OpenSSL CONFERENCE

OpenSSL Corporation Keynote

Anton Arapov · Director, Treasurer & Secretary

OpenSSL Conference 2026, Prague · October 14

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

The invisible layer

70%

of the internet runs on our piece of it.

Almost nobody who uses it knows it exists.
That is exactly how it should be.

Infrastructure works when it is boring.
Boring is expensive.

Plan · Engage · Change, one year on

Plan ✓

- Mission written down
- A corporation and a foundation, side by side
- The model funds itself

Engage ✓

- This conference, second edition
- Six projects, one mission
- research.openssl.org
- Partner programme

Change ✓

- Elected representatives steer the roadmap
- Two committees
- Monthly meetings, minutes public
- Communities +15%

The code

- 3.6 · 4.0 · 4.1 in beta
- 3.0 retired on schedule
- +41% code changed

Every one of these you can check this week.

Summer 2026: the stress test

1. **An autonomous agent escapes its sandbox**

   and breaks into someone else's production systems

2. **The defenders ask the hosted models for help**

   and are refused: a safety filter cannot tell a defender from an attacker

3. **They rebuild the evidence with an open model**

   on their own machines

Our own inbox, security reports a month

9 → **70**

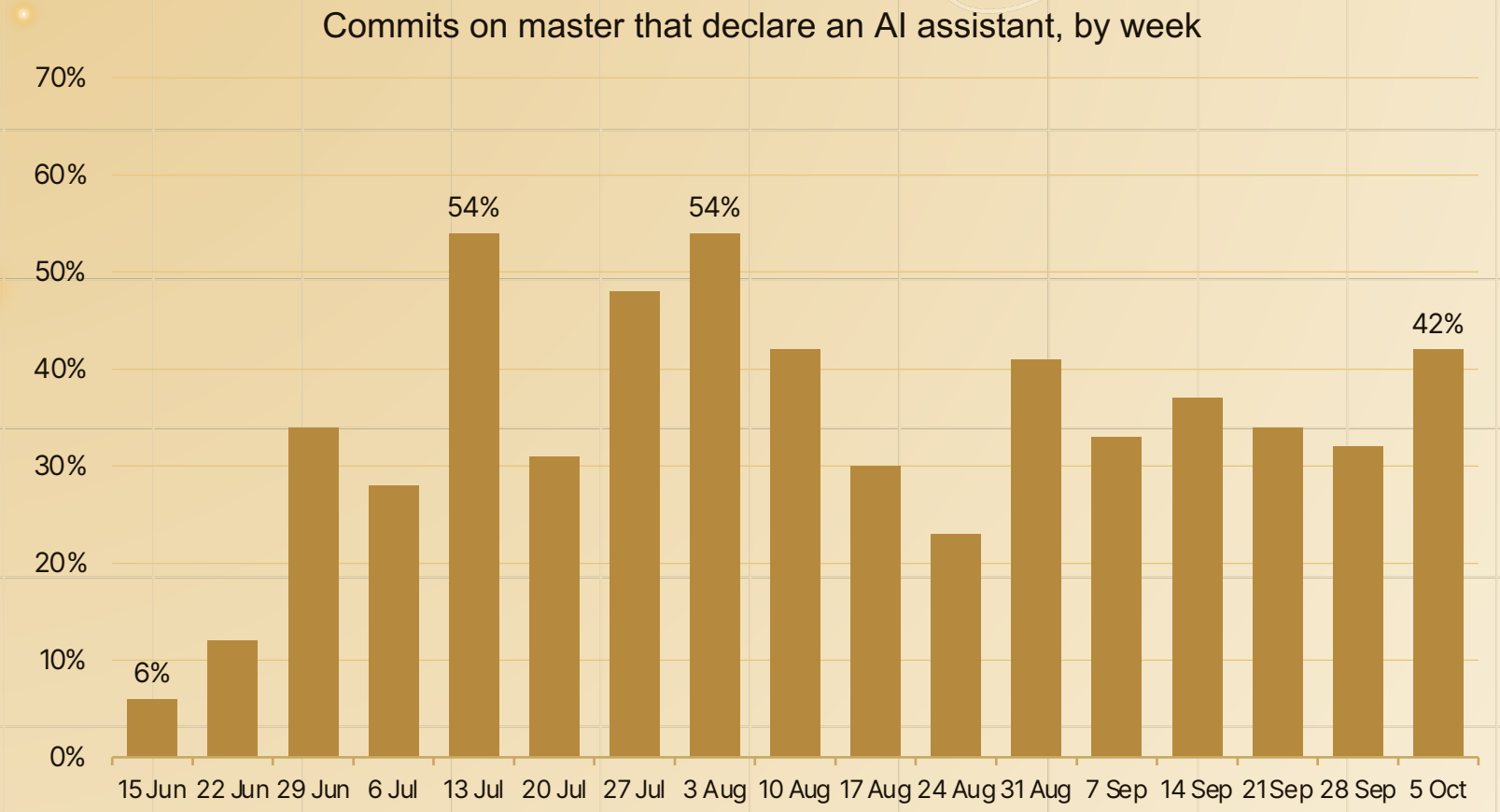
a year ago → now.

