Tao of Open Source Cryptography in China

Paul Yang

OpenSSL Corporation TAC Member

OpenSSL Committer

Agenda

- Background Info
  - Biography
  - Status of OpenSSL in China
- Popular Chinese Cryptography Open Source Projects
  - GMSSL
  - Tongsuo
  - RustyVault
  - openHiTLS
- Future Considerations
  - Trends of crypto open-source project development in China
  - Technologies that have received a lot of attention

Background - Biography

- Paul Yang (洋 Yang, 杨 Yang)
- Started to contribute code to OpenSSL since 2017
- Was invited to be a committer in 2018
- Work Experience
  - Neusoft (2008)
    - Network Security (Firewall, UTM, ADC…)
  - Alibaba/Ant Group (2014)
    - Cryptography
  - ToneFlow (2020): Music Composing/Recording/Mixing
  - Lenovo (2025): Privacy Computing

Background - Biography

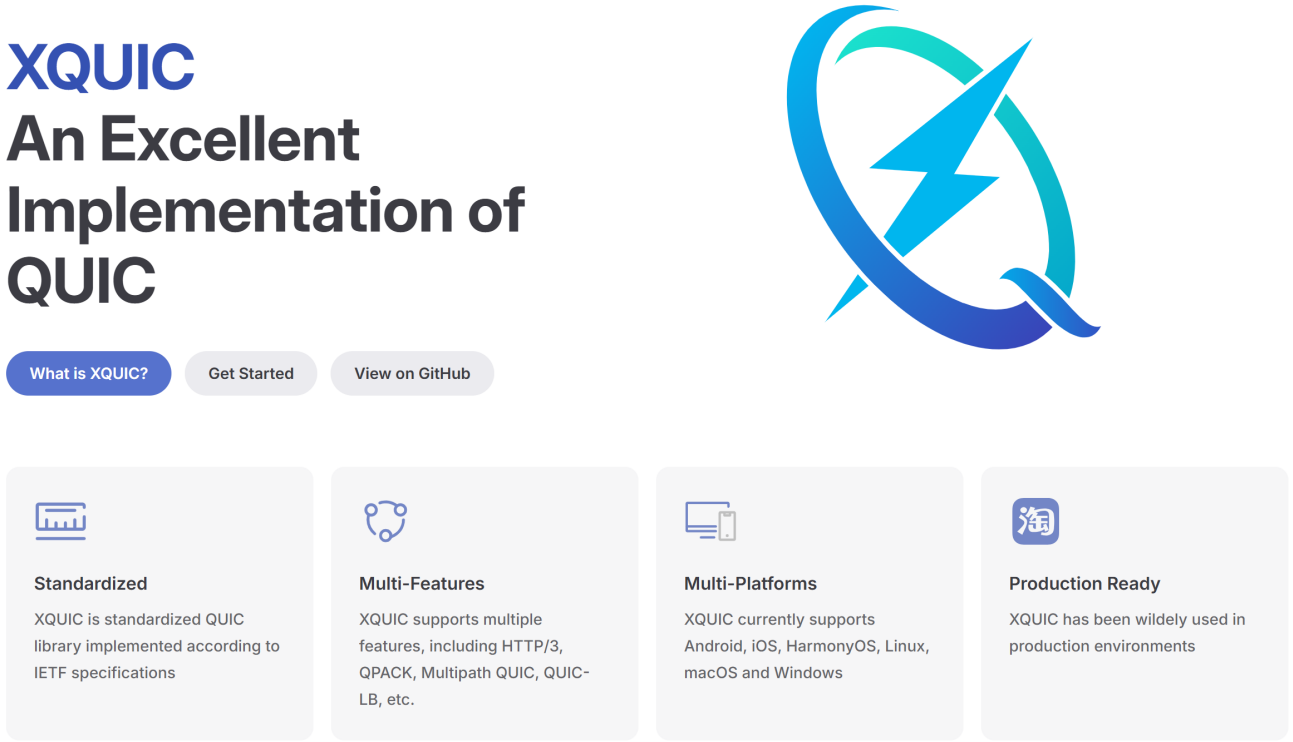
- Elected as a member of the Corporation TAC
  - May, 2025
  - Small Businesses (on behalf of ToneFlow)
- My Contributions to OpenSSL Community
  - Code and reviews
  - First China Tour in 2017
  - Extend the use of OpenSSL in China
  - Connect China regulatory agency with the community
  - Organize meet-ups in China (Doing)
  - Seek for more funds and tech contributions (Doing)

