



Building a better Internet

2025 ANNUAL REPORT

abetterinternet.org

Contents

10 Years of Let's Encrypt	3
Let's Encrypt: Encryption for Everybody	7
Prossimo: Making it Memory Safe	19
Divvi Up: Insights without Infringement	23
Digital Identity Research	29
ISRG: Leading to a Better Internet	31




JOSH AAS
EXECUTIVE DIRECTOR

10 years of Let's Encrypt

A NOTE FROM OUR EXECUTIVE DIRECTOR

This year was the 10th anniversary of Let's Encrypt. We've come a long way! Today we're serving more than 700 million websites, issuing ten million certificates on some days. Most importantly, when we started 39% of page loads on the Internet were encrypted. Today, in many parts of the world, over 95% of all page loads are encrypted. We can't claim all the credit for that, but we're proud of the leading role we played. Being able to help ISRG and Let's Encrypt get to where we are today has been the opportunity of a lifetime for me.

There's more I could talk about from the past ten years, but this tenth year was about as good as any before it so I want to focus on our most recent work. I'll get the headline for 2025 out right away: over the past year we went from serving 492 million websites to 762 million. That's a 50% increase in a single year, equivalent to the growth we saw over our first six years of existence combined. Our staff did an amazing job accommodating the additional traffic.



I'm also particularly proud of the things we did to improve privacy this year, across all of our projects.

At the start of 2025 we were serving over four billion Online Certificate Status Protocol (OCSP) requests per day. That's 180 million per hour, or 50,000 per second. OCSP has been an important mechanism for providing certificate revocation information for a long time, but the way it works is bad for privacy. It requires browsers to check with certificate authorities for every website they visit, which is basically providing your browsing history to third parties. Let's Encrypt never held onto that data, we dropped it immediately, but there is no way to know if that was standard practice across the industry, and even well-intentioned CAs could make a mistake or be compelled to save that data. It was a system ripe for abuse, so we decided to become the first major CA to turn off our OCSP service. We couldn't be sure what the full impact would be, but this was a way in which the Internet needed to get better. In August of 2025 we turned off our OCSP service, there was no major fallout, and we haven't looked back.

Another big privacy-focused change we made to Let's Encrypt in 2025 was no longer storing subscriber email addresses in our CA database, associated with issuance data. In June of this year we stopped adding the optional email addresses that subscribers send to our database, and we deleted the millions of email addresses that had accumulated over the years. Making this change was not an easy thing to decide to do— it limits our ability to contact subscribers and we had to turn off our expiration reminder email service— but we feel the ecosystem has grown enough over the past ten years that the privacy implications of holding onto the email addresses outweighed the utility.

Privacy was at the forefront for the folks at ISRG researching human digital identity as well. They have been hard at work on an implementation of the Anonymous Credentials from ECDSA scheme, also known as **Longfellow**. This is a cryptographic library that can be used in digital identity management, including things like digital wallets, in order to improve privacy when sharing credentials. Digital identity systems should have strong privacy and compatibility requirements, but such requirements pose challenges that existing digital credential technologies are going to struggle to meet. New schemes such as Longfellow aim to address these challenges, bringing privacy improvements to systems that need to work with existing cryptographic hardware. This is exciting stuff, but not easy to build (so much math!)— watching our talented engineers make progress has been thrilling.

The last example of great privacy work I want to highlight from 2025 is our Prossimo project's work towards encrypted recursive-to-authoritative DNS. Prossimo is focused on bringing memory safety to critical software infrastructure, but sometimes that dovetails nicely with other initiatives. DNS queries are fundamental to the operation of the Internet. Without getting into the details here too much, there are basically two types of DNS queries: stub-to-recursive and recursive-to-authoritative. A lot of work has gone into encrypting stub queries over the past decade, mostly through DNS over HTTPS (DoH) initiatives. Authoritative queries, however, remain almost entirely unencrypted. This is a particular problem for Certificate Authorities like Let's Encrypt.

During 2025, our Prossimo project started work on changing that, investing heavily in encrypted authoritative resolution by implementing **RFC 9539** Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS and other related improvements in Hickory DNS. Once this is ready, early in 2026, Hickory DNS will be a high performance and memory safe option that DNS operators can use to start making and receiving encrypted authoritative DNS queries. It can also be used for integration testing with other DNS implementations.

It's wonderful, and a real responsibility, to be able to have this kind of positive impact on the lives of everyone using the Internet. Charitable contributions from people like you and organizations around the world make what we do possible. We are particularly grateful to Jeff Atwood, Betsy Burton, and Stina Ehrensvärd for their special gifts this year. 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. If you're one of those people, thank you. If you're considering becoming a supporter, I hope this annual report will make the case that we're making every dollar count.

