IHE Change Proposal

Tracking information:

IHE Domain	IT Infrastructure
Change Proposal ID:	CP-ITI-1151
Change Proposal Status:	Final Text
Date of last update:	Aug 1, 2019
Person assigned:	John Moehrke

Change Proposal Summary information:

ATNA ITI-19 Authenticate-Node clarity – Update options in Vol 1 & 2a	
Submitter's Name(s) and e-mail address(es):	John Moehrke – JohnMoehrke@gmail.com
Submission Date:	September 5, 2018
Integration Profile(s) affected:	ATNA
Actor(s) affected:	Secure Node, Secure Application
IHE Technical Framework or Supplement modified:	ITI TF, Rev 16, July 2019
Volume(s) and Section(s) affected:	Volume 1 and 2a

Rationale for Change:

Since Final Text CP-ITI-1145-01 added the "FQDN Validation of Server Certificate" option and the two BCP195 options in 2018, there is a concern that a product/system will not be able to declare clearly in its IHE Integration Statement what that system has the ability to be configured for, and thus what it can't be configured as. For example: A system that can only support the FQDN Validation option. A system that has no Authenticate-Node capability and thus must be used on a secure network. A system that can only be configured for BCP 195 using TLS 1.2 without ability to downgrade.

Thus, this CP proposes that all possible configurations of ITI-19 be indicated as a named option, and thus from this point forward, all Secure Node or Secure Application systems must declare which one or more of these options that the system can be configured to use.

This presents the problem that Integration Statements prior to this change will not have one of these named options listed. This absence of one of these named options is detectable and shall be interpreted under prior rules. The unfortunate fact is that the prior rules were not all that clear as the prior rule allowed for (a) no TLS at all (use on secured network), (b) some version of TLS with support for crypto algorithm TLS_RSA_AES_SHA. This ambiguity is fact and can't be changed, as changing it would be a breaking change to the specification. We can thus only make the future clearer.

This CP presumes Final Text CP-ITI-1145 linked above --- WITH TWO EXCEPTIONS. (1) removed these ITI-19 options from purely audit actors, as ITI-19 is imposed upon ITI-20 just like any other transaction. (2) The BCP options were in the wrong location in 3.19.6.1 (certificate validation), when they should have been in 3.19.6.2 (the TLS section). **When this CP 1151 passes ballot and is Final Text, then CP 1145 will be Cancelled because it would be superseded by 1151.**

Note that there is now a published TLS 1.3, which I do NOT address in this CP, but we must recognize that it will eventually need to be recognized as adding more options.

Note also that updates for the Audit Consumer in the RESTful ATNA supplement are not addressed in this CP. Whether that is needed is a future consideration.

Lastly, AS4 support should really be recognized in this matrix as well, but I do NOT address it here. Just recognize it would add more options.

Thus, the options are:

0. No Security --> Must be used on a network that provides Node Authentication and Transport Security (Either has no support at all (e.g. no TLS, S/MIME, WS-Security), or can be configured to turn it off)
1. TLS 1.0 / AES --> Classic ATNA assumption
2. TLS 1.0 / AES with Server hostname Validation --> Vassil option on TLS 1.0
3. TLS 1.2 / BPC195 with support down to TLS 1.0 AES
4. TLS 1.2 / BCP195 with support down to TLS 1.0 AES with Server hostname Validation --> BCP195+Vassil
5. TLS 1.2 / BCP195 with TLS 1.2 floor
6. TLS 1.2 / BCP195 with TLS 1.2 floor with Server hostname Validation
7. S/MIME end-to-end security (current section 3.19.6.5)
8. WS-Security - async SOAP security (current section 3.19.6.4)

EDITOR: *Update Vol 1 Sec 9.2 as shown below.*

9.2 ATNA Actor Options

Options that may be selected for this Integration Profile are listed in the Table 9.2-1 along with the actors to which they apply. Dependencies between options when applicable are specified in notes.

