OpenSSL
CONFERENCE

From OpenSSL 3 to OpenSSL 4 in Fedora: true story

Dmitry Belyavskiy, Red Hat, Principal Software Engineer
OpenSSL conference, Prague

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

15.10.2026

Who Am I



- Red Hat Principal Software Engineer
- 20+ years with OpenSSL code
- OTC, Advisory Committees, SRT
- Maintain: OpenSSL, OpenSSH
- Current work: Post-Quantum transition

The distros I work on: from Fedora to RHEL

OpenSSL CONFERENCE

01 / UPSTREAM

Fedora

Community based distribution



ELN

Enterprise Linux Next

→

02 / MIDSTREAM

CentOS Stream

A rolling preview of RHEL



→

03 / DOWNSTREAM

RHEL

Commercial distribution



Why?
Why now?

- Fedora life cycle is short, RHEL is multi-year
- RHEL 11: as late LTS release as possible
- New features in 4.x series
- “Move fast, break things”

Limitations

- 3rd-party packages should work
  - ship also OpenSSL 3
- Minimal churn on update
- Several versions of OpenSSL are possible
- One file path - one package

Subpackages conflicts

Several subpackages, and all are problematic

- Libs: versioned, providers (including folder) is not
- Devel packages: same files with different content
- Command-line utility, OpenSSL-perl, man1/5/7: keep only from 4

Fedora configuration

- Config include snippets: crypto policies, providers
- We ship monolithic OpenSSL 3 config
- Provider snippets folder only for OpenSSL 4
    - Let’s see how good this decision is

Attempt 1 (failed)

- Land OpenSSL 4, OpenSSL 3, and OpenSSH
- Let “them” rebuild
- Result: rollback

Systemic approach

- List of depending packages, rebuild and patch
- Upstream: const and opaque ASN1_STRING

  Downstream: add no-sm3
- Vive la Claude!
- Maintainers don’t like extra patches

Result

- Landed in rawhide in June 2026
- Will be a part of Fedora 45
- 1 beta blocker issue
- Use Kryoptic as a FIPS provider
- Drop most of patches

Lessons learned - organizational

OpenSSL CONFERENCE

- Announce changes early with a test repository
- Avoid pre-release landings
- Coordinate with distro management and get a shepherd
- Report issues unresolved immediately to package maintainers

Lessons learned - technical

OpenSSL CONFERENCE

- Mass-prebuild (note the 'p'!) to establish a repo for the dependent packages.
- Differentiate packages by batches to properly deal with dependencies.
- Curl is the primary focus. Once it is built, most other packages can be built en masse.
- Land changes in the dependent packages before the mass-rebuild (without 'p'!)

Special thanks

- Yaakov Selkowitz
- Stephen Gallagher
- Simo Sorce
- Pavol Zacik

What we want from OpenSSL upstream

OpenSSL CONFERENCE

- Changes are expensive for the whole world
- Care of side-by-side installation
- Distros need longer release cycle
- Other forks API compatibility