Every year we aim to make the dollars entrusted to us go as far as possible, and next year will be no exception.

Josh Aas, Executive Director





Encryption for Everybody

SERVING 700 MILLION DOMAINS

In 2025, Let's Encrypt celebrated the 10th anniversary of its first certificate. Along the way, we issued over seven billion certificates. Even after a decade of growing the encrypted Internet, we continue to respond to an unmet need for reliable, free, and automated TLS certificates, frequently issuing over 8 million certificates in a single day.

An honor for our early team

Remembering Peter Eckersley

Peter was a passionate advocate for security and privacy. Among his other accomplishments, Peter was one of the founding members of Let's Encrypt during his time at Electronic Frontier Foundation.



The IEEE Cybersecurity Award for Practice recognizes individuals and small teams for game-changing ideas that substantially advanced the practice of cybersecurity. That's a perfect description of what Alex, ekr, Josh, Richard, and the late, great Peter achieved. The state of web security today would be far poorer without them. Congratulations to Let's Encrypt on its tenth anniversary."

RIANA PFEFFERKORN

Policy Fellow, Stanford Institute for Human-Centered AI and 2025 IEEE Cybersecurity Award for Practice Committee Chair

Reflections from our early team



Getting to help build Let's Encrypt over the past decade has been the honor of a lifetime. Serving more than 700 million websites and issuing 10 million certificates on some days would have been a wild thing to try to imagine back in 2015."

JOSH AAS
ISRG



The most impressive part of Let's Encrypt's impact isn't just the scale of certificates issued—it's how much of that impact comes from automation users never have to think about. By removing friction, removing barriers, and removing opportunities for error, Let's Encrypt has made a safer web the default condition. It's a model for how we should build all critical digital infrastructure."

J. ALEX HALDERMAN
University of Michigan



Let's Encrypt is really just so obvious when you think about it. We wanted to encrypt the whole Internet and people are only going to turn on encryption if it's cheap and easy. You need certificates to turn on encryption and that means certificates have to be cheap and easy, and ideally free. Once you do that, people don't really have any excuse not to encrypt."

ERIC RESCORLA
Knight-Georgetown Institute



I remember watching the number of certificates issued by Let's Encrypt go from single to double digits, and wondering if this thing would really take off, whether people would understand our vision. It has been amazing to watch as Let's Encrypt — and more importantly, the concept of certificate automation — have become core to how Internet security works."

RICHARD BARNES
Cisco

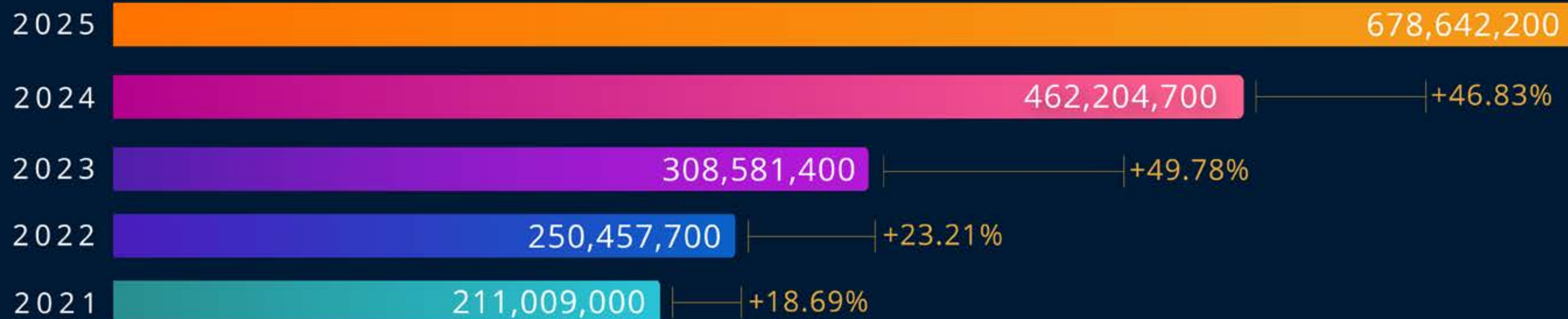
Issuance at Internet-Scale

Since 2015, Let's Encrypt has issued billions of certificates and helped make HTTPS the norm. In October 2025, Let's Encrypt reached over 700 million active domains, representing 60.4% of all websites, according to W3Techs.

