FIX-over-TLS (FIXS)

Version 1.1 RC 1

Technical Proposal

February 2021

v0.1

Proposal Status: Pending

For Global Technical Committee Governance Internal Use Only

Submission Date		Control Number	
Submission Status	Submitted	Ratified Date	
Primary Contact Person	Don Mendelson	Release Identifier	

r0.2

DISCLAIMER

THE INFORMATION CONTAINED HEREIN AND THE FINANCIAL INFORMATION EXCHANGE PROTOCOL (COLLECTIVELY, THE "FIX PROTOCOL") ARE PROVIDED "AS IS" AND NO PERSON OR ENTITY ASSOCIATED WITH THE FIX PROTOCOL MAKES ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, AS TO THE FIX PROTOCOL (OR THE RESULTS TO BE OBTAINED BY THE USE THEREOF) OR ANY OTHER MATTER AND EACH SUCH PERSON AND ENTITY SPECIFICALLY DISCLAIMS ANY WARRANTY OF ORIGINALITY, ACCURACY, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SUCH PERSONS AND ENTITIES DO NOT WARRANT THAT THE FIX PROTOCOL WILL CONFORM TO ANY DESCRIPTION THEREOF OR BE FREE OF ERRORS. THE ENTIRE RISK OF ANY USE OF THE FIX PROTOCOL IS ASSUMED BY THE USER.

NO PERSON OR ENTITY ASSOCIATED WITH THE FIX PROTOCOL SHALL HAVE ANY LIABILITY FOR DAMAGES OF ANY KIND ARISING IN ANY MANNER OUT OF OR IN CONNECTION WITH ANY USER'S USE OF (OR ANY INABILITY TO USE) THE FIX PROTOCOL, WHETHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL (INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF USE, CLAIMS OF THIRD PARTIES OR LOST PROFITS OR REVENUES OR OTHER ECONOMIC LOSS), WHETHER IN TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), CONTRACT OR OTHERWISE, WHETHER OR NOT ANY SUCH PERSON OR ENTITY HAS BEEN ADVISED OF, OR OTHERWISE MIGHT HAVE ANTICIPATED THE POSSIBILITY OF, SUCH DAMAGES.

DRAFT OR NOT RATIFIED PROPOSALS (REFER TO PROPOSAL STATUS AND/OR SUBMISSION STATUS ON COVER PAGE) ARE PROVIDED "AS IS" TO INTERESTED PARTIES FOR DISCUSSION ONLY. PARTIES THAT CHOOSE TO IMPLEMENT THIS DRAFT PROPOSAL DO SO AT THEIR OWN RISK. IT IS A DRAFT DOCUMENT AND MAY BE UPDATED, REPLACED, OR MADE OBSOLETE BY OTHER DOCUMENTS AT ANY TIME. THE FPL GLOBAL TECHNICAL COMMITTEE WILL NOT ALLOW EARLY IMPLEMENTATION TO CONSTRAIN ITS ABILITY TO MAKE CHANGES TO THIS SPECIFICATION PRIOR TO FINAL RELEASE. IT IS INAPPROPRIATE TO USE FPL WORKING DRAFTS AS REFERENCE MATERIAL OR TO CITE THEM AS OTHER THAN “WORKS IN PROGRESS”. THE FPL GLOBAL TECHNICAL COMMITTEE WILL ISSUE, UPON COMPLETION OF REVIEW AND RATIFICATION, AN OFFICIAL STATUS ("APPROVED") OF/FOR THE PROPOSAL AND A RELEASE NUMBER.

No proprietary or ownership interest of any kind is granted with respect to the FIX Protocol (or any rights therein).

Table of Contents

Contents

Document History

Revision	Date	Author	Revision Comments
V0.1	Feb 15,2021	Neil Horlock Zyxt Technology Ltd	Initial proposed RC1

1 Introduction

FIX-over-TLS (FIXS) is a technical standard that specifies how to use the Transport Layer Security (TLS) protocol with FIX. It provides some standardisation and ensures a minimum level of security is applied. We believe FIXS will make it easier for FIX participants to employ TLS, and hope that this will help to improve security across the industry.

