OpenSSL CONFERENCE

Fresh Eyes on OpenSSL: A Newcomer's Report

Stefan Eberle

20/10/2026

Purpose of the Talk

What it is

- Personal experience
- Opinion

of a **beginner**

What it is not

- Objective way to improve things
- Solution to a problem

Never implement crypto on your own. Use trusted libraries, because there are a hundred things you can get wrong while implementing it.

- paraphrase from a cryptography beginners lecture

OpenSSL CONFERENCE

How I got into this



- *Studied math and computer science to become a teacher*
- *Attended my first cryptography lectures in Prague*
- *Internship at IBM D Research & Development*
- *Have been trying to understand OpenSSL ever since*

20/10/2026

OpenSSL CONFERENCE

How I started learning

20/10/2026

Framework:

- *9 months time*
- *No prior knowledge of big code bases*
- *A lot of math to understand next to OpenSSL*

OpenSSL CONFERENCE

How I started learning

20/10/2026



OpenSSL CONFERENCE

How I developed

20/10/2026

Developing

- Documentation (= Code)
- Debugger
- Supported by AI

Testing

- Sanity checks
- Unit-Tests
- Openssl's `test`

*OpenSSL requires **thorough understanding** for*

- *Architecture*
- *Side-channel resistance*

Agentic development can't cover this!

Just experience through reading the codebase.

My approach:

Pen and paper proofs, great supervisor, debugging, flowcharts

Main pain points

Getting into the architecture with all its

- *providers*
- *hardware acceleration*
- *different platforms, partially C, various assemblers (Perl)*
- *dispatches, fallbacks, wrapper functions*

Podcast with Pythons Alex Gaynor and Paul Kehrer says that OpenSSL is too overcomplicated

OpenSSL
CONFERENCE

Sweet spots

- *Good documentation for users*
- *Very powerful*
- *Broad and extensible*

- ***Has a well organised conference***

20/10/2026

OpenSSL CONFERENCE

Quo vadis OpenSSL?

§ FRESH EYES ON OPENSSL: A NEWCOMER'S REPORT

20/10/2026

„Review, not authorship, is the scarce resource in this project

- openssl/CONTRIBUTING.md

OpenSSL CONFERENCE

Getting newcomers on board?

20/10/2026

Con

- Flood of AI-generated findings and pull requests
- Security first means gatekeeping

Pro

- Need for a new generation of developers and reviewers
- Fresh knowledge from recent research
- New tooling ideas

OpenSSL
CONFERENCE

What would be helpful for newcomer?

20/10/2026

Resources (developer tutorials, videos, workshops) for newcomers:

- *Overview of architecture*
- *Guide for documentation*
- *Suggestion of tools (OpenSSL speed...)*

→ *Better for **humans** not just for bots*

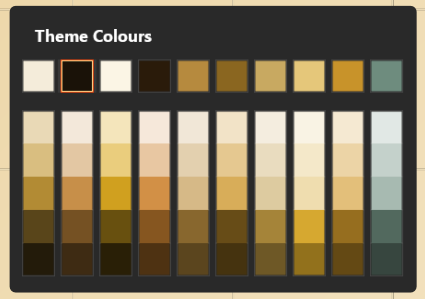
OpenSSL CONFERENCE

Thanks for your time

gap

Presentation Guidelines

- **Mind the gaps**
  - Make sure there is a gap between your added content and the frame's borders.
- **Fonts**
  - Titles: Newsreader **Bold** and *Italic*
    - *Max Size 80, Min Size 36*
  - Body text: Inter Tight
    - Max Size 24, Min Size 12
  - Footer: JetBrains Mono
- **Logo**
  - Nothing should be placed inside the safe zones of the logo.
- **Colours**
  - Avoid using colours that are not predefined in the **Theme Colours**.



gap

gap

gap

OpenSSL CONFERENCE

Lorem ipsum dolor sit amet, consectetur.

Cras id quam sed

Lorem ipsum dolor sit amet

Cras id quam sed ipsum aliquam tristique. Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor, ac tincidunt justo arcu et massa. Vestibulum ante est.