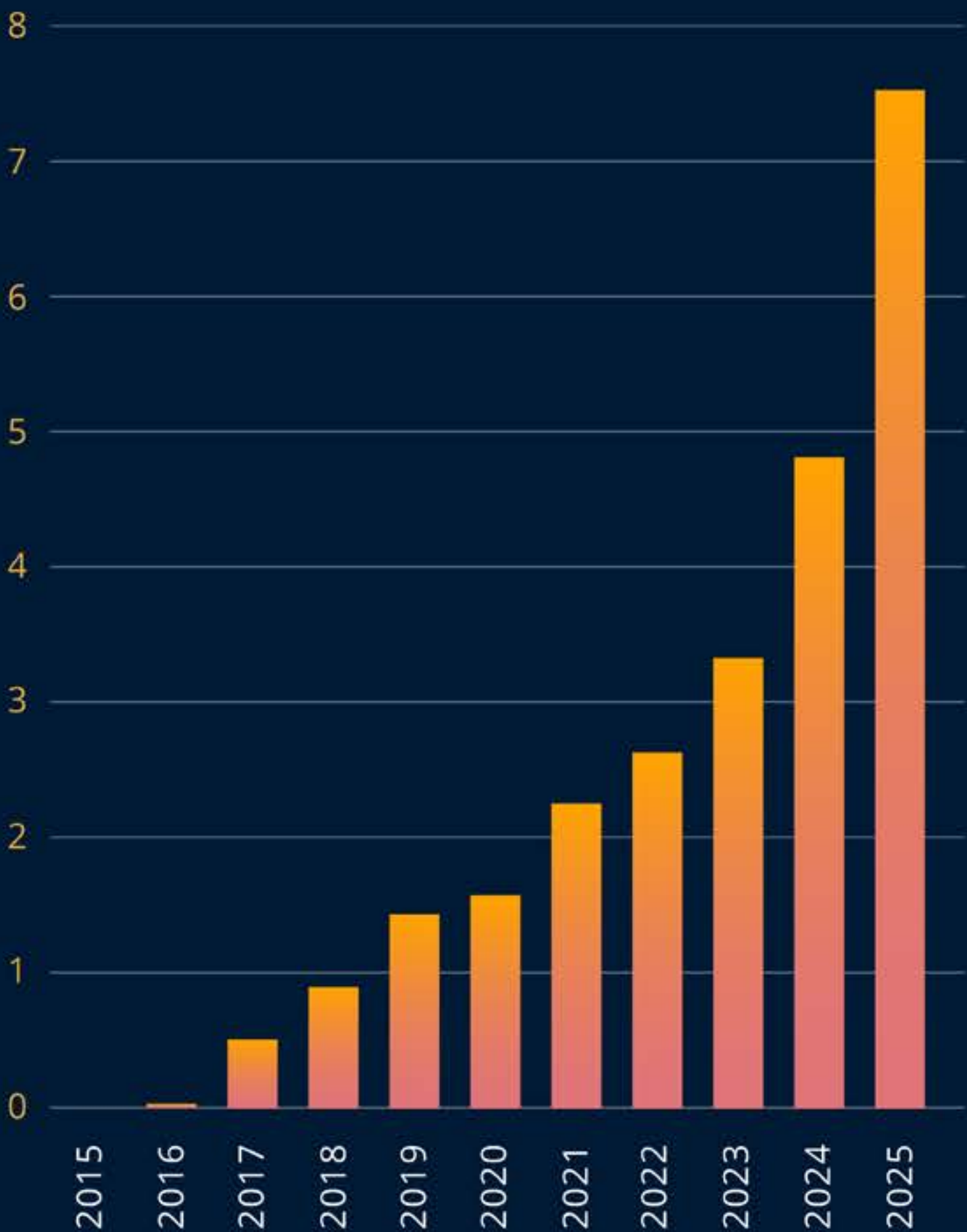
NUMBER OF CERTIFICATES ISSUED, ALL TIME

8,188,959,528

CERTIFICATES ACTIVE, YOY

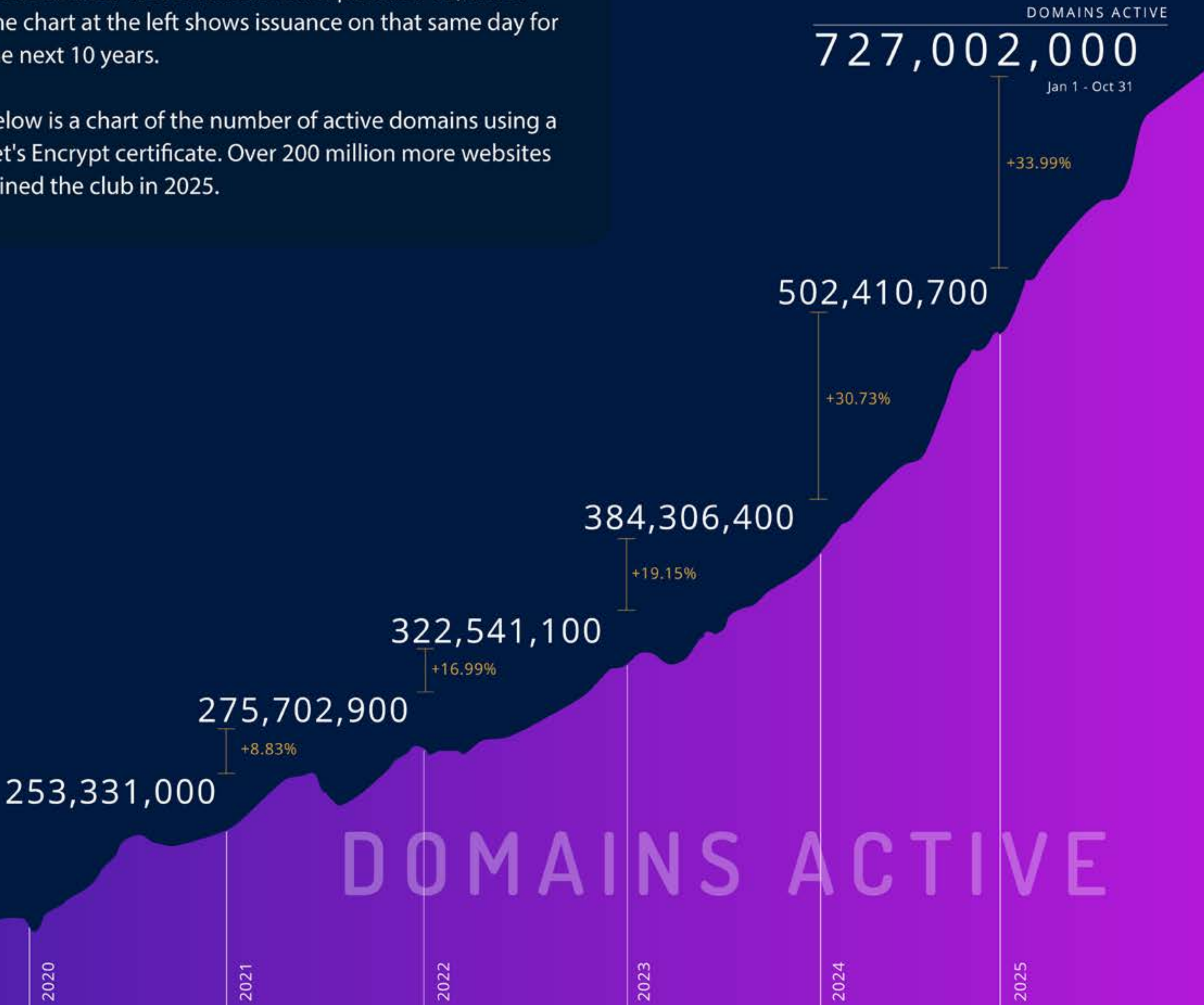


CERTIFICATES PER DAY
(MILLIONS)



We issued our first certificate on September 12, 2015. The chart at the left shows issuance on that same day for the next 10 years.

Below is a chart of the number of active domains using a Let's Encrypt certificate. Over 200 million more websites joined the club in 2025.



DOMAINS ACTIVE

A journey from 90 to 45

INCREASING SECURITY, RELIABILITY, AND AUTOMATION

Let's Encrypt has issued 90-day certificates for our entire history. Despite this lifetime being much shorter than the norm back when we launched, we knew that shorter lifetimes improved security. This concept is still true today, and even shorter certificate lifetimes will be more secure than the 90-day ones. The security ecosystem agrees, with the passage of a [new set of requirements](#) for certificate lifetimes culminating in all publicly-trusted CAs issuing certificates with lifetimes of no more than 47 days by 2029.

In order to move our subscribers forward over the next few years, we will be offering various profiles with different certificate lifetimes in addition to the 6-day and IP address certificates that are available now. Folks who want to jump to 45-day certificates in 2026 will be able to do so via the tlsserver ACME profile. In early 2027 we will move the classic ACME profile to 64-day certificate lifetimes, and a year later we will move that profile to 45 days.

KEY DATES

May 13, 2026: Let's Encrypt will switch our [tlsserver](#) ACME profiles to 45-day certificates by default. This profile is opt-in and can be used by early adopters and for testing.

February 10, 2027: Let's Encrypt will switch our default [classic](#) ACME profile to issuing 64-day certificates with a 10-day authorization reuse period. This will affect all users who have not opted into another profile.

February 16, 2028: We will further lower those profiles to their final configuration, with 45-day certificates and a 7-hour authorization reuse period.



Checklist for decreasing lifetimes

BELT AND SUSPENDERS

Ensure your ACME client uses ACME Renewal Information (ARI). It is a feature that help clients know when they need to renew their certificates.