Status of OpenSSL in China (Tech Aspect)

- Features that are heavily used
  - TLS 1.3 and older (libssl)
  - Conventional Cryptography Algorithms (libcrypto)
    - RSA, ECDSA
    - AES
    - SHA series
  - Chinese SM (Commercial Cryptography) algorithms
    - SM2, SM3, SM4
    - X.509 with those algorithms
  - Command-line tools (apps/)
  - Operating systems
    - Linux, iOS, Android
  - Hardware platform: x86, ARM

Status of OpenSSL in China (Tech Aspect Cont.)

- Features that are rarely used
  - DTLS
  - Some Cryptography Algorithms
    - DSA, blowfish, camellia, idea
  - QUIC
    - 3rd-party open source QUIC lib + OpenSSL
  - Provider mechanism
    - Still ’ENGINE’s
  - Other Unix-like systems
    - Most platforms in ‘Configurations’ directory are not used at all
  - Hardware other than x86 and ARM



For instance, Alibaba’s XQUIC
Tencent has its own TQUIC library as well

Status of OpenSSL in China (Tech Aspect Cont.)

- Features that are contributed to OpenSSL
  - Hardware support for domestic CPUs

```
89  +  * Added SHA-2 assembly implementation enhancing performance for LoongArch.
90  +    Added optimized SM3, MD5, SHA-256, SHA-512 implementation using Zbb extension
91  +    for RISC-V.
92  +
93  +    *Julian Zhu*
```

SM4 optimization for ARM by HW instruction `approval: ready to merge` `branch: master` `triaged: feature` 35

#17455 by daniel-hu-arm was closed on Feb 3, 2022 • Review required 2 tasks

SM3 acceleration with SM3 hardware instruction on aarch64 `approval: ready to merge` `branch: master` `triaged: feature` 15

#17454 by zorrorffm was closed on Jan 14, 2022 • Review required 2 tasks

2 Open 16 Closed Author Label Projects Milestones Reviews Assignee Sort

LoongArch: Accelerate SHA-2 message scheduling with LSX `severity: fips change` 6

#28192 opened on Aug 7 by xen0n • Review required

LoongArch perlasm cleanups `severity: fips change` 1

#28191 opened on Aug 7 by xen0n • Review required

LoongArch: Add SHA-2 assembly implementation for better performance `approval: ready to merge` `branch: master` `severity: fips change` `tests: exempted` `triaged: feature` `triaged: performance` 4

#27904 by HeliC829 was closed on Jul 24 • Approved

Make cpuid_setup non-constructor `approval: ready to merge` `branch: master` `severity: fips change` `tests: exempted` `triaged: bug` 9

#27466 by ZenithalHourlyRate was closed on Apr 29 • Approved

LoongArch: Fix output file name detection for Perl scripts `approval: ready to merge` `branch: master` `branch: 3.2` `branch: 3.3` `branch: 3.4` `severity: fips change` `tests: exempted` `triaged: bug` 7

#26717 by xry111 was closed on Feb 14 • Approved

LoongArch: we should access global symbol by la.global instead of la.pcrel `approval: ready to merge` `branch: master` `branch: 3.2` `branch: 3.3` `branch: 3.4` `severity: fips change` `tests: exempted` `triaged: bug` 12

#26336 by ywgrit was closed on Jan 14 • Approved

Define L_ENDIAN for linux64-loongarch64 `approval: ready to merge` `branch: master` `branch: 3.1` `branch: 3.2` `tests: exempted` `triaged: bug` 2

#23064 by xry111 was closed on Dec 18, 2023 • Approved

Add vector support detecting for linux64-loongarch64 `branch: master` `branch: 3.2` `branch: 3.3` `help wanted` `stalled: awaiting contributor response` `tests: exempted` `triaged: bug` 1 14

#23004 by heiher was closed on Jul 12, 2024 • Review required

LoongArch64 assembly pack: Really implement OPENSSL_rdtsc `approval: ready to merge` `branch: master` `severity: fips change` `tests: exempted` `triaged: feature` 5

Status of OpenSSL in China (Market Aspect)