Table 9.2-1: ATNA - Actors and Options

Actor	Options	Vol. & Section
Audit Record Repository **(Note 4)**	None	--
Audit Record Forwarder **(Note 4)**	None	--
Secure Node **(Note 1)**	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	FQDN Validation of Server Certificate (Note 2)	**ITI TF-1: 9.2.5** **ITI TF-2a: 3.19.6.1.4**
	STX: No Secure Transport	**ITI TF-1: 9.2.6.1**
	STX: TLS 1.0 Floor with AES	**ITI TF-1: 9.2.6.2**
	STX: TLS 1.0 Floor using BCP195	**ITI TF-1: 9.2.6.3**
	STX: TLS 1.2 Floor using BCP195	**ITI TF-1: 9.2.6.4**
	STX: S/MIME	**ITI TF-1: 9.2.6.5**
	STX: WS-Security	**ITI TF-1: 9.2.6.6**
Secure Application **(Note 1)**	Radiology Audit Trail	RAD TF-1: 2.2.1 RAD TF-3: 5.1
	FQDN Validation of Server Certificate (Note 2)	**ITI TF-1: 9.2.5** **ITI TF-2a: 3.19.6.1.4**
	STX: No Secure Transport	**ITI TF-1: 9.2.6.1**
	STX: TLS 1.0 Floor with AES (Note 3)	**ITI TF-1: 9.2.6.2**
	STX: TLS 1.0 Floor using BCP195	**ITI TF-1: 9.2.6.3**
	STX: TLS 1.2 Floor using BCP195	**ITI TF-1: 9.2.6.4**
	STX: S/MIME	**ITI TF-1: 9.2.6.5**
	STX: WS-Security	**ITI TF-1: 9.2.6.6**

Note 1: Secure Node and Secure Application SHALL support at least one of the "STX" (Secure Transport) options.

Note 2: The "FQDN Validation of Server Certificate" Option is only applicable to TLS-based Secure Transports.

Note 3: "STX: TLS 1.0 with AES" interoperates with "STX: TLS 1.0 Floor using BCP195".

Note 4: The Audit Record Repository and Audit Record Forwarder shall also support Secure Node or Secure Application. See Section 9.3.

EDITOR: *ADD Vol 1 Section 9.2.5*

Note: This new section was originally approved in CP-ITI-1145 (Ballot 49). It is unchanged by this CP, but this CP is adding the section because 1145 is now cancelled & superceded by this CP.

9.2.5 FQDN Validation of Server Certificate Option

The FQDN Validation of Server Certificate Option applies the rules presented in RFC6125 when a client authenticates the server using an X.509 certificate in the context of Transport Layer Security (TLS).

In an environment where clients have implemented this option, a server's X.509 certificate shall contain a subjectAltName entry of type DNS-ID, per RFC6125 Section 4.

See ITI TF-1: 9.4.1.2.2 and ITI TF-2a: 3.19.6.1.4.

Note: IETF Best Current Practice BCP195 recommends, but does not require, FQDN validation.

When an actor implements this option, it need not be capable of functioning without this validation.

EDITOR: *in Vol 1, add new Section 9.2.6 and subsections*

9.2.6 Secure Transport (STX) Options

At least one of the STX options shall be supported. A system may support many options, for which the system must then be configurable to enable each option.

Whether a particular network configuration is secure, or not, is a local policy decision, which should consider an ever-evolving risk landscape. A deploying organization will decide for themselves the best use of technology to enable secure and authenticated communications.

The following sections contain the requirements when a system is configured to utilize each option.

9.2.6.1 STX: No Secure Transport Option

The system must be used on a network that provides secure transport, such as a physically isolated network, Virtual Private Network (VPN), or some other method.

9.2.6.2 STX: TLS 1.0 Floor with AES Option

TLS 1.0 will be used with support for RSA authentication, AES encryption, and CBC SHA for integrity protection.

See ITI TF-2a: 3.19.6.2.1.

9.2.6.3 STX: TLS 1.0 Floor using BCP195 Option

Actors that support this option have the ability to both:

- Operate with the highest level of protection for the TLS-protected communication channel by adopting the IETF Best Current Practice (BCP195), and

- Continue to interoperate with systems that do not support BCP195, by downgrading from TLS Version 1.2 to TLS Version 1.1 or Version 1.0 and/or to less secure cipher suites under specific conditions that are allowed by BCP195.