If your client does not support ARI, ensure your certificates renew at approximately two thirds of the way through the current certificate's lifetime.

Make sure your systems have sufficient monitoring in place to alert appropriately if certificates aren't renewed when expected. There are many available options, check out our Monitoring Service Options page for suggestions.

FRIENDLY REMINDER:

Manually renewing certificates is not recommended, and will need to be done earlier with the shorter certificate lifetimes.



ACME Renewal Information (ARI) published as RFC 9773

The Internet Engineering Task Force (IETF) has published the latest addition to the ACME protocol, **ACME Renewal Information (ARI)**, as RFC 9773. ARI helps keep the renewal process reliable during unexpected events affecting certificate validity. ARI was initially conceived following incident in January 2022 where **we had to revoke approximately two million certificates** due to a technical error in our validation processes. ARI allows a Certificate Authority (CA) to advise a software client to perform an early renewal of a certificate in circumstances where the CA knows that an early renewal is helpful or necessary, even if the client would not yet have anticipated the cert needed to be renewed. In the mass revocation scenario, this allows ARI-aware clients to avoid outages due to certificate invalidity, because they can replace their certificates even before the revocation occurs.

Calling All ACME Client Developers!

Can you add implementing ARI to your 2026 roadmap? We have a handy **blog post** about integrating it and our community forum is always a resource for advice if you get stuck.

Let's make 2026 the year of improved renewals!



Our very shortest certs

SIX DAYS

This year we continued to pursue our commitment to improving the security of the Web Public Key Infrastructure (PKI) by introducing the option to get certificates with 6-day lifetimes. The primary advantage of short-lived certificates is that they greatly reduce the potential compromise window because they expire relatively quickly. This reduces the need for certificate revocation, which has historically been unreliable.

Our 6-day certificates also support including IP addresses as Subject Alternative Names. This will enable secure TLS connections, with publicly trusted certificates, to services made available via IP address, without the need for a domain name.



Ending TLS Client Authentication certificate support in 2026

Today, Let's Encrypt certificates contain two Extended Key Usages (EKUs):

- **TLS Server Authentication:** Used by clients to authenticate TLS Servers, like websites.
- **TLS Client Authentication:** Used by servers to authenticate TLS Clients, like web browsers. This feature is not typically used on the web, and is not required on the certificates used on a website.

In 2026, we will deprecate the Client Authentication EKU in compliance with new root program requirements. If you use Let's Encrypt certificates as client certificates to authenticate to a server, this change may impact you.

February 11, 2026: the default **classic** ACME profile will no longer contain the Client Authentication EKU.

May 13, 2026: the **tlsclient** ACME profile will no longer be available and no further certificates with the Client Authentication EKU will be issued.



Ten years of community support

Let's Encrypt marked ten years of community-driven support that has enabled billions of certificates, expanded ACME automation, and improved security and transparency across the web. This milestone demonstrates how collective action can make encryption accessible for everyone.

  **Welcome to Let's Encrypt Community Support**



system

10  Aug 2015

Community support is a critical part of how Let's Encrypt operates. We're hoping to create a great experience for those with questions and those helping to answer questions.

If you're here with a question, please search to see if your question has been asked before, and [scan the FAQ](#) 53k. Chances are it has. If it hasn't, ask away!

Helping to answer questions here is a great way to contribute to Let's Encrypt. We're a small non-profit organization and our services are provided for free. While we're going to do our best to help answer the questions that people have, we're not going to be able to provide the level of support that a strong community can.

Thank you for visiting. We hope you have a pleasant experience!



The volunteers on the Let's Encrypt forum have made a huge contribution to Let's Encrypt's success. It's easy to imagine that many users might have given up on Let's Encrypt in frustration were it not for the efforts of dedicated volunteers to draw out the necessary details, notice the relevant issues, and patiently explain concepts that were confusing people. There are also volunteer moderators who've worked hard to keep the forum on track, stop spam, and defuse distracting conflicts. Thanks to all of you."

SETH SCHOEN

Community forum participant and early contributor to Let's Encrypt



Two important privacy improvements

ENDING OCSP

This year, we ended support for OCSP. We took this step primarily because it represented a considerable risk to privacy on the Internet. When someone visited a website using a browser or other software that checked for certificate revocation via OCSP, we (or any other Certificate Authority (CA) operating the OCSP responder) immediately became aware of which website is being visited from that visitor's particular IP address. Let's Encrypt never retained this information, but it is possible that other CAs might do so. The maturation of Certificate Revocation Lists (CRLs) has made this risk unnecessary, so it was the perfect time to shed OCSP and move on.

