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

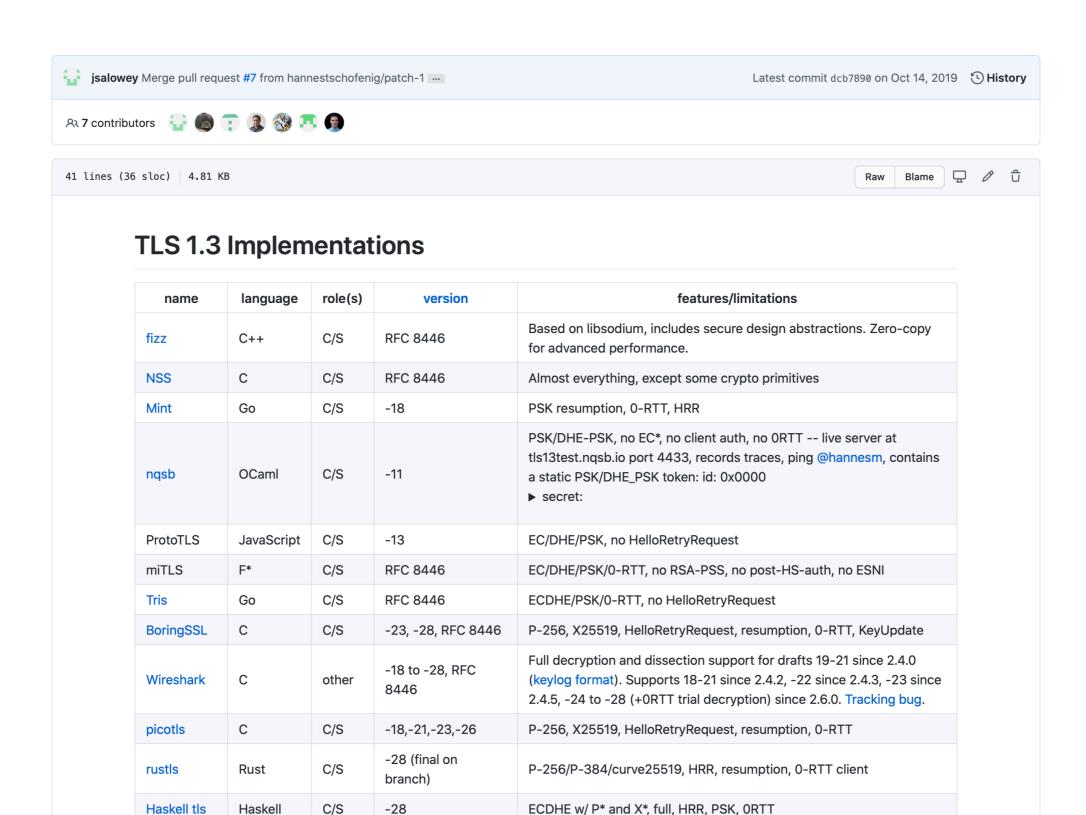
Deployability

Allow working groups to track running code

Catalog implementations and versions

Interoperability results

Active experiments



Implementations

Alessandro Ghedini edited this page on Jun 23 · 415 revisions

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: PythonVersion: 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)

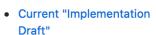
AppleQUIC

AppleQUIC is a client and server implementation.

Edit New Page



Top pages



- QUIC Implementations
- QUIC Tools
- QUIC Versions
- Related Activities
- Temporary IANA Registry
- QUIC Extensions Interop

Clone this wiki locally

https://github.com/quic

56 lines (33 sloc) | 2.05 KB 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-httpbishttpssvc-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.



IETF QUIC Interop Matrix 🔯 🐔 🙆





	server →																				
- `	A A	В	С	D	Е	F	G	Н	1	J	К	L		N O	Р	Q	R	S	Т	U	V
	server →	ri _{si} ,		•		,IIC	.6						cloudti	લું હ		amaiQi	.6	.C.			"anc
	client ↓	nZolanich	quant	ngtcpl	mytst	picoQUIC	rnsquic	4 5	5 t es t	ais	quiche	Isquic	gint clouds.	lete dric-de	Quinn	ama	aioquic	galic	n'i	Hedo	HaskellQUIL
	h2o/quicly																				
	quant		VHDCRZSQ MBAUPELT	VHDCRZSQ MBAU 3	VHDCRZQ MB 3	VHDCRZSQ MBAUP 3	VHDCRZSQ MBUP	VHDCRZSQ UEL 3			VHDCRZSQ 3	VHDCRZSQ MBAUPE 3	VHDCRZQ 3		VHDCRSQ MBAUPE 3		VHDCRZSQ MBAUP 3	VHDCRQ 3			VHDCRZSQ MB 3
	ngtcp2			VHDCRZS 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
	mvfst				VHDCRZQ B 3	VHDCRZSQ MBAUP 3															
	picoQUIC		VHDCRZSQ MBAUPLT	VHDCRZSQ MBAUT 3	VHDCRZQ MBAT 3	VHDCRZSQ MBAUPLT 3	VHDCRZSQ MBAUPT	VHDCRZSQ UPLT 3		DCRZSQ MBA 3	VHDCRZSQ 3	VHDCRZSQ MBAUPT 3	VHDCRQ 3		VHDCRZSQ MBAUP 3		VHDCRZSQ MBAUPLT 3	VHDCRQ 3			VHDCRZSQ MBATL 3
	msquic		VHDCRZSQ MBUPL		VHDCRZQ MB 3	VHDCRZSQ MBAUP 3	VHDCRZSQ MBAUP	VHCRSQ U			VHDCRZQ						VHDCRZSQ MBUPL				VHCRSQ MB
	f5		VHDCS PELT	VHDCS T 3	VHDC T 3d	VHDCS PL 3	VHDCS P	VHDCS PLT 3d	٧	/HDCS L 3	VHDCS 3d	VHDCS PE 3d	VHDC 3d		VHDCS P 3d		VHDCS P 3d	VHDC 3d			VHDCS T 3
	f5_test																				
	ATS																				
	quiche			1//100000	MIDODO	MIDODOO	v	MIDODOO			MIDODOO	1/1/202000	Minono		MIDODOO		MIDODOO	MIDODO			VIIIDODOO
	Isquic			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
	nginx-cloudflare																				
	AppleQUIC .																				
	quic-go		VHDCRZS	VHDCRZS		VHDCRZS	VHDCRZS	VHDCRZS			VHDCRZS	VHDCRZS	VHDCRZ				VHDCRZS	VHDCRZ			VHDCRZS
	Quinn		BU	BU 3d		BU 3	BU	BU 3d			B 3	BU 3d	В				BU 3d	B 3d			B
	AkamaiQUIC																				
	aioquic		VHDCRZSQ MBAULT		VHDCRZQ MBLT 3dp	VHDCRZSQ MBAUPLT 3	MBAUPL				VHDCRZSQ 3	VHDCRZSQ MBAUPT 3dp	VHDCQ 3				VHDCRZSQ MBAUPLT 3dp	M 3d			VHDCRZSQ MBAL 3
	~gQUIC		V					VHDCRZSQ 3d			VHDCRZSQ 3						VHDCRZQ B 3d	VHDCRZQ B 3d			
	Kwik&Flupke		HDCRZS		HDCRZS 3	HDCRZS 3	HDCRZS				HDCRZS 3			HDCRZS			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