

Internet Draft: TLS support in ITOT
Document: [draft-melnikov-itol-tls-01.txt](#)
Expires: July 2006
Intended category: Standard Track
Updates: RFC [2126](#)

D. Wilson
S. Kille
A. Melnikov
Isode Ltd.
January 2006

TLS support in ITOT

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

A revised version of this draft document will be submitted to the RFC editor as a Proposed Standard for the Internet Community. Discussion and suggestions for improvement are requested, and should be sent directly to the authors. Distribution of this draft is unlimited.

Abstract

This document describes an extension to the ITOT (ISO Transport Service on top of TCP) class 2 service that allows an ITOT Initiator and Responder to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives ITOT agents the ability to protect some or all of their communications from eavesdroppers and attackers.

1. Conventions Used in this Document

INTERNET DRAFT

TLS support in ITOT

January 2006

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[KEYWORDS](#)].

Editorial comments/questions or missing paragraphs are marked in the text with << and >>.

[2.](#) Negotiation of TLS in ITOT

This document extends Connection Establishment procedures defined in the Section 4.2.1 of [[ITOT](#)].

This document redefines bit 2 in the Additional Option parameter ([RFC 2126](#), [Section 6.6](#)), to be used for negotiating TLS. The bit #2 was chosen as this bit is not currently meaningful for the class 2.

Connection Request and Connection Confirmation TPDUs may negotiate use of TLS service. TLS service is selected by setting bit 2 of the "Additional Option" parameter, and is negotiated using the mechanism specified in ISO 8073.

The default is not to use the "TLS Service".

The Initiator requests to commencement of a TLS negotiation by setting the bit 2 in the Additional Option parameter. If the Responder replies with Connection Confirmation TPDU that also has this bit set, this means that the Initiator is able and willing to negotiate TLS.

<<Is this sufficient? What about client which don't know about this spec? We can select a new value for Protocol Version Number field in TPKT? We can also specify that the Responder should set some other field to prove that it actually supports TLS.>>

<<Can the Responder force the Initiator to start TLS negotiation by setting the bit # 2?>>

A [[TLS](#)] negotiation begins immediately after the end of TPKT Packet containing the Connection Confirmation with the Additional Option parameter bit # 2 set.

Note, that at this point the Initiator MUST NOT send further TPKT

Packets until TLS negotiation completes (successfully or not). Similarly, the Responder MUST generate and send replies to all requests received before the TPKT TLS Packet, before proceeding with TLS negotiation.

<<Currently there is no way for the Initiator to select Responder's hostname. Is this needed?>>

If the Responder receives a Connection Request packet containing TLS negotiation request and TLS is already active, it MUST refuse the request by not setting the bit # 2 in the corresponding Connection Confirmation response.

Note, that once TLS negotiation is successful, all further packets will be protected by TLS, even for connections established prior to TLS negotiation. <<An alternative is to force all established connections to be closed.>>

Note, that the Connect Request may contain Connect Data. Such data will be transferred in the clear. If the Initiator is willing to protect the data, it must not use the Connect Data in the Connect Request.

<<Describe how to properly close TLS connection>>

2.1. New NSAPA types for ITOT over TLS

This document extends the definition of "NSAPA for IPv6 address and port", Section 2 of [[NSAP-IPV6](#)].

The IDI value 1 is hereby reserved for ITOT over TLS, when the Initiator would like to perform TLS negotiation, but it is not required.

The IDI value 2 is reserved for ITOT over TLS, when successful TLS negotiation is mandatory. <<TCP connection must be closed if TLS negotiation fails.>>

This document also extends IPv4 NSAPAs: two new prefixes are allocated under the Telex number 00728722 (see also [[RFC1277](#)],

[section 4.5](#)). The prefix 13 is hereby reserved for ITOT over TLS, when the Initiator would like to perform TLS negotiation, but it is not required. The prefix 23 is reserved for ITOT over TLS, when successful TLS negotiation is mandatory.

