly on the forum, there's no way they could manage that volume of support requests on their own.

That's where our volunteers come in—thousands of people from every corner of the world, helping answer questions and share vital information. Some of our top contributors are on the forum every single day, reading and responding to hundreds of posts. Others have helped make Let's Encrypt more accessible globally by translating our documentation and support into twenty-seven different languages.

> **Let's Encrypt is one of my favorite tech organizations of all time."**
>
> KELSEY HIGHTOWER
> ENGINEER &
> DEVELOPER ADVOCATE

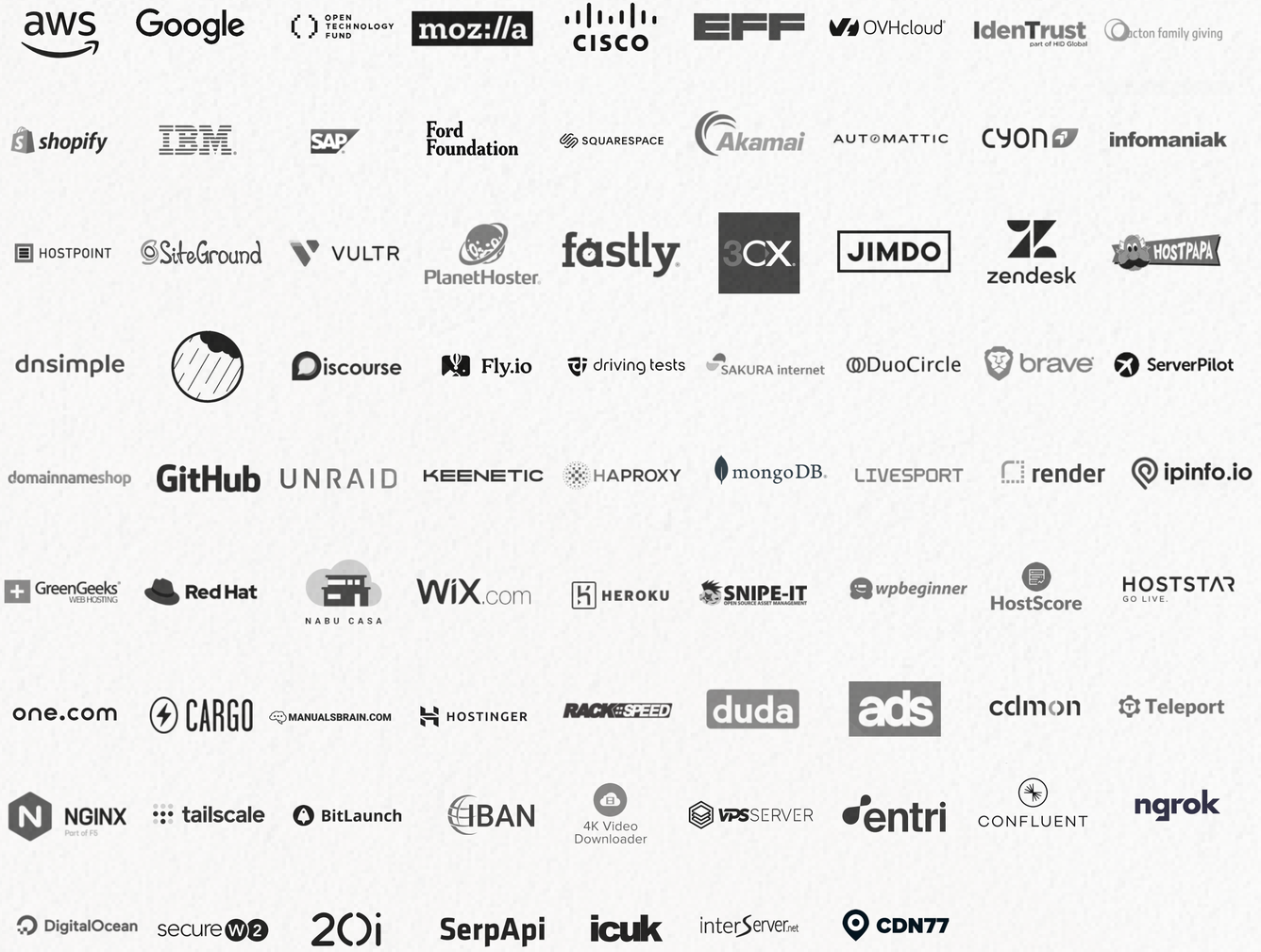
Let's Encrypt Funders

For nearly a decade, Let's Encrypt has helped secure the web thanks to the support from organizations all around the world. We're grateful to these funders for their commitment to ensuring access to free encryption is possible.