This option adopts valuable recommendations from the IETF BCP195 while providing flexibility when communicating with an installed base.

An actor that supports the STX: TLS 1.0 Floor using BCP195 Option shall be able to comply with BCP195 with the additional restrictions enumerated in ITI TF-2a: 3.19.6.2.2.

9.2.6.4 STX: TLS 1.2 Floor using BCP195 Option

Actors that support this option have the ability to both:

- Operate with the highest level of cyber protection for the TLS-protected communication channel per the IETF Best Current Practice (BCP195 with TLS 1.2 and selected cipher suites), and
- Restrict to the use of TLS version 1.2 [RFC5246] or higher.

This option adopts valuable recommendations from the IETF BCP195 and prohibits less secure behavior. It is well suited for ensuring a high level of cyber protection.

An actor that supports the STX: TLS 1.2 Floor using BCP195 Option shall be able to comply with BCP195 with the additional restrictions enumerated in ITI TF-2a: 3.19.6.2.3.

9.2.6.5 STX: S/MIME Option

The system will utilize S/MIME to protect the message for authentication of sender, restriction to specific recipients, encryption, and integrity protection. See ITI TF-2a: 3.19.6.5.

9.2.6.6 STX: WS-Security Option

The system will utilize WS-Security WS-I Basic Security Profile 1.1 to protect the message for authentication of sender, restriction to specific recipients, encryption, and integrity protection. See ITI TF-2a: 3.19.6.4.

EDITOR: *Update Section 9.3*

9.3 ATNA Required Actor Groupings

An actor from this profile (Column 1) shall implement all of the required transactions and/or content modules in this profile ***in addition to*** all of the transactions required for the grouped actor (Column 2).

Table 9.3-1: ATNA - Required Actor Groupings

ATNA Actor	Actor to be grouped with	Reference	Content Bindings Reference
Audit Record Repository	Consistent Time / Time Client	ITI TF-1:7	N/A

ATNA Actor	Actor to be grouped with	Reference	Content Bindings Reference
	Secure Node or Secure Application	**ITI TF-1:9**	**N/A**
Audit Record Forwarder	Consistent Time / Time Client	ITI TF-1:7	N/A
	Secure Node or Secure Application	**ITI TF-1:9**	**N/A**
Secure Node	Consistent Time / Time Client	ITI TF-1:7	N/A
Secure Application	Consistent Time / Time Client	ITI TF-1:7	N/A

EDITOR: *Update Vol 2a Section 3.19.3*

Note: These changes were approved in CP-ITI-1145 (Ballot 49). They are unchanged by this CP and are included in this CP because 1145 is now cancelled & superceded by this CP.

3.19.3 Referenced Standards

DICOM:

- PS3.15 Security Profiles. Annex B1: The Basic TLS Secure Transport Connection Profile.

IETF:

- RFC2246 - Transport Layer Security (TLS) **Protocol Version** 1.0 ~~**and later revisions**~~
- **RFC4346 - Transport Layer Security (TLS) Protocol Version 1.1**
- **RFC5246 - Transport Layer Security (TLS) Protocol Version 1.2**
- ~~**RFC7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**~~
- RFC3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
- **RFC6125 - Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)**
- **BCP195 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), MAY 2015**

ITU-T:

- Recommendation X.509 (03/00). “Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks"

WS-I:

- **WS-Security WS-I Basic Security Profile 1.1**

EDITOR: *Update Vol 2a Section 3.19.6.1.1 and add new Section 3.19.6.1.2.*

Note: These changes were approved in CP-ITI-1145 (Ballot 49). They are unchanged by this CP and are included in this CP because 1145 is now cancelled & superceded by this CP.

3.19.6 Message Semantics

…

3.19.6.1.1 Other Certificate requirements

The certificates used for mutual authentication shall be **X.509** ~~**X509**~~ certificates based on **either**:

- RSA key with key length in the range of 1024-4096, where the key length chosen is based on local site policy~~**, or**~~
- **BCP195 certificate recommendations.**

Maximum expiration time acceptable for certificates should be defined in the applicable security policy. The IHE Technical Framework recommends a maximum expiration time of 2 years.

