Superannuation Transaction Network
Binding Implementation Practice (BIP) Note

BIP Note 18

Title:	TLS Configuration and Cryptography Standards	**Date:**	10 Nov 2015
		Version:	1.0
Scope	[x] transport layer [ ] message payload [x] security	**Status:**	[ ] Draft [x] Ratified
		Live Date:	25 February 2016 *On this date this BIP note will be binding on all participants*

1. Change

This document sets requirements for SSL/TLS configuration within the STN.

2. Reason for Change

Secure message exchange within the STN is fully dependent on HTTPS protocol (HTTP over TLS). SSL 3.0 has existed for at least 15 years. It was superseded by TLS 1.0 which was in turn replaced by TLS 1.1 and TLS 1.2. Cryptography standards used in SSL and early versions of TLS are now deprecated and do not provide sufficient level of security.

Clause 6.6(a) of *Superannuation Data and Gateway Services Standards for Gateway Operators transaction within the Superannuation Transaction Network* document requires STN gateways to use "a minimum level of protection of Transport Layer Security (TLS) of version 1.1 or above".

Majority of the STN gateways supports TLS versions 1.0 through 1.2 at the server side (some gateways still support SSL 3.0). However, only a few gateways support modern TLS versions at the client side resulting majority of transactions within the STN being sent through TLS 1.0 channel.

In order to eliminate vulnerabilities of the obsolete SSL/TLS protocols, SSL 3.0 and TLS 1.0 must be completely disabled.

Mozilla Foundation recommends not to include TLS 1.0 into "Modern" configuration set for web-servers and limits its usage only for backward-compatibility purposes (given that STN is P2P network with a limited number of participants, backward-compatibility issue is not relevant).

The updated PCI DSS 3.1 standard specifies a deadline of June 30, 2016, after which SSL and TLS 1.0 must no longer be used by payment gateways and e-commerce applications.

Supported TLS protocol versions are important but not sufficient to achieve the highest standard in cryptography within the STN. The gateways must use strong cipher suites with perfect forward secrecy, disable weak or vulnerable ciphers, use X509 certificates with SHA-256 signatures, etc. This BIP sets requirements to various TLS configuration settings in order to achieve and maintain high security standard within the STN.

3. Standards Affected

Clause 6.6(a) of Superannuation Data and Gateway Services Standards for Gateway Operators transaction within the Superannuation Transaction Network

4. Description of Change

STN gateways must comply with the following requirements:

1. SSL 2.0 and SSL 3.0 protocols must be disabled.
2. TLS compression must not be used (CRIME attack).
3. Vulnerable or weak cipher suites listed in appendix A must be disabled.
4. STN gateways must use TLS 1.2 at the client end when establishing connection to another gateway within the STN over HTTPS.
5. STN gateways should enforce a preferred ordering of cipher suites by the server and prioritize stronger ciphers with Forward Secrecy support as per the guidelines in Appendix B.
6. As soon as each gateway proves its ability to establish TLS 1.2 connection, support of the earlier TLS versions must be disabled all over the STN.
7. STN gateways must use at least 2048-bit RSA or ECDSA private keys on their servers. X509 certificates used in SSL/TLS communication must be issued by a trusted CA (no self-signed certificates allowed). Certificates with expiration dates beyond 1 January 2016 must not contain SHA-1 signature.

BIP Implementation Timeline

Due Date	Requirements
1 April 2016	1, 2 and 3
1 June 2016	4 and 5
1 February 2018	6
1 January 2017	7

The gateways are encouraged to test their SSL/TLS configurations with SSL Labs test suite by Qualys: https://www.ssllabs.com/ssltest/ It is expected that a gateway archives at least 'A-' score.

5. Technical Impact of Change

The gateway operators need to make changes to their web-servers configuration and TLS client implementations.

6. Operational Impact of Change

None.

Appendix A. Prohibited Cipher Suites

The following cipher suites must be explicitly disabled:

IANA Code	Type	Reason for Exclusion
RC4	Block cipher	Weak. As of February 2015, the IETF prohibits the use of RC4
DHE/EDH, DH	Key exchange mechanism	Weak 1024-bit (or less) Diffie-Hellman groups are vulnerable to Logjam attacks. If a server cannot be configured for DH parameters that provide 2048 bits of security or above, all DHE cipher suites must be disabled.
MD5	Hash function	All ciphers using deprecated message digest 5 as the hashing algorithm
LOW, EXPORT	Block cipher	All cipher suites with keys shorter than 128 bits (e.g. DES, RC2)
aNULL	Authentication mechanism	Offer no authentication
eNULL	Block cipher	Offer no encryption

Appendix B. Preferred Cipher Suites

A cipher suite consists of 4 components: a key exchange mechanism (Kx), an authentication mechanism (Au), a block cipher algorithm (Enc) and a one-way hash function (Mac).

Perfect forward secrecy must be achieved by using Diffie-Hellman Ephemeral key exchange with priority given to its elliptic-curve variant (ECDHE) followed by DHE.

Authentication mechanism depends on type of the private key used on the server. Next generation ECDSA keys should be considered over the “standard” RSA keys.

Modern GCM mode of AES cipher should be given priority over conventional CBC mode which is vulnerable to BEAST attack in TLS 1.0. AES 128 is preferred to AES 256 due to speed and resistance to timing attacks. AES 256 security superiority is not evident.

Hash function depends on block cipher being used and TLS version. Generally SHA2 is preferred over SHA1. MD5 is prohibited.

Cipher Suite Components in Order of Preference

Key Exchange	Authentication	Block Cipher	Hash Function
1. ECDHE 2. DHE/EDH	1. ECDSA 2. RSA	1. AES_128_GCM 2. AES_256_GCM 3. AES_128_CBC 4. AES_256_CBC	1. AEAD 2. SHA256 3. SHA384 4. SHA1

Example of Cipher Suite configuration (in order of preference by the server):

1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

2. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
3. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
4. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
5. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256[1]
6. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384[1]
7. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
8. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
9. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
10. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
11. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
12. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
13. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
14. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
15. TLS_DHE_RSA_WITH_AES_256_CBC_SHA[1]
16. TLS_DHE_RSA_WITH_AES_128_CBC_SHA[1]
17. TLS_RSA_WITH_AES_256_CBC_SHA
18. TLS_RSA_WITH_AES_128_CBC_SHA

Version History

Version	Date	Changes	Date Ratified	Live Date
0.1	10 Nov 2015	Initial Version		
0.2	25 Nov 2015	Changes in implementation dates		
0.3	20 Jan 2016	TLS 1.1 support removed as per the feedback; this affects "Superannuation Data and Gateway Services Standards for Gateway Operators". Proposed implementation plan updated.		
0.4	17 Jan 2016	Changes in implementation dates		
0.5	18 Jan 2016	GOG Test Group agreed to push back implementation date for item 6 to 1 February 2018		
1.0	25 Feb 2016	Endorsed by the GOG.	25 Feb 2016	25 Feb 2016

[1] DH Prime must be at least 2048 bits long