BECOME A FUNDER

> **Let's Encrypt has revolutionized web security by providing free, automated, and open certificates, now serving half a billion domains. This monumental achievement underscores ISRG's unwavering commitment to making the Internet a safer place for everyone."**

AANCHAL GUPTA
BOARD MEMBER
ISRG



A memory safe tomorrow

MEMORY SAFETY ACROSS THE INTERNET

Through our Prossimo project, we're tackling the widespread issue of memory safety vulnerabilities by working to transition the Internet's critical infrastructure to memory safe code. We also aim to drive the development of memory safe alternatives for essential software in collaboration with our partners and funders.

PROSSIMO

FOR MEMORY SAFETY

The push for memory safety in critical infrastructure has been picking up speed throughout 2024, beginning with the joint report published by an international group of agencies at the end of last year that named memory safety among the top software development practices organizations should adopt. Further reports and articles from notable sources like the Cybersecurity and Infrastructure Security Agency (CISA) and Google about the prevalence of memory safety vulnerabilities and the critical steps needed to eliminate them have added a sense of urgency around solving this problem.

Over the next few years we hope to continue replacing C or C++ software with memory safe alternatives in the Let's Encrypt infrastructure where and when possible: OpenSSL and its derivatives with Rustls, our DNS software with Hickory, Nginx with River, and sudo with sudo-rs. Memory safety is just part of the overall security equation, but it's an important part and we're glad to be able to make these improvements.

We’re grateful to have CISA, Goolge, and others join us as we continue to work towards the elimination of memory safety vulnerabilities in the Internet’s critical software.

ready, set, rustls

BUILDING CODE, BUILDING MOMENTUM

ISRG has been investing heavily in the Rustls TLS library over the past few years. Our goal has been to build a library that is both memory safe and a leader in performance, with the aim of replacing less safe alternatives such as OpenSSL. The progress we have made in 2024 has brought us much closer to achieving that goal, with the next steps being widespread adoption.

What is Rustls?

Rustls is a low-level software library dedicated to implementing TLS. Rustls supports Server Name Indication (SNI), enabling a web server to host multiple HTTPS websites on the same IP address with distinct certificates. Rustls can also work with TLS certificates that use IP addresses instead of domain names.

Performance as a feature

As Rustls grows in popularity and industries trend towards memory safety, it has become more and more important to guarantee top-notch performance. Aside from correctness and security, it is important for a TLS implementation to keep overhead at a minimum. Consider, for instance, the case of a web server under heavy load: a performant TLS implementation will be able to serve more clients than a less performant one. Historically, this has led the industry to treat performance as a non-negotiable feature, preferring TLS implementations with low latency and a low resource footprint, even if they are written in unsafe languages such as C. With the rise of Rust, however, safer alternatives have become possible without compromising on performance.

The progress we've made this year with Rustls

Benchmarking: A robust system was developed by Adolfo Ochagavia to track performance and prevent regressions. Automated feedback now informs developers of potential issues, leading to more efficient improvements and faster fixes.

Cryptographic Flexibility: Rustls now supports pluggable cryptography, allowing users to choose from different cryptographic backends like AWS Libcrypto (aws-lc-rs), ring, and others, including FIPS-compliant options.

Post-Quantum Key Exchange: Experimental support for post-quantum hybrid key exchange (Kyber/X25519) is in place to prepare for future threats posed by quantum computing.

OpenSSL Compatibility: An OpenSSL compatibility layer allows Rustls to serve as a drop-in replacement for OpenSSL in applications like NGINX, significantly lowering the barrier to adoption.

NGINX Integration: Rustls can now be used with NGINX via the compatibility layer, enabling widespread use with minimal changes to existing infrastructure.

Memory Efficiency: Rustls sessions consume significantly less memory compared to OpenSSL—13KiB vs. 69KiB per session—improving scalability.

Encrypted Client Hello (ECH): Experimental support for ECH improves user privacy by encrypting domain names during TLS handshakes.

Rustls is ready for adoption

To date, we have focused on improving Rustls performance and functionality to make it competitive with the leading TLS library, OpenSSL. Open SSL is not memory safe, making it vulnerable to an entire class of prevalent bugs. Billions of phones, computers, servers, IoT devices, and embedded systems rely on TLS to securely communicate over networks. This means that providing a performant memory safe alternative to OpenSSL in the form of Rustls is critical to improving Internet security.