NO MORE SUBSCRIBER EMAIL ADDRESSES

For 10 years, Let's Encrypt sent expiry notification emails to subscribers who provided their email addresses. With more subscribers turning to automation for their certificate management, we decided it was time to remove the millions of email addresses from our database and end that communication. This improves privacy for our users and reduces the operational and financial burden of sending the emails.





PROSSIMO
FOR MEMORY SAFETY

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.



Memory safety for DNS

Prossimo invests heavily in the Hickory DNS project, in part because we believe the Internet needs a high performance and memory safe **Domain Name System (DNS)** resolver, but also because we want to use it for Let's Encrypt. Let's Encrypt performs huge numbers of DNS queries in order to issue millions of certificates per day.

Our work this year focused on improvements to Hickory that will prepare it for large-scale production use. For example, we **improved support for DNSSEC**, which adds digital signatures to DNS zones, allowing records to be authenticated.

We also **added support** for opportunistic encryption (RFC 9539), allowing the resolver to upgrade DNS queries to encrypted channels (DoT/DoQ) when available. This moves DNS traffic toward stronger privacy protections. Support for RFC 9539 opportunistic encryption provides a path toward more routinely protecting the privacy of DNS queries, and a chance to give the DNS community more experience with routine use of DoT and DoQ. Proactively encrypting DNS queries will also improve privacy and security for DNS users in the future when, we hope, Hickory is used by Internet service providers and others as a DNS resolver.

It's time for memory safe TLS



RUSTLS PERFORMANCE IMPROVES, ADOPTION GROWS

Rustls is a low-level software library dedicated to implementing TLS. ISRG has invested heavily in Rustls over the past few years; our goal is 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. We're pleased to report that Rustls **outperforms** OpenSSL and BoringSSL on handshake latency and traffic throughput for connections on the client and the server. This **trend continues** when processing many connections at the same time on a server.

Rustls became a **supported project** of the Rust Foundation this year and we hope that the roster of organizations adopting it will continue to grow.

sudo-rs Adoption in Ubuntu

Every day, system administrators all over the world ask their computers to perform security-sensitive tasks across privilege boundaries, such as a standard user executing a command as root. The software most commonly used to navigate privilege boundaries is sudo.

The original implementation was written in the C language, and has a long history of memory safety vulnerabilities, sometimes allowing any user or software on a system to completely take over that system.

The criticality of this software and the opportunity for improvement through memory safety made sudo a perfect fit for Prossimo. In collaboration with partners, we started planned work for sudo-rs, a Rust implementation, in 2022.

We were thrilled to see that sudo-rs was included in the Ubuntu 25.10 release this year. This release will only be supported until July 2026, but hopefully after that it will be adopted into the Long Term Support release, at which point millions of people will benefit from a more memory safe Ubuntu.

Users on earlier Ubuntu versions, or other popular Linux distributions, can opt in to try sudo-rs.



