

Evolvability, Deployability, & Maintainability

Proposed IAB Program
IETF 108, July 2020, Virtual



Evolvability

Design for greasing

draft-iab-use-it-or-lose-it, draft-iab-protocol-maintenance

QUIC greasing, HTTP greasing

Explain extension points

e.g., RFC 5507 Design Choices When Expanding the DNS

Which are preferred

Which are stable or ossified

Encourage practices for codepoint allocations that make extension easy

Deployability

Allow working groups to track running code




Catalog implementations and versions

Interoperability results

Active experiments


7 contributors

41 lines (36 sloc)
4.81 KB

[Raw](#)
[Blame](#)




TLS 1.3 Implementations

name	language	role(s)	version	features/limitations
fizz	C++	C/S	RFC 8446	Based on libsodium, includes secure design abstractions. Zero-copy for advanced performance.
NSS	C	C/S	RFC 8446	Almost everything, except some crypto primitives
Mint	Go	C/S	-18	PSK resumption, 0-RTT, HRR
nqsb	OCaml	C/S	-11	PSK/DHE-PSK, no EC*, no client auth, no 0RTT -- live server at tls13test.nqsb.io port 4433, records traces, ping @hannesm , contains a static PSK/DHE_PSK token: id: 0x0000 ► secret:
ProtoTLS	JavaScript	C/S	-13	EC/DHE/PSK, no HelloRetryRequest
miTLS	F*	C/S	RFC 8446	EC/DHE/PSK/0-RTT, no RSA-PSS, no post-HS-auth, no ESNI
Tris	Go	C/S	RFC 8446	ECDHE/PSK/0-RTT, no HelloRetryRequest
BoringSSL	C	C/S	-23, -28, RFC 8446	P-256, X25519, HelloRetryRequest, resumption, 0-RTT, KeyUpdate
Wireshark	C	other	-18 to -28, RFC 8446	Full decryption and dissection support for drafts 19-21 since 2.4.0 (keylog format). Supports 18-21 since 2.4.2, -22 since 2.4.3, -23 since 2.4.5, -24 to -28 (+0RTT trial decryption) since 2.6.0. Tracking bug .
picotls	C	C/S	-18,-21,-23,-26	P-256, X25519, HelloRetryRequest, resumption, 0-RTT
rustls	Rust	C/S	-28 (final on branch)	P-256/P-384/curve25519, HRR, resumption, 0-RTT client
Haskell tls	Haskell	C/S	-28	ECDHE w/ P* and X*, full, HRR, PSK, 0RTT

Implementations

Alessandro Ghedini edited this page on Jun 23 · 415 revisions

[Edit](#)[New Page](#)

This wiki tracks known implementations of QUIC. See also our [Tools listing](#). Current [interop status](#); make sure you are looking at or editing the correct tab.

Please add your implementation below. Keep sorted alphabetically. There are three sections, one for "IETF QUIC Transport", one for "IETF HTTP over QUIC", and one for "QPACK". Entries may appear in multiple sections e.g. where a stack provides both IETF QUIC Transport and IETF HTTP over QUIC.

Note

If you are working on a QUIC implementation, please consider joining the [QUIC Developers Slack Channel](#). Also, if possible, please set up a public server and publish its details below, so others can try and interoperate with your code.

IETF QUIC Transport

The following stacks implement the IETF versions of QUIC Transport. They may include an application layer mapping other than IETF HTTP over QUIC e.g. HTTP/0.9

[aioquic](#)

QUIC implementation using Python and asyncio.

- **Language:** Python
- **Version:** draft-29
- **Roles:** client, server, library
- **Handshake:** TLS 1.3
- **Protocol IDs:** `0xff00001d`, `0xff00001c`
- **Public server:**
 - quic.aiortc.org:443
 - quic.aiortc.org:4434 (Stateless Retry)

AppleQUIC

AppleQUIC is a client and server implementation.

► Pages 38

Top pages

- [Current "Implementation Draft"](#)
- [QUIC Implementations](#)
- [QUIC Tools](#)
- [QUIC Versions](#)
- [Related Activities](#)
- [Temporary IANA Registry](#)
- [QUIC Extensions Interop](#)

Clone this wiki locally

<https://github.com/quic>



The following are known prototype implementations of [draft-ietf-dnsop-svcb-https](#)

Note some prototypes started off using TYPE65479 and other private types but are now switching over to the production types now that the wire format is stable.

Please feel free to submit PRs to update this page.

Production / shipped implementations

(TBD)

Work-in-progress and prototype implementations

BIND9

[Work-in-progress implementation for BIND9](#)

- Author: Mark Andrews <marka@isc.org>
- Tracker: [BIND9 GL 1132](#)
- Version: Implement draft-ietf-dnsop-svcb-https-01 (work-in-progress) ** Previous versions implemented draft-nygren-httpbis-httpssvc-02 (and -01) and draft-nygren-dnsop-svcb-httpssvc-00 ** Previous versions used TYPENN of HTTPS/65482 and SVBC/65481

Unbound

- Prototype of draft-nygren-httpbis-httpssvc-02 during IETF 105 hackathon

dnspython

[Work-in-progress implementation for dnspython.](#)