20/10/2026

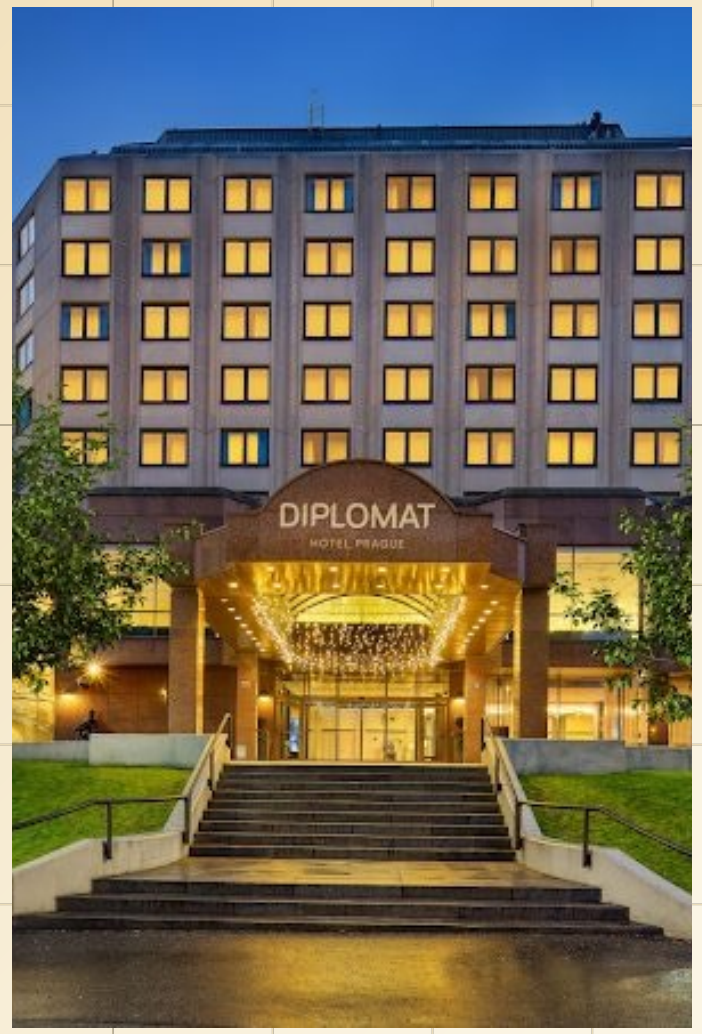
- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Cras id quam sed ipsum aliquam tristique.
- Duis ullamcorper, purus id gravida
- Duis viverra molestie libero vitae
- Nullam sit amet velit eleifend, ornare enim

Lorem ipsum dolor sit amet

Cras id quam sed ipsum aliquam tristique. Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor, ac tincidunt justo arcu et massa. Vestibulum ante est.

20/10/2026

- *Lorem ipsum dolor sit amet, consectetur adipiscing elit.*
- *Cras id quam sed ipsum aliquam tristique.*
- *Duis ullamcorper, purus id gravida*
- *Duis viverra molestie libero vitae*
- *Nullam sit amet velit eleifend, ornare enim*



OpenSSL
CONFERENCE

Lorem ipsum dolor sit amet

Cras id quam sed ipsum aliquam tristique. Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor, ac tincidunt justo arcu et massa. Vestibulum ante est.

20/10/2026

- *Lorem ipsum dolor sit amet, consectetur adipiscing elit.*
- *Cras id quam sed ipsum aliquam tristique.*
- *Duis ullamcorper, purus id gravida*
- *Duis viverra molestie libero vitae*
- *Nullam sit amet velit eleifend, ornare enim*

OpenSSL
CONFERENCE

Lorem ipsum dolor sit amet

Cras id quam sed ipsum aliquam tristique. Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor, ac tincidunt justo arcu et massa. Vestibulum ante est.