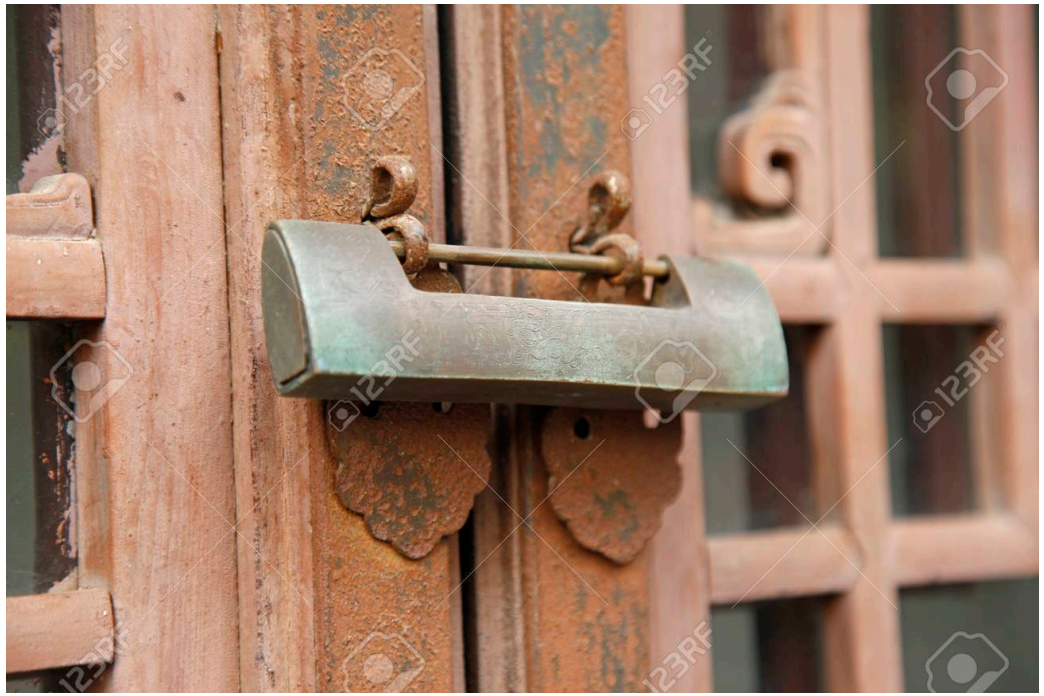
- Still the most popular cryptography library
  - Because it's open source and that means free of charge…
- But mostly limited to TLS and related realms
  - TLS
  - X.509
  - Traditional scenarios like secure network communication (HTTPS, SSH, VPN…), CA systems (digital signatures…), Key management (key-gen…)
- Not too many paid users – currently 0 as I've seen
  - Companies don't have strong will to pay for 'support' in China
  - Companies are keen to hire engineers to hack & even fork OpenSSL
  - Companies buy hardware that comes with software for free

Projects in China - GMSSL

- Forked in 2014, GM stands for (GuoMi, China National Cryptography)
- Initiated by Peking University
- Tech Highlights
  - More comprehensive Chinese SM algorithms support
  - Replaced Perl-based build system with Cmake
  - Move to C99
  - Reduce the memory usage and binary size
  - Enhanced security capabilities for ant-malware and side channel attacks
- Operating Status
  - 5.7K stars, 1.8K forks on GitHub
  - Latest commit: July 31, 2024 (inactive for more than 1 year)

Projects in China - Tongsuo

- Forked in 2019, Ant Group
  - Forked at 1.1.1
  - Then moved to 3.0.2
- Tongsuo means ‘Copper Lock’
- Now the project belongs to OpenAtom Open-Source Foundation



