2024

ANNUAL REPORT

Fiscal Year 2024
(August 1, 2023 – July 31, 2024)

OpenSSL FOUNDATION

CONTENTS

A Note from our President

MATT CASWELL

Dear Supporters,

Fiscal year 2024 was a year of celebration and transformation for the OpenSSL Foundation. Together with our communities, we celebrated the 25th anniversary of the first OpenSSL software release (version 0.9.1c), which was published on December 23, 1998. Back then, Windows 98 was cutting-edge, Google was only a few months old, and protecting data privacy meant protecting floppy disks. How far we have come!

So much has changed during OpenSSL's lifetime that it was fitting we also took this opportunity to undertake a reform of our organizational structure. Our goal was to put the community at the center of our work, and those changes have been the Foundation's chief focus over the last year. You'll read more about this in the following pages, but the work is still ongoing. We look forward to sharing further updates in the months to come.

The **OpenSSL mission**, adopted shortly before this fiscal year, reads: *We believe everyone should have access to security and privacy tools, whoever they are, wherever they are or whatever their personal beliefs are, as a fundamental human right.* This mission gets to the heart of why we do what we do. We provide online security and privacy tools that enable the free flow of information across boundaries and help everyone, everywhere enjoy freedom of expression, assembly, and association online.

Achieving our mission means not just creating security and privacy tools but getting them into the hands of as many people as possible. We make our security tools available to all, and we are building a large community of volunteers, downstream developers, and users to help us deliver OpenSSL to where it will protect the privacy of everyone. Our library is built into such a wide variety of other products that most people will never know that they are using OpenSSL (either directly or indirectly) in their everyday lives. However, its presence ensures that their privacy is protected nonetheless.

Our mission doesn't stop with just our library though. I am delighted that during the course of this year other projects have also decided to sign up to our mission, and I'm looking forward to working with those Partners in the year ahead.

I feel proud to be associated with such a vital project that is grounded not in the pursuit of profit but in the delivery of security and privacy tools for everyone, everywhere. We could not have achieved what we have without all your contributions. I hope that you too will feel proud and inspired by what we've accomplished together.

Matt Caswell
President
OpenSSL Software Foundation
December 2024

New governance structure

The OpenSSL Software Foundation is one of two entities that supports OpenSSL projects. It is a US registered nonprofit entity, but not at this time a 501c3 charitable organization under US tax law. Financially, the Foundation has relied entirely on the support of corporate sponsors, in-kind contributions, and individual donors.

OpenSSL Software Services (the Corporation) is a separate US registered commercial entity that sells service contracts to companies who pay an annual fee in exchange for guaranteed customer support and other exclusive services related to OpenSSL. Those service fees have long provided the funding to maintain and improve OpenSSL, and they are an important part of the overall revenue strategy for the OpenSSL project's long-term sustainability.

For many years, all OpenSSL staff were contracted by the Corporation (none by the Foundation), and decisions for both entities were made by the OpenSSL Management Committee.

Following a series of meetings and consultations, we adopted several changes to our governance framework. As of March 1, 2024, the Foundation and Corporation's purposes were redefined, with the Corporation focusing on commercial communities and aspects of our mission, and the Foundation focusing on the non-commercial communities and aspects of our mission. The joint Management Committee was disbanded, and decisions are now made by each entity's separate group of elected directors.

The Foundation's directors are:

Matt Caswell
President through February 28, 2026

Tomáš Mráz
Secretary through February 28, 2027

Richard Levitte
Treasurer through February 28, 2025

These directors are now direct hires of the Foundation, giving them the opportunity to focus on our mission to deliver security and privacy tools for everyone, everywhere. This means that we can give even greater attention to the non-profit aspects of our work, including community development and support. It also means that the Foundation is now incurring salary expenses for the first time. While the Foundation will receive some initial financial support from the Corporation, fundraising is becoming more important than ever and will be a major focus of the coming year.

The restructuring also paved the way for a new committee structure with separate Business Advisory Committees (BAC) and Technical Advisory Committees (TAC) for the Foundation and the Corporation. The members of our communities will elect the BACs and TACs, creating a direct channel for community input. The BACs and TACs are on track to be rolled out in fiscal year 2025.

New projects under the mission

Bolstered by alignment around the new OpenSSL mission, we have extended the opportunity for other projects to join us by adopting this mission and, in return, receiving support from the Foundation and Corporation. These Partners are independently governed organizations that share our belief in security and privacy as a human right and with whom we've agreed to have ongoing collaboration.

In addition to our own OpenSSL Library, the other two projects to adopt our mission in the last year are Bouncy Castle and cryptlib.

Bouncy Castle provides open-source cryptographic APIs for Java and C#, FIPS-certified solutions, long-term support releases, and quantum-ready cryptographic support.

cryptlib is a comprehensive security software development toolkit that supports a broad range of security protocols including SSL, TLS, SSH, S/MIME, and PGP.