In the latest round of performance tests, Rustls outperformed both OpenSSL and BoringSSL in every handshake and throughput scenario, proving that not only is Rustls safer, it is also the most performant of the three. With the advancements made to Rustls over the last few years, and this year in particular, we see it as a viable, performant, and memory safe alternative to OpenSSL that is ready for adoption across a range of projects and organizations.

A memory safety moment

THE PROGRESS WE'VE MADE THIS YEAR

Recognizing the amount of work it will take to move significant portions of the Internet's C and C++ software infrastructure to memory safe code, we're tackling the transition through select initiatives. By being smart about our investments and focusing on the most critical Internet infrastructure components, we're seeing significant returns.

> **We, as a nation, have the ability – and the responsibility – to reduce the attack surface in cyberspace and prevent entire classes of security bugs from entering the digital ecosystem but that means we need to tackle the hard problem of moving to memory safe programming languages."**

HARRY COKER
NATIONAL CYBER DIRECTOR
THE WHITE HOUSE

ntpd-rs

Ntpd-rs is a memory safe implementation of the Network Time Protocol (NTP), developed by Tweede golf under contract with the Prossimo project to enhance the security of critical Internet infrastructure. Its recent deployment within Let's Encrypt is a significant milestone, marking the first memory safe software from Prossimo integrated into our Let’s Encrypt infrastructure.

NTP plays a vital role in ensuring accurate timekeeping for operating systems, which is crucial for secure and reliable online communication. By replacing traditional NTP implementations written in unsafe languages like C and C++, ntpd-rs helps reduce vulnerabilities and strengthen Let's Encrypt's security posture.

Ntpd-rs has matured and is now housed and maintained by Tweede golf’s Project Pendulum.

River reverse proxy

In February, we announced plans to build a new high performance and memory safe reverse proxy in partnership with Cloudflare, Shopify, and Chainguard. The new software is being built on top of Cloudflare's Pingora, a Rust-based HTTP proxy, the open sourcing of which was also announced in February.

Nearly every major deployment on the Internet relies on reverse proxy software, but the most commonly used reverse proxies are not memory safe. As a result, many deployments have millions of lines of C and C++ code managing incoming traffic at the network's edge, posing a significant security risk. River aims to deliver excellent performance while drastically reducing the likelihood of memory safety vulnerabilities.

AV1

AV1 is an increasingly important video format and it needs a memory safe, high performance decoder. That's why we worked with the team at Immunant to develop rav1d, a port of the high performance dav1d AV1 decoder from C to memory safe Rust. The project's main objective is to achieve performance parity with the original C-based dav1d while ensuring memory safety through Rust.

To optimize performance, the Immunant team reused performance-critical assembly code from dav1d in rav1d for low-level operations. Performance was measured across multiple hardware platforms, with the Ryzen 7700X used as a baseline. Initial tests showed a 3.8% slowdown in the Rust-transpiled version compared to the original C code, prompting deeper optimization efforts. Bounds checking, which Rust enforces for safety, accounted for less than 1% of the slowdown, while other overhead was due to type conversions and arithmetic inefficiencies. The team focused on minimizing dynamic dispatch, improving bounds checking, reducing stack usage, and eliminating unnecessary branches and panics.

After implementing these optimization techniques, the performance overhead has been reduced from an initial peak of about 11% when we began serious optimization to under 6%. There is still potential for further improvements, but the work the Immunant team has done this year is a great start.

Hickory

DNS is a crucial part of Internet infrastructure, translating domain names into IP addresses for nearly all clients and servers. While some DNS implementations are memory safe, there are none that are also open-source, high-performance, fully recursive DNS resolvers available. This forces many operators to rely on unsafe languages, risking critical infrastructure.

Hickory is now production-ready, with ongoing investments in features, security, and performance to make it a leading DNS resolver for various use cases. Let's Encrypt will be among the first to deploy it, helping to prove Hickory's performance at scale while enhancing its infrastructure with a memory safe language.

To prepare for deployment, several improvements were completed this year, including support for DNSSEC validation, NSEC(3), IP allow lists, denylists for outbound ports, a "do-not-query" list, cache policies by record type, and NS round-robin to reduce rate-limiting. A third-party security audit was also conducted. Continued performance optimizations will ensure Hickory meets the demands of critical environments.