Projects in China - Tongsuo

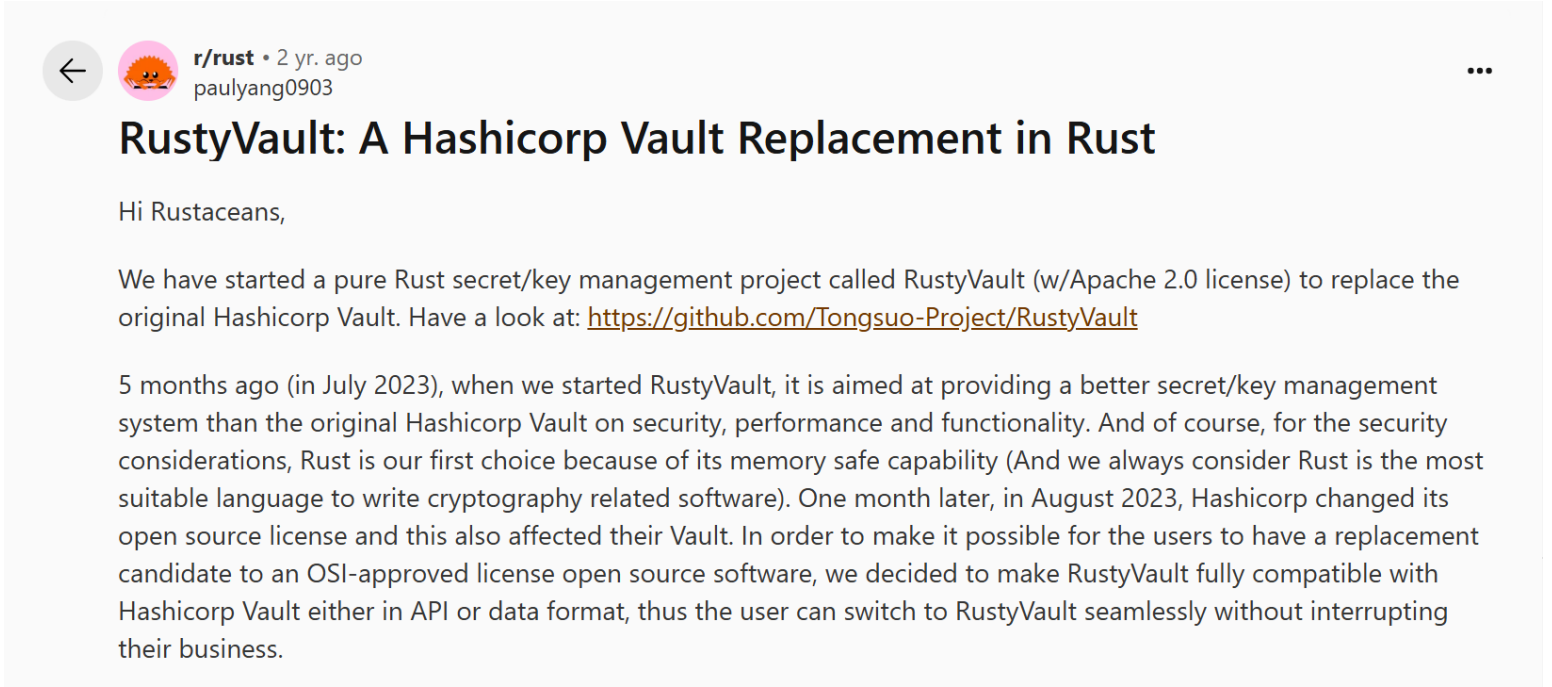
- Tech Highlights
  - Certificated for China regulation compliance
    - Software Cryptographic Module – Security Level 1
  - Combined SM ciphers with TLS (RFC 8998)
  - Co-exist with other OpenSSL versions in one process
  - TLCP (A protocol that compiles to China cryptography regulation)
  - Rarely used algorithms are removed
  - Privacy computing capabilities
    - ZKP: Bulletproofs
    - Partial Homomorphic Encryption: Paillier, EC-ElGamal

Projects in China - Tongsuo

- Covered many scenarios in different industries
  - Alipay
  - Alibaba Cloud Computing
  - ByteDance
  - Lenovo
  - Hygon
  - ……

Projects in China - RustyVault

- Started in 2023, by Ant Group
- A pure Rust written key and secrets management system
- An alternative of Hashicorp Vault



r/rust • 2 yr. ago
paulyang0903

RustyVault: A Hashicorp Vault Replacement in Rust

Hi Rustaceans,

We have started a pure Rust secret/key management project called RustyVault (w/Apache 2.0 license) to replace the original Hashicorp Vault. Have a look at: https://github.com/Tongsuo-Project/RustyVault

5 months ago (in July 2023), when we started RustyVault, it is aimed at providing a better secret/key management system than the original Hashicorp Vault on security, performance and functionality. And of course, for the security considerations, Rust is our first choice because of its memory safe capability (And we always consider Rust is the most suitable language to write cryptography related software). One month later, in August 2023, Hashicorp changed its open source license and this also affected their Vault. In order to make it possible for the users to have a replacement candidate to an OSI-approved license open source software, we decided to make RustyVault fully compatible with Hashicorp Vault either in API or data format, thus the user can switch to RustyVault seamlessly without interrupting their business.