Others



IETF QUIC Interop Matrix



File Edit View Insert Format Data Tools Add-ons Help



100% \$ % .0 .00 123 Arial 9 B I A

server →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	server →	h2o/quickly	quant	ngtcp2	mvfst	picoQUIC	msquic	f5	f5_test	ATS	quiche	lsquic	nginx-cloudflare	AppleQUIC	quic-go	Quinn	AkamaiQUIC	aiokuic	~gQUIC	wi	Nego	Haskell QUIC	indur
2	client ↓																						
3	h2o/quickly																						
4	quant		VHDCRSQ MBAUPELT	VHDCRSQ MBAU 3	VHDCRZQ MB 3	VHDCRSQ MBAUP 3	VHDCRSQ MBUP	VHDCRSQ UEL 3			VHDCRSQ 3	VHDCRSQ MBAUPE 3	VHDCRZQ 3			VHDCRSQ MBAUPE 3		VHDCRSQ MBAUP 3	VHDCRQ 3			VHDCRSQ MB 3	
5	ngtcp2			VHDCRS MBAU 3dp	VHDCRZ MBA 3d	VHDCRZS MBAU 3		VHDCRZS U 3d			VHDCRS 3	VHDCRZS MBAU 3dp	VHDCR 3			VHDCRZS MBAU 3d		VHDCRZS MBAU 3dp	VHDCRZ 3d			VHDCRZS MBA 3d	
6	mvfst				VHDCRZQ B 3	VHDCRSQ MBAUP 3																	
7	picoQUIC		VHDCRSQ MBAUPLT	VHDCRSQ MBAUT 3	VHDCRZQ MBAT 3	VHDCRSQ MBAUPLT 3	VHDCRSQ MBAUPT	VHDCRSQ UPLT 3		VHDCRSQ MBA 3	VHDCRSQ 3	VHDCRSQ MBAUPT 3	VHDCRQ 3			VHDCRSQ MBAUP 3		VHDCRSQ MBAUPLT 3	VHDCRQ 3			VHDCRSQ MBATL 3	
8	msquic		VHDCRSQ MBUPL		VHDCRZQ MB 3	VHDCRSQ MBAUP 3	VHDCRSQ MBAUP	VHCRSQ U			VHDCRZQ							VHDCRSQ MBUPL				VHCRSQ MB	
9	f5		VHDCS PELT	VHDCS T 3	VHDC T 3d	VHDCS PL 3	VHDCS P	VHDCS PLT 3d		VHDCS L 3	VHDCS 3d	VHDCS PE 3d	VHDC 3d			VHDCS P 3d		VHDCS P 3d	VHDC 3d			VHDCS T 3	
10	f5_test																						
11	ATS																						
12	quiche																						
13	lsquic			VHDCRSQ MAT 3dp	VHDCRQ T 3d	VHDCRSQ MPT 3	V	VHDCRSQ ET 3d			VHDCRSQ 3	VHDCRSQ MPET 3dp	VHDCRQ 3			VHDCRSQ MP 3d		VHDCRSQ MPT 3dp	VHDCRQ 3d			VHDCRSQ 3d	
14	nginx-cloudflare																						
15	AppleQUIC																						
16	quic-go																						
17	Quinn		VHDCRZS BU 3d	VHDCRZS BU 3d		VHDCRZS BU 3	VHDCRZS BU	VHDCRZS BU 3d			VHDCRZS B 3	VHDCRZS BU 3d	VHDCRZ B					VHDCRZS BU 3d	VHDCRZ B 3d			VHDCRZS B	
18	AkamaiQUIC																						
19	aiokuic		VHDCRSQ MBAULT	VHDCRSQ MBAU 3dp	VHDCRZQ MBLT 3dp	VHDCRSQ MBAUPLT 3	VHDCRSQ MBAUPL				VHDCRSQ 3	VHDCRSQ MBAUPT 3dp	VHDCQ 3					VHDCRSQ MBAUPLT 3dp	VHDCRZQ M 3d			VHDCRSQ MBAL 3	
20	~gQUIC		V					VHDCRSQ 3d			VHDCRSQ 3							VHDCRZQ B 3d	VHDCRZQ B 3d				
21	Kwik&Flupke		HDCRZS		HDCRZS 3	HDCRZS 3	HDCRZS				HDCRZS 3					HDCRZS 3		HDCRZS 3					

Maintainability

Support a community of implementers

Current deployment practices

Non-RFC content: wikis and FAQs

Discussion venues

What happens when a working group closes?

TLS Testing Resources

This page lists correctness and safety testing resources for TLS implementations and related software dependencies. It excludes implementation-specific tests.

*Note that **there is no official conformance test suite**.*

- [badssl](#) - Insecure and uncommon server configurations
- [BoGo](#) - Test harness for (D)TLS, supported by BoringSSL and [NSS](#). See [PORTING.md](#) for information about supporting other implementations.
- [TLS Attacker](#) - TLS-Attacker is a Java-based framework for analyzing TLS libraries.
- [tlsfuzzer](#) - Fuzzer and test suite for TLS (SSLv2, SSLv3, v1.0, v1.1, v1.2, v1.3) implementations.
- [Frankencerts](#) - Specially crafted certificates for testing certificate validation code in TLS implementations.

The following tools lists may help identify features or properties of different TLS implementations:

- [SSL Labs Browser and Server Tester](#) - Browser-based tool for checking features of TLS servers and browser implementations.

Tasks

Get representatives from IESG, Tools Team,
broader community

Review successful models in working groups

Review cases where protocols struggle

Output

Write documents

Hold workshops

Build new IETF tools

Provide guidance for WGs and IETF reviews