These collaborations encourage innovation, improve security standards, and help all of us address common challenges more effectively. We are proud to welcome Bouncy Castle and cryptlib to our mission!

1,970 **TOTAL COMMITS** TO THE "MASTER" BRANCH

OpenSSL Project updates

199

UNIQUE AUTHORS
WHO CONTRIBUTED

The OpenSSL Project is run collaboratively by the Foundation and Corporation. In August 2023, we jointly announced a shift in how we release the OpenSSL Library and the adoption of a **time-based release policy**, which became effective in April 2024. Under this policy, new feature releases will be issued in October and April each year. This change of approach aims to make updates more regular and predictable for users while maintaining optimal workflow and efficient resource management.

Releases and updates made in fiscal year 2024 included:

- **November 23, 2023:** OpenSSL 3.2, the first General Availability release of the OpenSSL 3.2 release line. OpenSSL 3.2 implemented a client API (Application Programming Interface) for the **QUIC protocol**, **Hybrid Public Key Encryption** (HPKE), a protocol that aims to provide a flexible and secure way to perform public key encryption in various scenarios. It also added support for **Raw Public Keys** and included a series of new tutorials to help new users get a quick start on developing applications using the OpenSSL libraries.
- **January 23, 2024:** Update to **FIPS 140-2** certificate #4282, which now validates the FIPS provider built from the 3.0.8 and 3.0.9 releases.
- **April 10, 2024:** OpenSSL 3.3, the first regular release made under the terms of our new time-based release policy.
- **April 16, 2024:** Released an early technology preview of our OpenSSL QUIC server functionality to seek feedback from the communities.

In order to further improve transparency and efficiency across all of our communities, we also established **OpenSSL GitHub** as the main source of OpenSSL releases and moved our mailing lists to Google Groups.

Community development and education

One goal of OpenSSL's reorganization was to put the community more at the heart of our work. With that goal in mind, we launched a **YouTube channel** and began offering a regular series of educational webinars and workshops aimed at our users. These efforts also are undertaken collaboratively between the Foundation and Corporation.

Highlights included:

- **OpenSSL Providers Workshops**
  Various dates in December 2023
- **Getting Started with OpenSSL webinar**
  February 6, 2024
- **Writing Your First OpenSSL Application webinar**
  March 28, 2024
- **Writing a TLS Client webinar**
  April 25, 2024
- **Getting Started with QUIC and OpenSSL webinar**
  May 30, 2024

OpenSSL representatives also participated in some important industry conferences to network, share information, and engage our communities, including:

- **International Cryptographic Module Conference (ICMC)**
  September 20-22, 2023 in Ottawa, Canada
  An OpenSSL Update was delivered by Anton Arapov, Engineering Manager at the Corporation and Tomáš Mráz, who is now Public Support & Security Manager at the Foundation.
- **Free and Open Source Software Developers' European Meeting (FOSDEM)**
  February 3-4, 2024 in Brussels, Belgium
  The OpenSSL Corporation hosted a stand at this conference.
- **RSA Conference**
  May 6-9, 2024 in San Francisco, California, USA
  The OpenSSL Corporation attended.

1,043 **PULL REQUESTS** MERGED

Funder Spotlight: Alpha-Omega

Thank you to **Alpha-Omega** for funding an OpenSSL security audit organized by the **Open Source Technology Improvement Fund (OSTIF)**, and carried out by **Trail of Bits** in March/April 2024. The secure code review, including fuzzing enhancements, was performed over a four calendar-week period, for a total of eight engineer-weeks.

The audit focused on the libcrypto component of OpenSSL, looking for potential vulnerabilities or bugs. Overall, auditors found that OpenSSL is defensively implemented and well tested.

There were a total of 24 findings with a security impact, none of which warranted allocating a CVE. Outputs also included the development and addition of 4 fuzzers, a codebase maturity evaluation, and further security hardening guidance.

Thank you to Alpha-Omega for funding this audit, to OSTIF for organizing the audit, and to Max Ammann, Fredrik Dahlgren, Spencer Michael, Jim Miller, and Jeff Braswell from Trail of Bits for their detailed and thorough work.

Corporate sponsors

OpenSSL Foundation is grateful to the following corporate sponsors who provided generous support within the period of August 1, 2023 through July 31, 2024:

Platinum

Bloomberg

Gold

NetApp

Silver

Microsoft

Shiguredo

Bronze

beslist.nl

Mercedes-Benz

Sakura Internet Inc

Financials

In fiscal year 2024, the Foundation had minimal expenses, as most employee costs and other expenses were managed by the Corporation through February 29, 2024. The Corporation also holds a cash reserve that is intended to be shared between the two organizations; conversations about the specifics of how that reserve will be managed are still ongoing. As such, the financials for fiscal year 2024 are not representative of what we expect for future expenses and revenue requirements following the organizational restructure that went into effect on March 1, 2024.