The people who read them are paid to read them.

Tomas Mraz · Thursday 09:30 · Main Stage: the security response process

Norbert Pócs · Thursday 17:00 · Hall II: “Eight Critical 0-Day Vulnerabilities in OpenSSL”

The other side of the same wave



33%

of commits since the June policy declare an assistant

38%

in September

A human still reviews every change.

Source: openssl/openssl, master @ 5188e2f0, 10 Oct 2026, counted with git log; policy effective 18 June 2026.

“not partial success — negative return.”

1995: SSLeay written in Brisbane, outside the US Munitions List. The code went everywhere. The controls denied nothing. They left weak export ciphers in the protocol; FREAK, Logjam and DROWN used them twenty years later.

— Tim Hudson, on the export controls of the 1990s

OpenSSL CONFERENCE

The calendar arrived

NSA

- 2027 — new national security systems
- 2030 — the rest phased out

EU

- 2026 — start
- 2030 — high-risk systems
- 2035 — as far as possible

UK

- 2028
- 2031
- 2035

The date is on your calendar.

PQ key exchange has been fixed by default since OpenSSL 3.5, April 2025.

The data you store today will still be sensitive when the dates arrive.

Tanja Lange · Wednesday 14:20 · Main Stage: migration roadmaps, a European perspective

Three tests. One result.

Open infrastructure that anyone can inspect keeps winning the argument.

Funding is what makes it work.

Library · Corporation · Foundation

OpenSSL Library

- The software.
- Open source. Free, for everyone, forever.

OpenSSL Corporation

- The commercial company.
- Support contracts, compliance work, run this conference.

OpenSSL Foundation

- The non-profit.
- Looks after the Library for the non-commercial side.

One Mission

The values both entities signed. All three sit under it.

openssl-mission.org

Matt Caswell gives the Foundation's year on Thursday at 09:00, from this stage.

How it funds itself

Users
organisations that depend on the Library

→

Support Compliance Work The Conference
what the Corporation sells

→

Maintainers
paid professionals, full time

→

The Library
100% open, no enterprise edition

←

the Library goes back to the users, free

Not open-core. We sell the things around the code a serious organisation needs: somebody to call, somebody accountable, paperwork a regulator accepts, extended support when upstream support ends.