Rust in the Linux kernel

With the Rust for Linux initiative, we're working to make the Linux kernel—the heart of billions of devices and systems—more secure and reliable by adding support for the Rust programming language. Rust's memory safety features offer a modern way to tackle some of the most persistent security challenges in kernel development, and we're excited about what this means for the future of the kernel.

We've made great progress since Rust was officially added as a second language in the kernel back in 2022. Behind the scenes, the Rust for Linux team has been building the infrastructure and safe abstractions needed to support production drivers written in Rust. These are the building blocks for critical components like Rust Binder, which could eventually replace the C version in Android devices, making phones and other systems safer from memory-related vulnerabilities.

This is a team effort. Developers, maintainers, companies, and community members are coming together to make Rust for Linux a reality. We're seeing more kernel subsystems get involved, more conversations happening at conferences, and growing interest from companies that want to use Rust in their own projects.

By sticking to our plan and continuing to build momentum, we're confident Rust will become an essential tool for building a more secure Linux kernel.

sudo-rs

Through a partnership with Tweede golf and Ferrous Systems we've reimagined sudo, a critical Unix utility for privilege management, by rewriting it in Rust to prioritize memory safety and modern security practices. The development of sudo-rs highlighted key challenges, particularly in managing Rust crate dependencies. While initially incorporating around 135 transitive dependencies to accelerate prototyping, the team systematically reduced this to just three core crates: libc, glob, and log. This meticulous process enhanced security by minimizing external codebases and simplifying trust validation.

Feedback from the broader community about dependency overuse validated our efforts, underscoring the importance of scrutinizing dependencies for security-critical applications. By stripping down to essential crates, sudo-rs balances functionality with a minimal attack surface, ensuring reliability for downstream users, including Linux distributions like Fedora, which now provides sudo-rs packages.

Sudo-rs is ready for adoption and has a new long-term home at the Trifecta Tech Foundation, which was founded by the team from Tweede golf.

Thanks to our community of funders

We're deeply grateful to the funders and technical partners who make Prossimo's work possible. Their support helps us tackle some of the toughest challenges in Internet security, creating high-impact solutions that benefit millions of people worldwide.

We also want to highlight the incredible contributions of our technical partners who are at the heart of this work. People like Daniel McCarney, Joe Birr-Pixton, Dirkjan Ochtman, Adolfo Ochogavía, Miguel Ojeda, and Benjamin Fry, as well as the teams at Ferrous Systems, Immunant, and Tweede golf, are the ones bringing these initiatives to life. We're proud of the work we've accomplished together to create a more secure and resilient Internet.

SUPPORT THIS WORK

Privacy for the public's benefit

INSIGHTS WITHOUT INFRINGEMENT

Divvi Up is a privacy-preserving measurement solution for applications that prioritizes user privacy. Using the Distributed Aggregation Protocol (DAP), Divvi Up allows data collection while safeguarding individual identities, working by splitting each user's data into anonymized shares distributed across separate, non-colluding servers. This setup protects user data while enabling applications to derive insights through aggregated analysis. Recent enhancements, including the integration of Oblivious HTTP (OHTTP) and Differential Privacy, provide even greater privacy safeguards for clients.