Privacy for the public's benefit

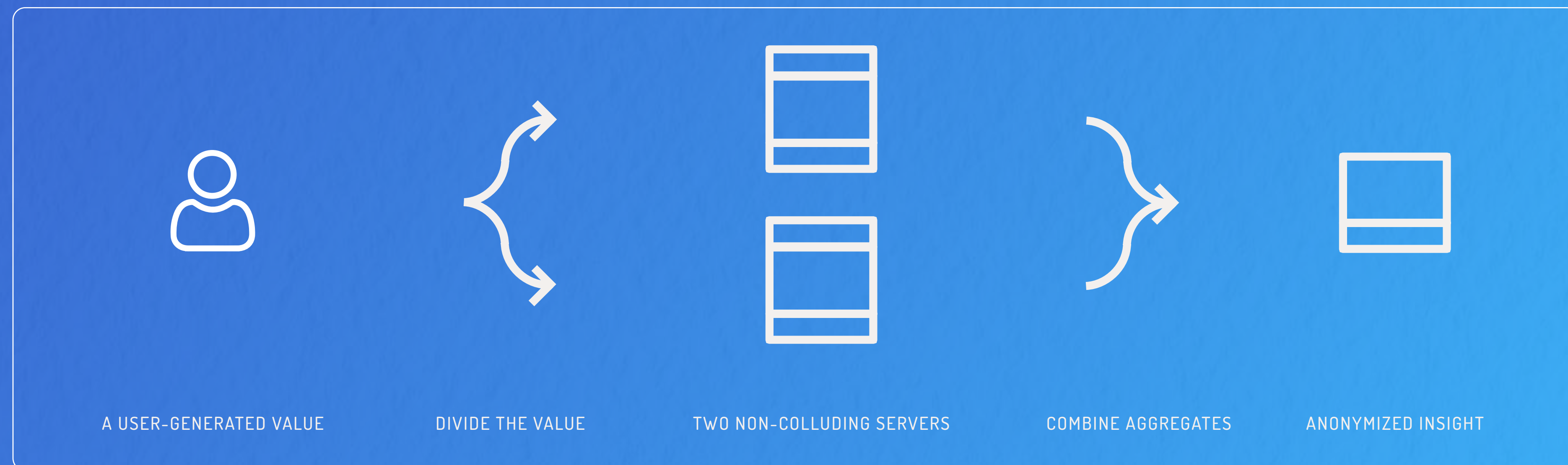
INSIGHTS WITHOUT INTRUSION

Divvi Up is a privacy-preserving measurement solution for applications that prioritizes user privacy. Using the Distributed Aggregation Protocol, 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 and Differential Privacy, provide even greater privacy safeguards for clients.

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 technical deep dive

KEY PRIVACY MECHANISMS: DAP AND VDAF

Divvi Up's privacy-first model is founded on two critical technologies: 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 indistinguishable from 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

BRINGING FURTHER ANONYMIZATION

Divvi Up continues to develop additional solutions towards greater privacy while serving Internet-scale applications. We continued to scale up private aggregation workloads with our subscribers, and applied our privacy enhancing technologies to new use cases.

IMPROVED SCALABILITY

Throughout the year, we have improved the scalability and efficiency of our aggregation software. We made operational improvements, and optimized performance on the diverse workloads that we've seen in practice.

We recently implemented further optimizations incorporating algorithmic improvements developed by our frequent collaborator Armando Faz-Hernandez of Cloudflare. These changes significantly reduce the computational overhead of the Prio3 VDAF, lowering a barrier to adoption for DAP's privacy improvements.

A protocol built with flexibility in mind

A NEW VDAF

Together with our collaborators at Mozilla, we defined a new VDAF called **Prio3L1BoundSum**. This allows for secure private aggregation of new kinds of measurements. It also integrates efficiently with differential privacy, which can safeguard user data even beyond the protections offered by DAP. The specification of the Prio3L1BoundSum VDAF has now been adopted by the IETF Privacy Preserving Measurement working group. This development demonstrates the flexibility and extensibility of DAP.

“

Divvi Up is the ideal DAP partner: phenomenal technical depth, responsive to customer needs, and most importantly, unshakable integrity and reputation. The world is lucky to have such a committed player in the space of privacy-first measurement."

BOBBY HOLLEY

CTO, Mozilla Firefox

Progress toward standardization

HEADING TOWARDS AN IETF STANDARD

The Distributed Aggregation Protocol (DAP) and Verifiable Distributed Aggregation Functions (VDAF) drafts are in the final stages of becoming proposed IETF standards. This is a big deal for the Divvi Up team and our protocol collaborators at Cloudflare, Apple, Mozilla and elsewhere, but these documents are just the beginning. In modern protocol design, we make sure to include extensibility points so that designs can incorporate new ideas and features even after they're finalized. To that end, VDAF is a flexible framework for private aggregation systems, and DAP's API can be extended to accommodate new use cases. Divvi Up is already solving problems in production, but in the years to come, we are optimistic that new work we'll do at the IETF will bring strong privacy guarantees to still more parts of the internet.

We're already working with the IETF community on new VDAFs like Prio3L1BoundSum and Private Inexpensive Norm Enforcement, which respectively enable private cross-site event attributions and machine learning. And work like Late Report Binding Extensions makes DAP more flexible, allowing collectors to better manage their privacy budgets.

ISRG Research: Digital Identity

ZERO KNOWLEDGE PROOFS FROM CREDENTIALS

A growing number of jurisdictions around the world are requiring websites to verify the age of users. Unfortunately, naive technical solutions to this requirement impose significant privacy risks on users. For example, some services store copies of government IDs that can later be leaked if the service is compromised.

Fortunately, modern cryptography provides tools we can use to do better. Zero knowledge proofs enable proving statements about digital credentials without revealing anything beyond the minimum necessary. Instead of showing an entire ID or even a birthdate, a user can prove that they are over 18 without disclosing any other personal details.

At ISRG, we have been researching **Longfellow**, a zero knowledge proof system optimized for proving statements from legacy cryptography like ECDSA with P256 curves and SHA-256 digests. As part of our work on human digital identity, ISRG is collaborating with the scheme's inventors on a specification of the proof system, and our own Rust implementation. Besides deepening ISRG's expertise in these emerging technologies, our partners at the **SIROS Foundation** plan to integrate this work into wwWallet, their European Union Digital Identity wallet.

A zero knowledge proof system is just one piece of a big puzzle, and there's lots of other exciting developments underway in this area. Standards development organizations like the Internet Engineering Task Force are starting to take notice of this problem space, and we also look forward to collaborating openly with industry, academia and government in such venues.