20/10/2026



- *Lorem ipsum dolor sit amet, consectetur adipiscing elit.*
- *Cras id quam sed ipsum aliquam tristique.*
- *Duis ullamcorper, purus id gravida*
- *Duis viverra molestie libero vitae*
- *Nullam sit amet velit eleifend, ornare enim*

Lorem ipsum dolor sit amet

OpenSSL CONFERENCE

- *Lorem ipsum dolor sit amet, consectetur adipiscing elit.*
- *Cras id quam sed ipsum aliquam tristique.*
- *Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor.*
- *Ac tincidunt justo arcu et massa. Vestibulum ante est, aliquam nec felis iaculis.*
- *Vestibulum semper ligula. Duis viverra molestie libero vitae commodo.*
- *Aliquam placerat massa vel urna congue fermentum.*
- *Tempor ut sapien id, rhoncus interdum tortor. Fusce auctor lorem non tellus dapibus dictum.*
- *Proin mollis dolor at velit convallis, eu eleifend metus maximus.*
- *Nullam sit amet velit eleifend, ornare enim id, vehicula metus.*
- *Duis fringilla justo metus, eget pulvinar lacus vestibulum nec.*
- *Cras dignissim aliquam rhoncus.*

Lorem ipsum dolor sit amet

- Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Cras id quam sed ipsum aliquam tristique.
- Duis ullamcorper, purus id gravida fringilla, est tortor tristique tortor.
- Ac tincidunt justo arcu et massa. Vestibulum ante est, aliquam nec felis iaculis.
- Vestibulum semper ligula. Duis viverra molestie libero vitae commodo.
- Aliquam placerat massa vel urna congue fermentum.
- Tempor ut sapien id, rhoncus interdum tortor. Fusce auctor lorem non tellus dapibus dictum.
- Proin mollis dolor at velit convallis, eu eleifend metus maximus.
- Nullam sit amet velit eleifend, ornare enim id, vehicula metus.
- Duis fringilla justo metus, eget pulvinar lacus vestibulum nec. Cras dignissim aliquam rhoncus.



Lorem ipsum dolor sit amet, consectetur adipiscing elit.

OpenSSL CONFERENCE

Lorem ipsum dolor sit amet, consectetur.

Proin mollis dolor at velit convallis, eu eleifend metus maximus. Nullam sit amet velit eleifend, ornare enim id, vehicula metus. Duis fringilla justo metus, eget pulvinar lacus vestibulum nec. Cras dignissim aliquam rhoncus.

Lorem ipsum dolor sit amet, consectetur.

Proin mollis dolor at velit convallis, eu eleifend metus maximus. Nullam sit amet velit eleifend, ornare enim id, vehicula metus. Duis fringilla justo metus, eget pulvinar lacus vestibulum nec. Cras dignissim aliquam rhoncus.

Lorem ipsum dolor sit amet, consectetur.

Proin mollis dolor at velit convallis, eu eleifend metus maximus. Nullam sit amet velit eleifend, ornare enim id, vehicula metus. Duis fringilla justo metus, eget pulvinar lacus vestibulum nec. Cras dignissim aliquam rhoncus

Lorem ipsum dolor sit amet, consectetur.

Nunc ut dos orci convallis tortor sollicitudin, in varius ex viverra. Vivamus dictum, dolor in viverra dictum.

Aenean volutpat urna nec cursus vestibulum. Curabitur aliquam mi lacus, id mattis leo aliquet sed. Proin ac purus odio.

„Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris eget aliquet sapien. Praesent vestibulum egestas fermentum. Suspendisse sit amet libero non ligula pretium porttitor. Cras est justo, consectetur et urna ut, faucibus mattis lacus. Suspendisse non tristique erat, sit amet commodo sem. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Integer sed molestie dui. Suspendisse metus risus, tincidunt non ullamcorper id, vulputate commodo ante. Vestibulum semper et ex eu tempus. Nunc mi nunc, lacinia vel neque a, tincidunt congue augue. Maecenas consequat ut ligula non varius.

- Lorem Ipsum, 1998



The Grand Bohemia

night · on the river