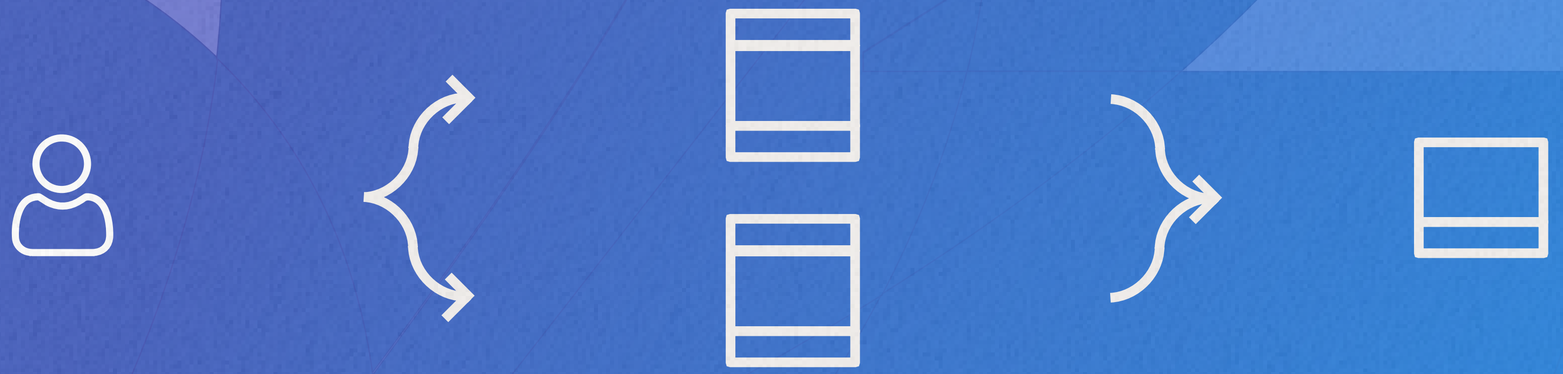
Divvi Up

Data divided. Data secured.

How it works

A SIMPLE SCHEME. COMPLEX MATH.

Divvi Up takes a user-generated metric from a mobile device, web browser, or other application, and divides the metric into two encrypted shares as it leaves the origin. One half of that metric is sent to a Divvi Up server, the other to a third-party server. When an application owner queries an aggregate statistic of its users, Divvi Up combines the divided metrics from all users and produces a privacy-preserving aggregate.



A USER-GENERATED VALUE

DIVIDE THE VALUE

TWO NON-COLLUDING SERVERS

COMBINE AGGREGATES

ANONYMIZED INSIGHT

Key Privacy Mechanisms: DAP & VDAFs

Divvi Up's privacy-first model is founded on two protocols: the Distributed Aggregation Protocol (DAP) and Verifiable Distributed Aggregation Functions (VDAFs).

In this framework, user data is divided into two encrypted shares using a pre-agreed VDAF. One share is sent to the Leader aggregator and the other to the Helper. Each aggregator processes only its shares, which are mathematically structured to look like random noise, making them useless alone. When the aggregated shares are collected and combined, they produce accurate insights while keeping individual contributions secure and private.

The integration of VDAFs into the DAP workflow provides strong cryptographic guarantees for data integrity and privacy. Specifically, VDAFs allow Divvi Up to verify that submitted shares are correctly formed without exposing the underlying user data. This is achieved through a combination of zero-knowledge proofs and multi-party computation (MPC). During the aggregation phase, the servers collaborate to compute the desired aggregate (e.g., sums, averages, or histograms) while ensuring the validity of the individual measurements by verifying proofs included with each measurement. This process makes it possible to detect and discard malicious or malformed contributions, preserving the reliability of the aggregated result.

Expanding privacy

ENHANCING DIVVI UP

Divvi Up continues to develop additional ways towards greater privacy while serving at Internet-scale. The integration this year of OHTTP and Differential Privacy are two ways we're moving towards shifting the privacy paradigm.

OHTTP

The recent integration of Oblivious HTTP (OHTTP) into Divvi Up as an optional feature further enhances the privacy of data collection by shielding participating clients from being identified by the DAP aggregators.

More specifically, OHTTP is a privacy-enhancing protocol that anonymizes HTTP interactions by separating the client's identity from the content of their requests. Here's how it works: OHTTP encapsulates HTTP messages, encrypting them with a gateway's public key and routing them through a relay server. The relay strips any identifying metadata from the request before forwarding the encrypted message to the gateway, which decrypts and sends it to the final destination, without learning who the client is. The relay only knows who sent the data but not its content, while the gateway accesses the data but has no identifying information about the client. This dual-layer approach ensures that even potentially identifying metadata (e.g., IP addresses or DAP task IDs) cannot be easily linked back to clients, providing stronger anonymity.

Applying OHTTP in Divvi Up

In some situations, both the leader and helper aggregators can learn some pieces of information about the participating clients. Potentially identifying metadata such as IP addresses, user agents and TLS ciphersuites are revealed when clients fetch HPKE configurations from either aggregator or upload reports to the leader. This could allow aggregators to fingerprint clients and associate them with DAP tasks, since the task ID appears in the request paths for uploads and (optionally) HPKE configurations.

While OHTTP can enhance the privacy aspects of Divvi Up, it also introduces additional computational and network overhead due to message encapsulation and the need for an independently operated relay server. These operational complexities must be balanced against the privacy benefits in each deployment. For many use cases, the existing privacy guarantees of DAP without OHTTP may be sufficient, making OHTTP best suited for scenarios where the additional anonymity is essential and justifies the trade-offs.