TLS is a rich protocol with many features and options. The protocol, for example, allows for new security functions to be added and vulnerable functions to be dropped. Additionally, information security is wide and varied. Understanding the TLS protocol features and options is complex and time consuming, and incorrect configuration or management of TLS can result in insecure linkage or no security at all. The FIXS standard therefore aims to make employing TLS simpler, and further provides guidance and best practice that is valid at the time of writing.

FIXS is primary focused on how to use TLS reliably with a minimum level of standardisation across the FIX community. The standard first concentrates on possible methods to authenticate the parties connecting to one another. It then goes into the different aspects of each authentication method as well as the different protocol options and what is recommended. This includes the different available cipher suites as well as certificate properties and validation.

FIXS optionally includes authentication of clients as part of the FIX session. This is termed using FIX User Authentication (FIXA) and it can be used to authenticate FIX clients at the FIX session level rather than authenticating clients at the TLS level.

FIXS does not prevent participants using additional security controls. FIXS defines a minimum set of requirements, which are needed for common use cases and interoperability. Participants may choose to use security controls beyond what is specified in FIXS for extra security or to address the latest vulnerabilities.

Security is only one aspect of using TLS. Another aspect is performance and a further consideration is compatibility with out-of-band monitoring solutions. We therefore try to balance security with the needs of performance and compatibility, in order to keep FIXS suitable for trading and other activities within banking and finance.

1.1 Authors

Name	Affiliation	Contact	Role
Don Mendelson	Silver Flash LLC	Donmendelson@gmail.com	Technical Architect
Neil Horlock	Zyxt Technology	nhorlock@gmail.com	Co-chair FIX Cyber Security Working Group

2 Requirements

2.1 Business Requirements

2.1.1 Promotion to Technical Standard

It is proposed that FIX over TLS (FIXS) version 1.1 published for review as release candidate 1. This will be the first Release Candidate and is intended to inform the community of the directions being assessed by the FIX Cyber Security Working Group, further release candidates are expected.

The Cybersecurity Working Group continues to keep abreast of industry developments. It is expected to produce later versions of this standard, guided by the FIX technical standard process.

2.1.1.1 Public Review

2.1.1.2 Interoperable Implementations

Not applicable at this stage

2.2 Technical Requirements

No new requirements

3 Issues and Discussion Points

Since the publication of version FIXS version 1.0 Draft Standard, version 1.3 of the TLS standard has been standardized, and security technologies advance on other fronts. Meanwhile, older versions of TLS have been deprecated. The Cybersecurity Working Group are reviewing and updating the FIXS1.0 standard with a view to producing V1.1, this release candidate marks the first public view of that update.

This Release Candidate removes the specific inclusion of cipher suites from the standard. Recommended cipher suites will be maintained within the official FIX Protocol Ltd GitHub repository for FIXS, where they can be revised and maintained more regularly as is appropriate to a security focused protocol.

The work to update all sections of the standard to ensure compatibility with TLS1.3 is ongoing. The Cybersecurity Working Group welcome comments from experts and implementers.

4 References

Reference	Version	Relevance	Normative
FIX-over-TLS (FIXS) Technical Specification	Version 1.1RC1	Submitted for review as potential V1.1	Yes

5 Relevant and Related Standards

Related Standard	Version	Reference location	Relationship	Normative
TLS	1.2	https://tools.ietf.org/html/rfc5246		
TLS	1.3	https://tools.ietf.org/html/rfc8446		
FIX	4.2	https://www.fixtrading.org/standards/fix-4-2/	Uses FIXS	Yes
FIX	4.4	https://www.fixtrading.org/standards/fix-4-4/	Uses FIXS	Yes
FIXT	1.1	https://www.fixtrading.org/standards/fix-session-layer/	Uses FIXS	Yes
LFIXT	Nov 2020	https://www.fixtrading.org/standards/fix-session-layer/	Uses FIXS	Yes

6 Intellectual Property Disclosure

Related Intellection Property	Type of IP (copyright, patent)	IP Owner	Relationship to proposed standard
None			

7 Definitions

Term	Definition
FIXA	FIX User Authentication – relates to proposed standardization of common User Authentication practices. This work is not yet finalized.