Projects in China - RustyVault

- Tech Highlights
- Switchable underlying cryptography library
  - OpenSSL
  - Tongsuo
- Support for TEE remote attestation
  - As an attestation service
- Work mode
  - Standalone
  - SDK (a Rust crate)

Projects in China - openHiTLS

- Developed from Scratch by Huawei
- Supports many scenarios from embedded to cloud
  - Protocols: TLS1.3, TLS1.3-Hybrid-Key-Exchange, TLS-Provider, TLS-Multi-KeyShare, TLS-Custom-Extension, TLCP, DTLCP, TLS1.2, DTLS1.2 ;
  - Algorithms: ML-DSA, ML-KEM, SLH-DSA, AES, SM4, Chacha20, RSA, RSA-Bind, DSA, ECDSA, ECDH, DH, SM2, DRBG, DRBG-GM, HKDF, SCRYPT, PBKDF2, SHA2, SHA3, MD5, SM3, HMAC etc. ;
  - Highly modular features, support trimming features as required.
  - Algorithm performance optimization based on ARMv8 and x86_64 CPU.

What is the future

- Trends in China
  - PQC
  - Confidential Computing
  - Other Privacy Computing like FHE, DPE, SMPC
  - Hardware Support
  - Rust Language

What is the future

- PQC
  - Call for proposals of NGCC
    - Institute of Commercial Cryptography Standards
    - Next-Generation Commercial Cryptographic Algorithms Program
      - NGCC-PK
      - NGCC-CH
      - NGCC-BC
    - Take Quantum-Resistant into consideration
  - Transition
    - Hard to transit, cost and complexity
    - Software-based solutions will dominate the market
    - Hybrid status will last for a long time

INSTITUTE OF COMMERCIAL CRYPTOGRAPHY STANDARDS
商用密码标准研究院

Next-generation Commercial Cryptographic Algorithms Program (NGCC)

Home > Notice

Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)

2025-02-05

Font size: Big Middle Small

In response to the threat of quantum computing and to promote the standardization of the next-generation commercial cryptographic algorithms, the Institute of Commercial Cryptography Standards (ICCS) is launching a global program to call for proposals for next-generation public-key cryptographic algorithms (NGCC-PK), cryptographic hash algorithms (NGCC-CH) and block cipher algorithms (NGCC-BC), according to the arrangement of Chinese Cryptography Standardization Technical Committee. The candidate algorithms will be evaluated in terms of security, performance and other features, and the finalists will be considered for standardization. ICCS looks forward to global algorithm submissions and comments, and encourages international cooperations in algorithm design.

Further notifications of the program will be released on *www.niccs.org.cn*

What is the future

- Confidential Computing
  - Protect ‘data in use’
  - Becoming popular due to LLM usage
  - Production environment deployment at large scale
    - Nubia – a Chinese smart phone vendor
    - Lenovo
- Other Privacy Computing
  - DPE, Distance-Preserving Encryption
  - SMPC
  - Full Homomorphic Encryption (with hardware acceleration)
  - PSI

What is the future

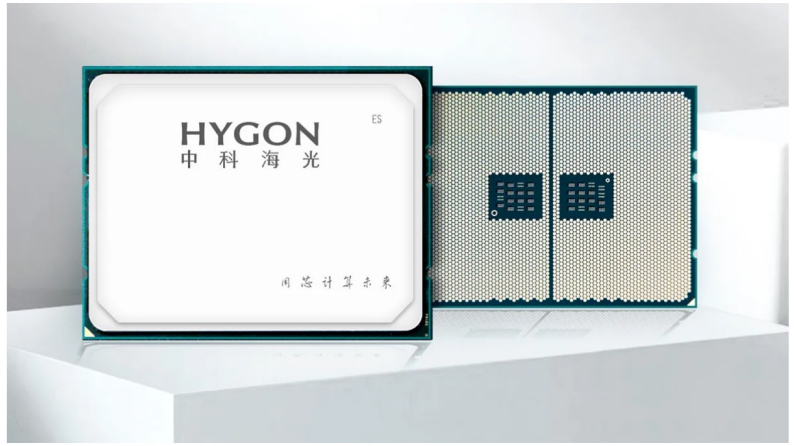
- Chinese CPU and other hardware support
  - Hygon
  - RISC-V
  - Loongson (LoongArch)
  - Phytium
- Built-in cryptography instruction set
- No need to depend on HSMs