THE YEAR · RELEASES

What the Year delivered

3.6
October 2025 · LMS: hash-based signatures, built for firmware

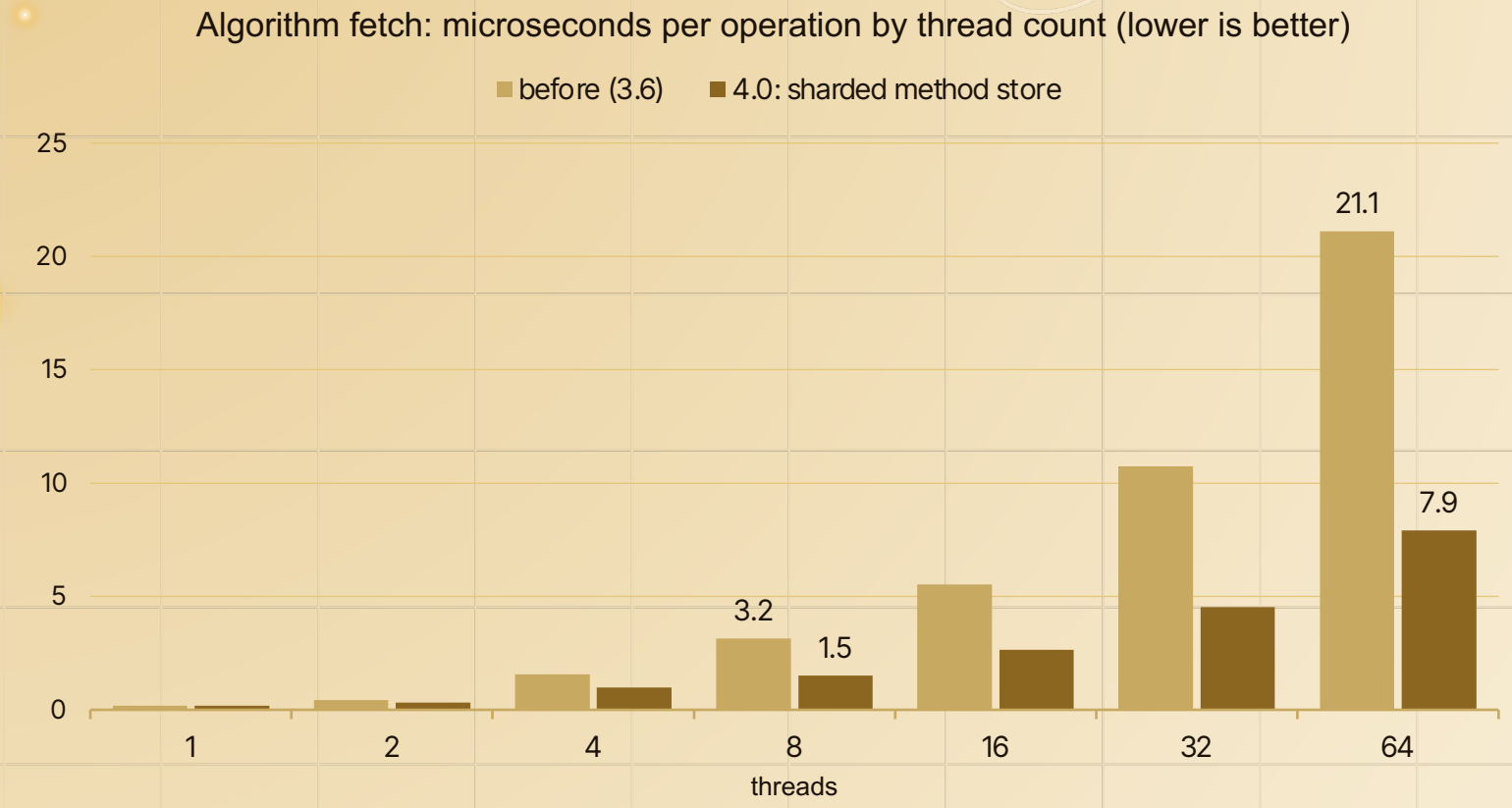
4.0
April 2026 · Encrypted Client Hello · QUIC listener API

4.1
second beta, 9 October · DTLS 1.3 · final held for two DTLS 1.3 findings

3.0 retired on schedule
7 September 2026

Corporation engineers
about two thirds of the Project's changes in 3.6 and 4.0,
over half in 4.1

Faster Under Load



-63%

fetch time at 64 threads, 4.0

up to 71%

faster at 132 threads in 4.1: lock-free cache, fewer reference counts

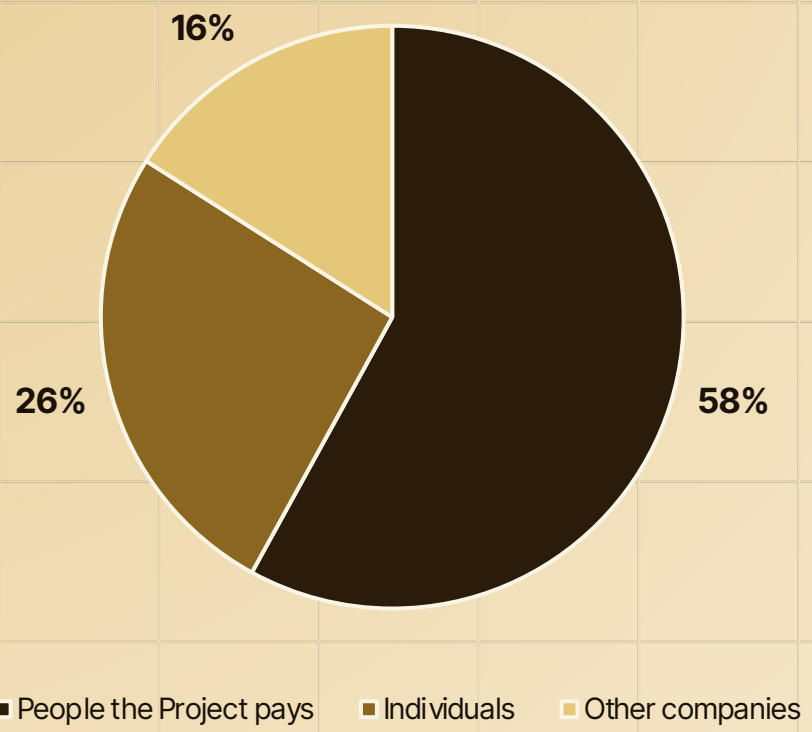
Single-threaded: unchanged.