Total revenue

$61,753.01

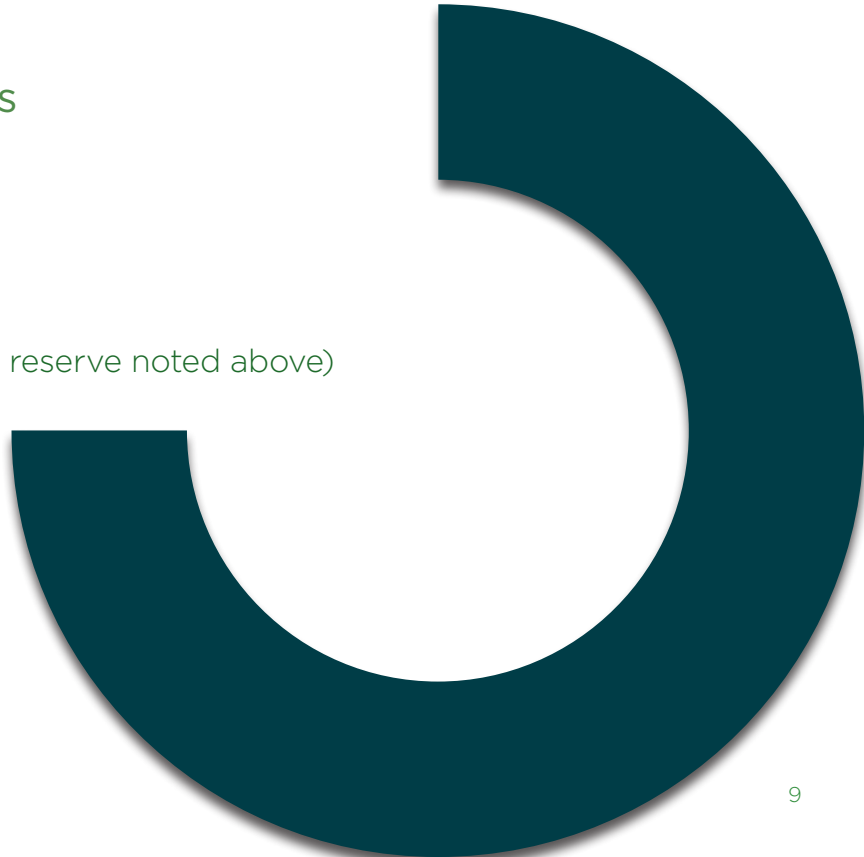
Total expenses

$171,054.55

Bank reserves

$493,817.36

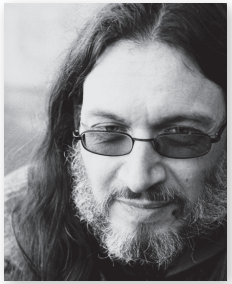
(plus share of cash reserve noted above)



Who we are

Foundation Staff

Matt Caswell
President and
Senior Software Engineer



Richard Levitte
Senior
Software Engineer

Tomáš Mráz
Public Support &
Security Manager
and Senior
Software Engineer

Amy Parker
Chief Funding Officer

Foundation Board of Directors

Matt Caswell, President
March 1, 2024 through February 28, 2026

Tomáš Mráz, Secretary
March 1, 2024 through February 28, 2027

Richard Levitte, Treasurer
June 5, 2024 through February 28, 2025

Previous Board of Directors

The following individuals also served as Foundation Directors during the course of fiscal year 2024:

Anton Arapov
Mark Cox
Tim Hudson

Foundation Members

Anton Arapov
Matt Caswell
Tim Chevalier
Mark Cox
Denis Gauthier
Tim Hudson
Hugo Landau
Richard Levitte
Tomáš Mráz
Kurt Roeckx

Information is accurate as of December 2, 2024.

Stay connected

Your support helps everyone, everywhere have access to security and privacy tools that underpin countless internet connections worldwide.

Stay connected with us by:

- Joining our **online community**
  https://openssl-communities.org/hub/
- Subscribing to our **mailing lists**
  https://openssl-library.org/community/mailinglists/index.html
- Visiting our **YouTube channel**
  https://www.youtube.com/@OpenSSL_
- Connecting with us on **LinkedIn**
  https://www.linkedin.com/company/openssl-software-foundation
- Becoming a **corporate sponsor**
  https://openssl-foundation.org/sponsorship/
- **Contacting us** to explore bespoke sponsorship opportunities
  Email amy.parker@openssl.org
- Making a personal contribution via **Github Sponsors**
  https://github.com/sponsors/openssl

Thank you for sharing our vision of a safer and more secure digital world!


openSSL
FOUNDATION