By selectively layering DAP interactions over OHTTP, Divvi Up strengthens privacy guarantees, especially for sensitive use cases where client anonymity is critical.

Differential Privacy

Integrating differential privacy into Divvi Up enhances the system's ability to safeguard user data even beyond the protections offered by DAP. While DAP ensures individual measurements remain private by design, it reveals aggregate results to the collector. In some scenarios, these aggregate results could inadvertently expose sensitive information—particularly when dealing with high-dimensional data, such as histograms with rarely populated buckets. Differential privacy addresses this by introducing carefully calibrated noise to the aggregated results, limiting the amount of information that can be inferred about individual contributions, even from edge cases or outliers.

Adding Noise in Divvi Up

In Divvi Up, differential privacy fits neatly into the system's design by having each aggregator independently add noise to its part of the data before sending it to the collector. In this way, as long as at least one aggregator is honest, the added noise protects everyone's privacy. The amount and type of noise – whether Gaussian, Laplace, or binomial – depends on the aggregation method and the privacy level chosen. Certain data types, like histograms, are particularly well-suited for this approach because they naturally limit how much a single contribution can influence the results, improving the balance between privacy and useful insights.

Differential privacy is a proven approach to handling private data. Building on top of DAP as a secure aggregation protocol is especially useful, because no one party has access to all the raw data, which is rare in differential privacy mechanisms. Offering differential privacy within Divvi Up allows applications to adapt to diverse privacy goals and threat models, and it's a great option for situations where the added layer of security is worth the trade-off in precision or the extra computational effort.

Getting started with Divvi Up

A COMMAND LINE INTRODUCTION

To make it easy to test and develop against the Divvi Up system, the Divvi Up team released a tutorial this year on how to set up the entire Divvi Up stack in a few commands.

Behind the scenes, the Divvi Up service is composed of several modular components, each packaged as a container image for scalability and debuggability. In production, these containers are orchestrated using Kubernetes to handle massive workloads, processing hundreds of millions of reports each month. The command line tutorial simplifies this setup by using the same container images, configured with a docker-compose file that we provide, allowing developers to spin up a local environment that mirrors a production deployment.

Divvi Up is designed to collect data and integrate directly into your application with our TypeScript, Android, or Rust libraries. These libraries are general purpose and should work with any server implementing the IETF draft of the Distributed Aggregation Protocol (DAP). To streamline the setup process, we've also introduced the divviup command line tool, which simplifies tasks like configuring accounts, creating tasks, uploading telemetry data, and running aggregations.

The inclusion of libraries for popular languages like TypeScript, Android, and Rust, combined with detailed documentation, makes it easy to integrate Divvi Up into different types of applications and the ability to customize or simplify components during testing means it can scale to fit a variety of needs. For teams focused on user privacy and data security, the alignment with open standards like DAP and the support for modern tools like Kubernetes and Docker instills confidence that Divvi Up is both cutting-edge and production-ready.

It's a comprehensive, developer-friendly approach to building trust with users by protecting their data while still gaining valuable insights.