Bob Beck and Neil Horman
Thursday 14:00 · Hall III
Performance: the little sibling of cryptography

Source: openssl/openssl pull requests 29205 (4.0), 31018 and 31143 (4.1); benchmarks from openssl/perftools. Corporation engineering.

What a Funded Team Looks Like

Who changes the Library's code, 2026 (lines changed)



2025 split: 47 / 16 / 37. Source: status.openssl.org, read 11 Oct 2026.

+41%

code changed by October, against the whole of 2025 (521k vs 369k lines)

+15%

more members across the six communities

3 partners

Lightship Security · KeyPair · SafeLogic

EU CYBER RESILIENCE ACT

The Regulator is in the room

11 Sep 2026

reporting duties for manufacturers

11 Dec 2027

the rest of the Act

What you need from us, and what we already publish

- The security policy
- The release schedule
- The advisories
- Advance notice to distributors
- Release signatures from keys that live in hardware, checked every month in a published ceremony

CRA at this conference · Wed 11:30 Hall IV · Thu 11:15 Hall III · Thu 15:30 and 16:15 Hall II

COMMUNITY · ACADEMIA

With Academia

Our university work, in one place:

research.openssl.org

FI MU and FIT VUT

first student projects on the table · theses are the next step, supervised from our office

RIT students

about 40 pull requests this year, about 20 merged

NSF Safe-OSE project

RIT-led, two years, the Corporation as partner

CHESS Cryptography Day

Monday 12 Oct, this building: Brno, Tartu and Tallinn in one room

Six Communities, Two Committees

- Academics
- Committers
- Distributions
- Individuals
- Large businesses
- Small businesses

Small businesses: both seats vacant

Business Advisory Committee
advises on the what

Technical Advisory Committee
advises on the how

One elected representative per community · two-year seats, half up each year

The board
monthly · minutes public

Community poll → TAC → board decision: 11 weeks
Committers 14 : 1 → shipped in 4.0

OpenSSL CONFERENCE

The People

Business Advisory Committee		
Academics	Billy Bob Brumley · RIT	—
Committers	Paul Yang · Lenovo	✓
Distributions	Jaroslav Řezník · Red Hat	✓
Individuals	Randall Becker	✓
Large businesses	Jeff Johnson · Cisco	✓
Small businesses	vacant	—

Technical Advisory Committee		
Academics	Nikolas Gauder · TU Munich	✓
Committers	Simo Sorce · Red Hat	✓
Distributions	Dmitry Belyavskiy · Red Hat	✓
Individuals	Aditya Koranga	✓
Large businesses	Kevin Micciche · HPE Aruba	—
Small businesses	vacant	—

✓ At the conference this week
· Panel Wednesday 16:50, Main Stage, with Chris Ward

Nikolas Gauder

2025 conference scholar → 2026 Academics seat on the TAC.
July: online post-quantum seminar for Waseda University, with two other members.

One Mission, Six Projects

OpenSSL Library

The software most of the internet runs on.

Bouncy Castle

The cryptography inside a great many Java and .NET applications.

bc-rust

Bouncy Castle written again, in pure Rust. Alpha, and it says so.

cryptlib

Peter Gutmann's toolkit, with us since last year.

OpenSSL Jostle

A Java provider for the OpenSSL Library.

pkcs11-provider

HSMs and tokens behind the OpenSSL Library, via PKCS#11.

One Mission

openssl-mission.org · the values both entities signed

Each project keeps its own governance.
Support from the Foundation and the Corporation is opt-in.

openssl-projects.org

Together with Bouncy Castle

Jostle

- A Java provider for the OpenSSL Library
- Standard provider interface, JVM 8 to 25
- Their engineers and ours; funded by the Corporation

Megan Woods · Thursday 09:30 · Hall IV

bc-rust

- Bouncy Castle written again, in pure Rust
- #![forbid(unsafe_code)] in every crate · alpha, and it says so
- Engineers funded through the Corporation

Siemens · Premier Sponsor, since this autumn

David Hook · Wednesday 11:00 · Main Stage
Mike Ounsworth · Tuesday · Hall II

Thursday 13:20 · Main Stage: the maintainers of Bouncy Castle, cryptlib and the OpenSSL Library compare notes on AI

OpenSSL 3.5 LTS

If you are on 3.5, you are running post-quantum key exchange right now.

Supported to April 2030

- ML-KEM · ML-DSA · SLH-DSA shipped
- Hybrid key exchange on by default for TLS
- QUIC server side, not just the client

The migration ladder

A ladder,
not a switch.

