

Independent Submission  
Internet-Draft  
Updates: [4642](#) (if approved)  
Intended status: Standards Track  
Expires: June 29, 2017

J. Elie  
December 26, 2016

Use of Transport Layer Security (TLS)  
in the Network News Transfer Protocol (NNTP)  
draft-elie-nntp-tls-recommendations-03

## Abstract

This document provides recommendations for improving the security of the Network News Transfer Protocol (NNTP) when using Transport Layer Security (TLS). It modernizes the NNTP usage of TLS to be consistent with TLS best current practices. If approved, this document updates [RFC 4642](#).

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on June 29, 2017.

## Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

Internet-Draft

Use of TLS in NNTP

December 2016

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">2</a>
<a href="#">1.1.</a>	<a href="#">Conventions Used in This Document</a>	<a href="#">3</a>
<a href="#">1.2.</a>	<a href="#">Author's Note</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Updates/Changes to <a href="#">RFC 4642</a></a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">Recommendations</a>	<a href="#">4</a>
<a href="#">3.1.</a>	<a href="#">Compression</a>	<a href="#">5</a>
<a href="#">3.2.</a>	<a href="#">Protocol Versions and Security Preferences</a>	<a href="#">5</a>
<a href="#">3.3.</a>	<a href="#">Server Name Indication</a>	<a href="#">5</a>
<a href="#">3.4.</a>	<a href="#">Prevention of SSL Stripping</a>	<a href="#">5</a>
<a href="#">3.5.</a>	<a href="#">Authenticated Connections</a>	<a href="#">6</a>
<a href="#">3.6.</a>	<a href="#">Human Factors</a>	<a href="#">6</a>
<a href="#">4.</a>	<a href="#">Security Considerations</a>	<a href="#">7</a>
<a href="#">5.</a>	<a href="#">IANA Considerations</a>	<a href="#">7</a>
<a href="#">6.</a>	<a href="#">References</a>	<a href="#">8</a>
<a href="#">6.1.</a>	<a href="#">Normative References</a>	<a href="#">8</a>
<a href="#">6.2.</a>	<a href="#">Informative References</a>	<a href="#">8</a>
<a href="#">Appendix A.</a>	<a href="#">Detailed Changes to <a href="#">RFC 4642</a></a>	<a href="#">11</a>
<a href="#">A.1.</a>	<a href="#">Related to TLS-level Compression</a>	<a href="#">11</a>
<a href="#">A.2.</a>	<a href="#">Related to Implicit TLS</a>	<a href="#">11</a>
<a href="#">A.3.</a>	<a href="#">Related to RC4 Cipher Suites</a>	<a href="#">12</a>
<a href="#">A.4.</a>	<a href="#">Related to Server Name Indication</a>	<a href="#">12</a>
<a href="#">A.5.</a>	<a href="#">Related to Certificate Verification</a>	<a href="#">12</a>
<a href="#">A.6.</a>	<a href="#">Related to Other Obsolete Wording</a>	<a href="#">13</a>
<a href="#">Appendix B.</a>	<a href="#">Acknowledgments</a>	<a href="#">13</a>
<a href="#">Appendix C.</a>	<a href="#">Document History (to be removed by RFC Editor before publication)</a>	<a href="#">13</a>
<a href="#">C.1.</a>	<a href="#">Changes since -02</a>	<a href="#">13</a>
<a href="#">C.2.</a>	<a href="#">Changes since -01</a>	<a href="#">14</a>
<a href="#">C.3.</a>	<a href="#">Changes since -00</a>	<a href="#">15</a>
	<a href="#">Author's Address</a>	<a href="#">15</a>

## [1.](#) Introduction

The Network News Transfer Protocol (NNTP) [[RFC3977](#)] has been using Transport Layer Security (TLS) [[RFC5246](#)] (along with its precursor, Secure Sockets Layer or SSL) since at least year 2000. The use of TLS in NNTP was formalized in [[RFC4642](#)], providing at the same time implementation recommendations. In order to address the evolving

threat model on the Internet today, this document provides stronger recommendations regarding that use.