Chinese chipmaker readies 128-core, 512-thread CPU with AVX-512 and 16-channel DDR5-5600 support

News By Zhiye Liu published May 9, 2025

Comments (9)

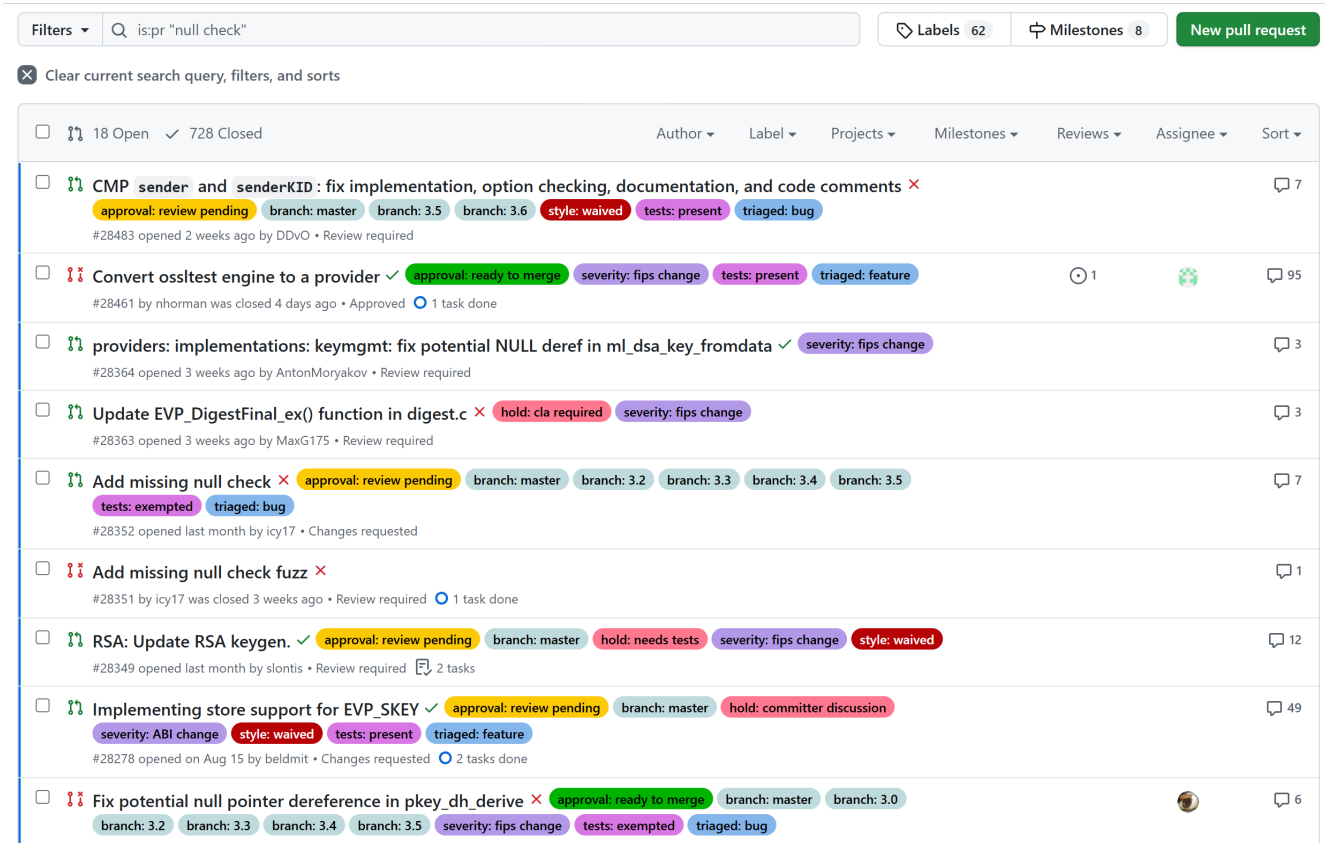
When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.



(Image credit: Hygon)

What is the future

- Avoid unnecessary work
  - 750~ PRs related to NULL check
  - Lots of review comments are addressing NULL check missing
- Rust can help!



What is the future

- Move to Rust
  - Memory safe
  - Fast
- New security open source projects like to use Rust
  - CNCF Confidential Containers
  - RustyVault
  - Ring/Rustls
  - …
- Rust Foundation funds Rustls project

Thanks!

Paul Yang

OpenSSL Corporation TAC Member

OpenSSL Committer