Internet
Security
Research
Group

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.

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 | PRINCIPAL ENGINEER

AMEER | STAFF ENGINEER

ANDREW | SENIOR ENGINEER

BRAD | STAFF ENGINEER

CARRISSA | HEAD OF PEOPLE

DAVID | STAFF ENGINEER

JACOB | PRINCIPAL ENGINEER

JAMES | SENIOR ENGINEER

J.C. | SENIOR ENGINEER

JONATHAN | ASSISTANT DIRECTOR OF ADVANCEMENT

JOSH | EXECUTIVE DIRECTOR

KIEL | STAFF ENGINEER

KRISTIN | GENERAL COUNSEL

LENA | STAFF ENGINEER

LIZ | PEOPLE MANAGER FOR ENGINEERS

MATTHEW | SENIOR ENGINEER

OLENA | FINANCE MANAGER

PHIL | STAFF ENGINEER

PRESTON | STAFF ENGINEER

SALLY | DIRECTOR OF ADVANCEMENT

SAMANTHA | SENIOR ENGINEER

SARAH | VP OF ADVANCEMENT

SARAH | CHIEF FINANCIAL OFFICER

SHANNON | DIRECTOR OF ADVANCEMENT

TIM | PRINCIPAL ENGINEER

Thank You

None of what ISRG has accomplished would be possible without the trust and generosity of our supporters around the world. From corporate sponsors to individual donors and foundation partners, your belief in our mission drives everything we do. Together, we're building a more secure and privacy-respecting Internet, one that serves everyone, everywhere.

Diamond Level Funders



Sovereign Tech Agency



Platinum Level Funders



Gold Level Funders



craig newmark philanthropies



SerpApi



Silver Level Funders



We receive thousands of donations each year that help us run ISRG and its projects. Each donor's motivations differ, but we are connected in our commitment to making the Internet better. We wanted to share the perspectives of a few donors in their own words:



Supporting Let's Encrypt aligns with my belief in a privacy-conscious world, where encrypted communication is the default."



I want to financially support the Prossimo initiative to rewrite critical technical infrastructure in memory-safe languages (such as Rust). I believe this is difficult work that is unlikely to be done at a reasonable pace without engineers working on it full-time."



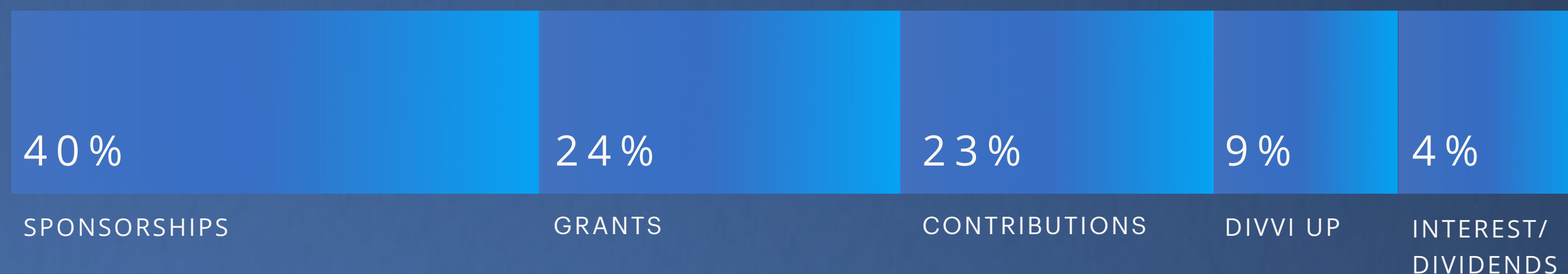
For my 18th birthday, I got my last name as a domain. As a young tech enthusiast with little money, Let's Encrypt made it possible for me to get a TLS certificate and learn about technology. Back then, I was a student using it for free. Now that I have a stable income, donating is my way of giving back and helping others have the same opportunities I did."

Please consider donating if you are able to do so.

D O N A T E

Financials

REVENUE



EXPENSE



PERCENTAGES BASED ON UNAUDITED FINANCIALS JAN-OCT 2025



Let's Encrypt has transformed website security. Just ten years ago, less than 39% of web pages loaded by users were protected with encryption. Today, for most users it's nearly 100%. Digital certificates issued by Let's Encrypt secure more than 700 million websites that are used by governments, businesses, communities, and individuals all over the world, every day.

In that time, Let's Encrypt has also led important enhancements to the certificate ecosystem such as certificate automation, certificate transparency, and memory-safe software. All these features have strengthened the security and resilience of digital certificates."

CHRISTINE RUNNEGAR
ISRG Board of Directors Chairperson

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.



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: abetterinternet.org