In particular, this document updates [\[RFC4642\]](#) by specifying that NNTP implementations and deployments MUST follow the best current

practices documented in the "Recommendations for Secure Use of TLS and DTLS" [\[RFC7525\]](#). This includes stronger recommendations regarding SSL/TLS protocol versions, fallback to lower versions, TLS negotiation, TLS-level compression, TLS session resumption, cipher suites, public key lengths, forward secrecy, hostname validation, certificate verification, and other aspects of using TLS with NNTP.

[[Q1: For RFC Editor: Throughout the document, should [\[RFC7525\]](#) be referenced as [\[BCP195\]](#) or [\[RFC7525\]](#)? Same question for other BCP documents.]]

[[Q2: For RFC Editor: Throughout the document, the references to [\[MUA-STIS\]](#) ([draft-ietf-uta-email-deep](#)) and [\[NNTP-COMPRESS\]](#) ([draft-murchison-nntp-compress](#)) should be referenced as their equivalent [\[RFCxxxx\]](#), once published.]]

### [1.1.](#) Conventions Used in This Document

Any term not defined in this document has the same meaning as it does in [\[RFC4642\]](#) or the NNTP core specification [\[RFC3977\]](#).

When this document uses the terms "implicit TLS", it refers to TLS negotiation immediately upon connection on a separate port.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

### [1.2.](#) Author's Note

Please write the first letter of "Elie" with an acute accent wherever possible -- it is U+00C9 ("[&#201;](#);" in XML). The third letter of "Stephane" and the penultimate letter of "allee" similarly have an acute accent (U+00E9, "[&#233;](#);" in XML). Also, the letters "ae" in "Baeuerle" should be written as an a-umlaut (U+00E4, "[&#228;](#);" in

XML).

## 2. Updates/Changes to [RFC 4642](#)

This document updates [[RFC4642](#)] in the following aspects:

- o NNTP implementations and deployments SHOULD disable TLS-level compression ([Section 3.3 of \[RFC7525\]](#)), thus no longer using TLS as a means to provide data compression (contrary to Abstract and [Section 2.2.2 of \[RFC4642\]](#)).

Elie

Expires June 29, 2017

[Page 3]

---

Internet-Draft

Use of TLS in NNTP

December 2016

- o NNTP implementations and deployments SHOULD prefer implicit TLS and therefore use strict TLS configuration ([Section 3.2 of \[RFC7525\]](#)), that is to say they SHOULD use a port dedicated to NNTP over TLS, and begin the TLS negotiation immediately upon connection (contrary to a dynamic upgrade from unencrypted to TLS-protected traffic via the use of the STARTTLS command, as [Section 1 of \[RFC4642\]](#) was encouraging). For the same reasons, transposed to NNTP, as those given in [Appendix A of \[MUA-ST5\]](#) (whose one of the authors was also one of the authors of [[RFC4642](#)]), implicit TLS is the preferred way of using TLS with NNTP.
- o NNTP implementations and deployments MUST NOT negotiate RC4 cipher suites ([\[RFC7465\]](#)) contrary to [Section 5 of \[RFC4642\]](#) that REQUIRED them to implement the TLS\_RSA\_WITH\_RC4\_128\_MD5 cipher suite so as to ensure that any two NNTP compliant implementations can be configured to interoperate. This document removes that requirement, so that NNTP client and server implementations follow the recommendations given in Sections [4.2](#) and [4.2.1](#) of [[RFC7525](#)] instead. The mandatory-to-implement cipher(s) suite(s) depend on the TLS protocol version. For instance, when TLS 1.2 is used, the TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA cipher suite MUST be implemented ([Section 9 of \[RFC5246\]](#)).
- o NNTP implementations and deployments MUST support the Server Name Indication (SNI) extension defined in [Section 3 of \[RFC6066\]](#), contrary to [Section 2.2.2 of \[RFC4642\]](#) for which it was only a SHOULD. All clients and servers known by multiple names MUST support the SNI extension, in conformance with [Section 3.6 of](#)

[\[RFC7525\]](#).

- o NNTP implementations and deployments MUST follow the rules and guidelines defined in [\[RFC6125\]](#) and [\[RFC5280\]](#) for hostname validation and certificate verification. Part of [Section 5 of \[RFC4642\]](#) is therefore rationalized in favour of following those two documents.

[Appendix A](#) of this document gives detailed changes with regards to the wording of [\[RFC4642\]](#).