CHECK OUT THE TUTORIAL

Ever towards standardization

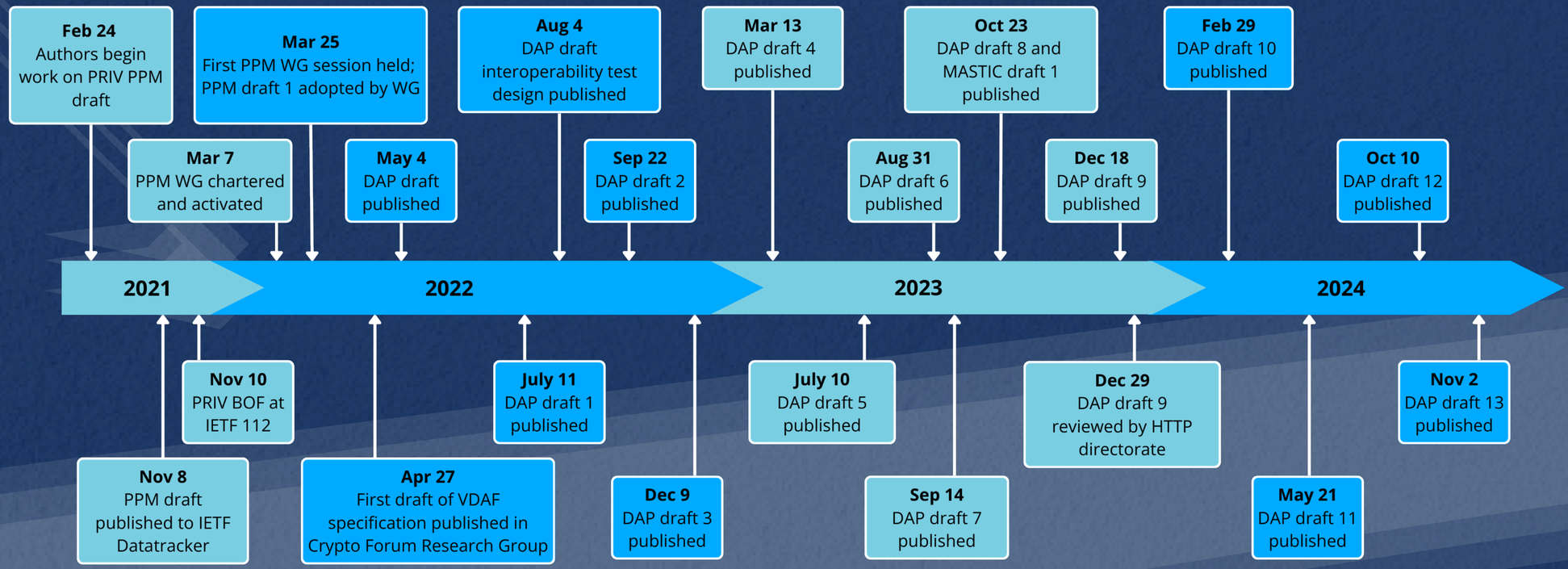
HEADING TOWARDS AN IETF STANDARD

This year the Divvi Up team has helped to progress the DAP and VDAF drafts through the IETF standards process. These technologies make it possible to collect metrics and telemetry while keeping individual data private, using clever cryptographic techniques that split data across non-colluding servers.

Since its inception in 2021, DAP has evolved through thirteen (and counting) iterations of its draft, refining everything from protocol design to real-world usability. A major milestone was the adoption of the draft by the Privacy Preserving Measurement (PPM) working group in early 2022. Over the past year, Divvi Up engineers have worked alongside collaborators to refine protocol features, address scalability challenges, and incorporate feedback from IETF directorates and working group members.

One of our big wins this year has been making sure DAP works seamlessly across different implementations. We've collaborated with organizations like Cloudflare, whose Daphne implementation has a totally different architecture from our own Janus system. Together, we've used interoperability tests to make sure both systems can work together without a hitch—proof that the protocol is flexible and robust.

The timeline below shows the key moments of the DAP IETF process:



Leading to a better Internet

PEOPLE, FUNDERS, & FINANCIALS

Now in its second decade, ISRG is the nonprofit home for projects focused on building a better Internet. Here is a closer look at the organization, its people, and financials.

ISRG

Internet Security Research Group

Not a minute goes by

LETTER FROM ISRG BOARD CHAIR, CHRISTINE RUNNEGAR

Next year, we ask you to join the Internet Security Research Group in celebrating the 10th anniversary of Let's Encrypt. Not a minute goes by without someone in the world accessing a website using a Let's Encrypt certificate to secure the communication, and they are probably not even aware of Let's Encrypt. That's okay. Good security and privacy don't need a label. They just need to happen.

I am very proud of what the Internet Security Research Group has achieved and its ongoing commitment to providing more security and privacy on the Internet.

The founding directors of the Internet Security Research Group, Josh Aas and Eric Rescorla as well as its founding sponsors and partners Mozilla, the Electronic Frontier Foundation, the University of Michigan, Cisco, and Akamai, saw an unmet need in Internet security in 2014 and figured out how to solve it. At the same time, in setting up ISRG, they knew that there would be other needs for public benefit infrastructure beyond TLS certificates. Thanks to their foresight, ISRG has been ready and able to tackle new and difficult Internet security challenges. For instance, the Internet Security Research Group is the home of the Prossimo project which is moving Internet security-sensitive software to memory safe code. That work is even more under the hood than Let's Encrypt. But it is key to removing security vulnerabilities from software that is used everyday to provide Internet communications.

To celebrate Let's Encrypt's 10th anniversary, please join us in making the Internet more secure and privacy protecting by using TLS certificates, contributing through the ISRG community, sponsoring the Internet Security Research Group, donating to support its public benefit projects, and partnering with us to find new ways to secure the Internet.