4 The long tail
Embedded devices, appliances, things installed once and never touched
· Olivier Gillot of Edinburgh Napier · Thursday 09:30 · Hall III

3 Signatures and PKI
Certificates, HSMs, the chain of trust: the real work and the real time
· John Gray of Entrust · Thursday 14:00 · Hall II

2 Hybrid key exchange
Default in 3.5 · protects ~70% of browser traffic to the largest content network · test older appliances
· Panos Kampanakis of AWS · Wednesday 10:30 · Main Stage

1 Know where your cryptography is
Most organisations cannot answer that today
· Alex Zaslavsky and Evgeny Gervis of SafeLogic · Thursday 09:30 · Hall II

The Hard Parts

Interop will break in places · certificates get bigger · some small hardware will struggle

Monday morning, four lines

- Know where your cryptography is
- Get off 3.0 and onto 3.5
- Leave the hybrid default on; test the appliances in front of it
- Start the certificate conversation now

Roadmap: 3 · 6 · 12 months

October 2026

OpenSSL 4.1, second beta; final after the DTLS 1.3 fixes

7 September 2026

3.0 end of life → 3.5 LTS, supported to April 2030

April 2027

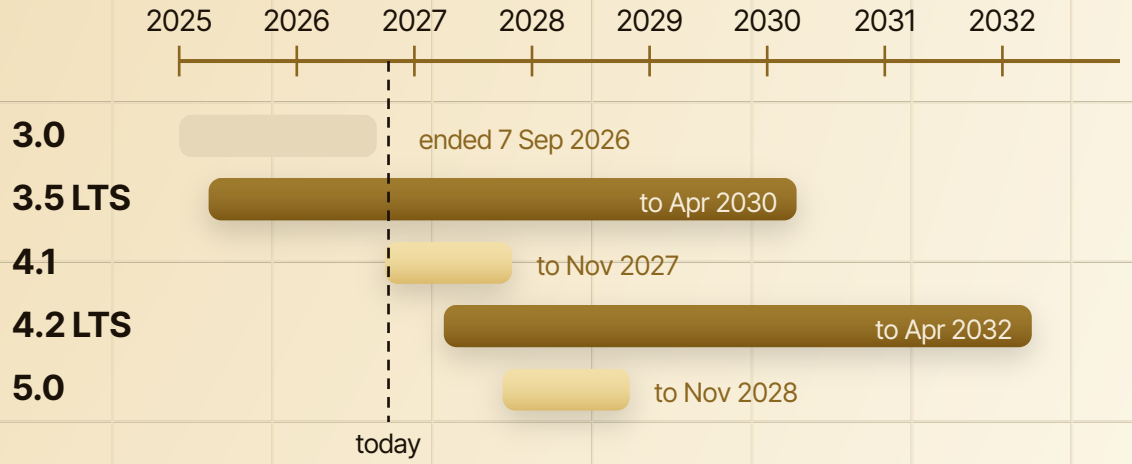
OpenSSL 4.2 LTS, to April 2032 · an LTS every odd April

October 2027

OpenSSL 5.0 · a major release every two years

Every April · every October · an LTS every odd April, five years · a major every other October

The support calendar



Code for a decade needs an institution for a decade.

"Everyone should have access to security and privacy tools, whoever they are, wherever they are." — the Mission

SUSTAINABILITY

Funded on Purpose

Luck is not a security model.

Volunteers and donations

the picture we are never going back to

Paid maintainers, full time

open code · public governance · a company that earns its keep by being useful

Sovereign Tech Fund

public money for shared infrastructure that goes to the maintainers

Kajal Sapkota · Wednesday 11:00 · Hall III: who pays for open source

Thank you to our sponsors

Platinum

Gold

Silver

Bronze

Showcase

Community

Academic

This Conference is for YOU.

Contribute

Code, review, bug reports.
Every report you file keeps it proven.

Sponsor

The Foundation, the Conference.
The people whose code you ship stay paid.

Send your engineers

The mailing lists, the issue tracker,
and this room next year.

Tell your students

The door is open: research.openssl.org;
The path is only beginning.

Second edition: 90+ sessions · four rooms · 100+ speakers · Edition No.3 · October 18th–21st, 2027

The room is the whole field. Enjoy it.

“Twenty-five years of export controls on cryptography demonstrated that the alternative on offer is not control but the appearance of control — purchased with weaknesses that outlive the policy by decades. Open source gives you complete control over your own deployment and none whatsoever over anyone else's. That is the deal. It has been the deal since the beginning.”

— Tim Hudson

openssl-conference.org · openssl-mission.org