### [3.](#) Recommendations

The best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [\[RFC7525\]](#) are included here by reference. Therefore, NNTP implementations and deployments compliant with this document are REQUIRED to also comply with [\[RFC7525\]](#).

Elie

Expires June 29, 2017

[Page 4]

---

Internet-Draft

Use of TLS in NNTP

December 2016

Instead of repeating those recommendations here, this document mostly provides supplementary information regarding secure implementation and deployment of NNTP technologies.

#### [3.1.](#) Compression

NNTP supports the use of the COMPRESS command, defined in Section 2.2 of [\[NNTP-COMPRESS\]](#), to compress data between an NNTP client and server. Although this NNTP extension might have slightly stronger security properties than TLS-level compression [\[RFC3749\]](#) (since NNTP compression can be activated after authentication has completed, thus reducing the chances that authentication credentials can be leaked via for instance a CRIME attack, as described in Section 2.6 of [\[CRIME\]](#)), this document neither encourages nor discourages the use of the NNTP COMPRESS extension.

#### [3.2.](#) Protocol Versions and Security Preferences

NNTP implementations of news servers are encouraged to support options to configure the minimal TLS protocol version to accept, and which cipher suites, signature algorithms or groups (like elliptic curves) to use for incoming connections. Additional options can

naturally also be supported. The goal is to enable administrators of news servers to easily and quickly strengthen security, if need be (for instance by rejecting cipher suites considered unsafe with regards to local policy).

News clients may also support similar options, either configurable by the user or enforced by the news reader.

### [3.3.](#) Server Name Indication

The TLS extension for Server Name Indication (SNI) defined in [Section 3 of \[RFC6066\]](#) MUST be implemented by all news clients. It also MUST be implemented by any news server that is known by multiple names. (Otherwise, it is not possible for a server with several hostnames to present the correct certificate to the client.)

### [3.4.](#) Prevention of SSL Stripping

In order to help prevent SSL Stripping attacks ([Section 2.1 of \[RFC7457\]](#)), NNTP implementations and deployments are encouraged to follow the recommendations provided in [Section 3.2 of \[RFC7525\]](#). Notably, in case implicit TLS is not used, news clients SHOULD attempt to negotiate TLS even if the server does not advertise the STARTTLS capability label in response to the CAPABILITIES command ([Section 2.1 of \[RFC4642\]](#)).

### [3.5.](#) Authenticated Connections

[RFC4642] already provides recommendations and requirements for certificate validation in the context of checking the client or the server's identity. Those requirements are strengthened by [Appendix A.5](#) of this document.

Wherever possible, it is best to prefer certificate-based authentication (along with SASL [\[RFC4422\]](#)), and ensure that:

- o Clients authenticate servers.
- o Servers authenticate clients.
- o Servers authenticate other peer servers.

This document does not mandate certificate-based authentication, although such authentication is strongly preferred. As mentioned in [Section 2.2.2 of \[RFC4642\]](#), the AUTHINFO SASL command ([Section 2.4 of \[RFC4643\]](#)) with the EXTERNAL mechanism (Appendix A of [\[RFC4422\]](#)) MAY be used to authenticate a client once its TLS credentials have been successfully exchanged.

Given the pervasiveness of eavesdropping [\[RFC7258\]](#), even an encrypted but unauthenticated connection might be better than an unencrypted connection (this is similar to the "better-than-nothing security" approach for IPsec [\[RFC5386\]](#)). Encrypted but unauthenticated connections include connections negotiated using anonymous Diffie-Hellman mechanisms or using self-signed certificates, among others.

Note: when an NNTP server receives a Netnews article, it MAY add a <diag-match> ([Section 3.1.5 of \[RFC5536\]](#)), which appears as "!!" in the Path header field of that article, to indicate that it verified the identity of the client or peer server. This document encourages the construction of such Path header fields, as described in [Section 3.2.1 of \[RFC5537\]](#).

### [3.6.](#) Human Factors

It is strongly encouraged that NNTP clients provide ways for end users (and that NNTP servers provide ways for administrators) to complete at least the following tasks:

- o Determine if a given incoming or outgoing connection is encrypted using a security layer (either using TLS or an SASL mechanism that negotiates a security layer).

- o Determine the version of TLS used for encryption of a given stream.
- o If authenticated encryption is used, determine how the connection was authenticated or verified.
- o Inspect the certificate offered by an NNTP server.