The method used to determine whether a node is authorized to perform transactions is not specified. This may be use of a set of trusted certificates, based on some attribute value contained in the certificates, access control lists, or some other method. Using a certificate chain back to an external trusted certificate authority to determine authorizations is strongly discouraged.

3.19.6.1.2 FQDN Validation of Server Certificate Option

The FQDN Validation of Server Certificate Option applies the rules presented in RFC6125 when a client authenticates the server using an X.509 certificate in the context of Transport Layer Security (TLS).

A client, who is validating a server's identity, shall validate that the reference identifier present in a subjectAltName entry of type DNS-ID matches the source domain of the server, per RFC6125 Section 6. Note that the rules described in RFC6125 Section 6 require the validation to be performed based on the input source and the DNS-ID fully-qualified domain name.

In an environment where clients have implemented this option, a server's X.509 certificate shall contain a subjectAltName entry of type DNS-ID, per RFC6125 Section 4.

EDITOR: *Update Vol 2a Section 3.19.6.2 as follows.*

3.19.6.2 All Connections carrying Protected Information (PI) using TLS

This section contains TLS requirements.

~~**When configured for use on a physically secured network, the normal connection mechanisms may be used.**~~

~~**When configured for use not on a physically secured network implementations shall use the TLS protocol, and the following ciphersuite shall be supported:**~~

~~**TLS_RSA_WITH_AES_128_CBC_SHA.**~~

~~**The recommended "well-known port 2762" as specified by DICOM shall be used when the Secure node is configured for use not on a physically secured network. When the secure node is configured for use on a physically secured network, a different port number shall be used, preferably the standard port 104. HL7 does not specify port numbers, but the port number used when configured for use on a physically secured network shall be different than the port number used when configured for use not on a physically secured network.**~~

~~**All Secure Nodes shall be configurable for use on a physically secured network or not on a physically secured network. If Secure Node is configured for physical security, then it may use the non-TLS DICOM port and protocol.**~~

~~**See RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" for recommendations on proper use of TLS and appropriate fallback rules.**~~

EDITOR: *Update Vol 2a Section 3.19.6.2 to add the following new subsections: 3.19.6.2.1, 3.19.6.2.2, and 3.19.6.2.3.*

3.19.6.2.1 STX: TLS 1.0 Floor with AES Option

An actor using the STX: TLS 1.0 Floor with AES Option shall support the TLS 1.0 protocol, and shall support at least the following cipher suite:

- TLS_RSA_WITH_AES_128_CBC_SHA

Higher versions of TLS may be used, but the actor shall be able to negotiate TLS 1.0 protocol.

See RFC7525 "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)" for recommendations on proper use of TLS and appropriate fallback rules.

3.19.6.2.2 STX: TLS 1.0 Floor using BCP195 Option

An actor using the STX: TLS 1.0 Floor using BCP195 Option:

- Shall be able to comply with BCP195. This implies that the implementation:
    - Utilizes the framework and negotiation mechanism specified by the Transport Layer Security protocol.
    - Supports TLS version 1.0, version 1.1, version 1.2 or higher.
    - Should support the following cipher suites:
        - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Additional cipher suites may be supported.

- Shall also be able to negotiate down to TLS version 1.1 [RFC4346] or TLS version 1.0 [RFC2246] following the BCP195 version negotiation criteria.

3.19.6.2.3 STX: TLS 1.2 floor using BCP195 Option

An actor using the STX: TLS 1.2 floor using BCP195 Option:

- Shall be able to comply with BCP195. This implies that the implementation:
  - Utilizes the framework and negotiation mechanism specified by the Transport Layer Security protocol.
  - Supports TLS version 1.2 or higher
- Shall also be able to restrict to use TLS version 1.2 [RFC5246] or higher.
- Shall also support the following cipher suites:
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Additional cipher suites of similar or greater cryptographic strength may be supported.