2.1. Macro for ITOT over TLS NSAPA types

This section adds a couple of macro to the list defined in [\[RFC1278bis\]](#).

Macro	Value
-------	-------

ITOT-TLSOPT-IPv6	IPV6FULL+1+ RFC-1006 ++
ITOT-TLSREQ-IPv6	IPV6FULL+2+ RFC-1006 ++

3. Security Considerations

Initiators and Responders that implement the TLS extension to ITOT as defined in this document MUST implement the TLS_RSA_WITH_RC4_128_MD5 [\[TLS\]](#) cipher suite, and SHOULD implement the TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA [\[TLS\]](#) cipher suite. This is important as it assures that any two compliant implementations can be configured to interoperate. All other cipher suites are OPTIONAL.

During the [\[TLS\]](#) negotiation, the Initiator MUST check its understanding of the Responder's hostname against the Responder's identity as presented in the server Certificate message, in order to prevent man-in-the-middle attacks. If the match fails, the Initiator SHOULD either ask for explicit user confirmation, or terminate the connection and indicate that the Responder's identity is suspect. Matching is performed according to these rules:

The Initiator MUST use the Responder's hostname it used to open the connection as the value to compare against the Responder name as expressed in the Responder (server) certificate. The Initiator MUST NOT use any form of the Responder hostname derived from an insecure remote source (e.g., insecure DNS lookup). CNAME canonicalization is not done.

If a subjectAltName extension of type dNSName is present in the certificate, it SHOULD be used as the source of the Responder's identity.

Matching is case-insensitive.

A "*" wildcard character MAY be used as the left-most name component in the certificate. For example, *.example.com would match a.example.com, foo.example.com, etc. but would not match example.com.

If the certificate contains multiple names (e.g., more than one dNSName field), then a match with any one of the fields is considered acceptable.

Both the Initiator and Responder MUST check the result of the TLS request and subsequent [TLS] negotiation to see whether acceptable authentication or privacy was achieved.

[4.](#) IANA Considerations

IANA is requested to add the following IDIs below the AFI <<TBD - see [draft-melnikov-nsap-ipv6](#)>> in the registry of the OSI NSAPAs:

<<http://www.iana.org/assignments/osi-nsapa-numbers>>:

IDI Value	Description	Format Definition
'1'	ITOT over TLS over IPv6 (optional TLS)	<this document>, section 2.1
'2'	ITOT over TLS over IPv6 (mandatory TLS)	<this document>, section 2.1

[5.](#) Acknowledgments

This document borrows some text from [RFC 2126](#) and [RFC 3501](#).

[6.](#) References

6.1. Normative references

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.

[ITOT] Pouffary, Y. and A. Young, "ISO Transport Service on top of TCP (ITOT)", [RFC 2126](#), March 1997.

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), January 1999.

[RFC1277] Kille, S., "Encoding Network Addresses to support operation over non-OSI lower layers", [RFC 1277](#), November 1991.

[NSAP-IPV6] Wilson, D., Kille, S. and A. Melnikov, "Network Address to support OSI over IPv6", work in progress, [draft-melnikov-nsap-ipv6-XX.txt](#).

[RFC1278bis] Kille, S. and A. Melnikov, "A string encoding of Presentation Address", work in progress, [draft-melnikov-rfc1278bis-XX.txt](#).

6.2. Informative references

<<[IS08348] ISO. "International Standard 8348. Information Processing Systems - Open Systems Interconnection: Network Service

Wilson et al

Expires: July 2006

[Page 5]

INTERNET DRAFT

TLS support in ITOT

January 2006

Definition." [ITU Recommendation X.213]>>

7. Author's Addresses

David Wilson <David.Wilson@isode.com>
Steve Kille <Steve.Kille@isode.com>
Alexey Melnikov <Alexey.Melnikov@isode.com>

Isode Ltd.
5 Castle Business Village,
36 Station Road,
Hampton, Middlesex,
TW12 2BX, United Kingdom

8. Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

9. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any

copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.