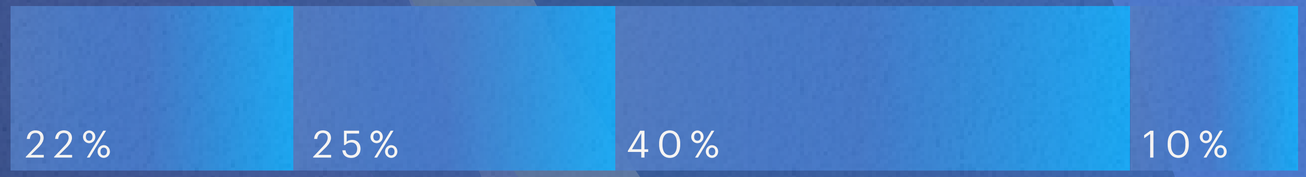
CHRISTINE RUNNEGAR

CHAIR

ISRG BOARD OF DIRECTORS

Financials

REVENUE



EXPENSE

PERCENTAGES BASED ON UNAUDITED FINANCIALS JAN-OCT 2024

> **Let's Encrypt has made the web more secure and privacy protecting for people everywhere in the world. In just ten years, Let's Encrypt's practical success and leadership in best practices has become a beacon for Internet security. I would like to thank the founders of the Internet Security Research Group for their vision, commitment and courage."**

CHRISTINE RUNNEGAR
CHAIR
ISRG BOARD OF DIRECTORS

Board & Staff

BOARD OF DIRECTORS

AANCHAL GUPTA
INDEPENDENT

CHRISTINE RUNNEGAR
BOARD CHAIR, INDEPENDENT

DAVID NALLEY
AMAZON WEB SERVICES

JENNIFER GRANICK
INDEPENDENT

J. ALEX HALDERMAN
UNIVERSITY OF MICHIGAN

JOSH AAS
INTERNET SECURITY RESEARCH GROUP

ERICA PORTNOY
ELECTRONIC FRONTIER FOUNDATION

PASCAL JAILLON
OVHCLOUD

RICHARD BARNES
CISCO

VICKY CHIN
MOZILLA

STAFF

AARON | SOFTWARE ENGINEER
AMEER | SOFTWARE ENGINEER
ANDREW | SOFTWARE ENGINEER
BRAD | SITE RELIABILITY ENGINEER
BRANDON | SENIOR SOFTWARE ENGINEER
CARRISSA | PEOPLE MANAGER
DAN | DIRECTOR BRAND & DONOR DEVELOPMENT
DAVID | SOFTWARE ENGINEER
JACOB | SOFTWARE ENGINEER
JAMES | SITE RELIABILITY ENGINEER
J.C. | SITE RELIABILITY ENGINEER
JOSH | EXECUTIVE DIRECTOR
KIEL | SITE RELIABILITY ENGINEER
KRISTIN | GENERAL COUNSEL
KRUTI | SITE RELIABILITY ENGINEER
LENA | SITE RELIABILITY ENGINEER
MATTHEW | SITE RELIABILITY ENGINEER
MEGAN | BRAND & DONOR DEVELOPMENT SPECIALIST
OLENA | FINANCE MANAGER
PHIL | SITE RELIABILITY ENGINEER
PRESTON | SITE RELIABILITY ENGINEER
SAMANTHA | SOFTWARE ENGINEER
SARAH | VP BRAND & DONOR DEVELOPMENT
SARAH | CHIEF FINANCIAL OFFICER
SARAH | BRAND & DONOR DEVELOPMENT SPECIALIST
SHANNON | DIRECTOR BRAND & DONOR DEVELOPMENT
TIM | SITE RELIABILITY ENGINEER

14 cents a day

DONOR CONTRIBUTIONS HELP POWER OUR IMPACT

Each day we issue millions of certificates, made possible in part thanks to our donors who give $51.70, on average—that's 14 cents a day. These few thousand individuals help enable our impact of serving nearly six billion people using the Internet every single day. We're proud to recive support from people based in 73 different countries around the world. If you've supported ISRG this year with a contribution of any amount, thank you.

DONATE

Let's build a better Internet together

SUPPORT OUR WORK

Thanks to our staff, community, users, sponsors, grantmakers, and individual donors, ISRG and its projects are building a more secure and privacy-respecting Internet for everyone, everywhere.

ISRG Internet Security Research Group · Let's Encrypt · PROSSIMO · Divvi Up

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