- o Determine the cipher suite used to encrypt a connection.
- o Be warned if the certificate changes for a given server.
- o When a security layer is not already in place, be warned if a given server stops advertising the STARTTLS capability label in response to the CAPABILITIES command ([Section 2.1 of \[RFC4642\]](#)) whereas it advertised the STARTTLS capability label during any previous connection within a (possibly configurable) time frame. (Otherwise, a human might not see the warning the first time, and the warning would disappear immediately after that.)
- o Be warned if a failure response to the STARTTLS command is received from the server whereas the STARTTLS capability label was advertised.

Note that the last two tasks cannot occur when implicit TLS is used, and that the penultimate task helps prevent an attack known as SSL Stripping ([Section 2.1 of \[RFC7457\]](#)).

#### [4.](#) Security Considerations

Beyond the security considerations already described in [[RFC4642](#)], [[RFC6125](#)] and [[RFC7525](#)], the author wishes to add the following caveat when not using implicit TLS.

NNTP servers need ensure that they are not vulnerable to the STARTTLS command injection vulnerability ([Section 2.2 of \[RFC7457\]](#)). Though this command MUST NOT be pipelined, an attacker could pipeline it. Therefore, NNTP servers MUST discard any NNTP command received between the use of STARTTLS and the end of TLS negotiation.

#### [5.](#) IANA Considerations

This document does not change the formal definition of the STARTTLS extension ([Section 6 of \[RFC4642\]](#)). Nonetheless, as implementations of the STARTTLS extension should follow this document, IANA will add its reference to the existing STARTTLS label in the NNTP capability labels registry contained in the Network News Transfer Protocol (NNTP) Parameters registry:

Label	Meaning	Reference
STARTTLS	Transport layer security	[RFC4642][RFC-to-be]

## 6. References

### 6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC3977] Feather, C., "Network News Transfer Protocol (NNTP)", [RFC 3977](#), DOI 10.17487/RFC3977, October 2006, <<http://www.rfc-editor.org/info/rfc3977>>.
- [RFC4642] Murchison, K., Vinocur, J., and C. Newman, "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", [RFC 4642](#), DOI 10.17487/RFC4642, October 2006, <<http://www.rfc-editor.org/info/rfc4642>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), DOI 10.17487/RFC5246, August 2008, <<http://www.rfc-editor.org/info/rfc5246>>.
- [RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", [RFC 6066](#), DOI 10.17487/RFC6066, January 2011, <<http://www.rfc-editor.org/info/rfc6066>>.

### 6.2. Informative References

- [CRIME] Rizzo, J. and T. Duong, "The CRIME Attack", Ekoparty Security Conference, 2012.
- [MUA-STTS] Moore, K. and C. Newman, "Mail User Agent Strict Transport Security (MUA-STTS)", July 2016.
- [NNTP-COMPRESS] Murchison, K. and J. Elie, "Network News Transfer Protocol (NNTP) Extension for Compression", October 2016.

- 
- [RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", [RFC 3749](#), DOI 10.17487/RFC3749, May 2004, <<http://www.rfc-editor.org/info/rfc3749>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.
- [RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", [RFC 4422](#), DOI 10.17487/RFC4422, June 2006, <<http://www.rfc-editor.org/info/rfc4422>>.
- [RFC4643] Vinocur, J. and K. Murchison, "Network News Transfer Protocol (NNTP) Extension for Authentication", [RFC 4643](#), DOI 10.17487/RFC4643, October 2006, <<http://www.rfc-editor.org/info/rfc4643>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 5280](#), DOI 10.17487/RFC5280, May 2008, <<http://www.rfc-editor.org/info/rfc5280>>.
- [RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", [RFC 5386](#), DOI 10.17487/RFC5386, November 2008, <<http://www.rfc-editor.org/info/rfc5386>>.
- [RFC5536] Murchison, K., Ed., Lindsey, C., and D. Kohn, "Netnews Article Format", [RFC 5536](#), DOI 10.17487/RFC5536, November 2009, <<http://www.rfc-editor.org/info/rfc5536>>.
- [RFC5537] Allbery, R., Ed. and C. Lindsey, "Netnews Architecture and Protocols", [RFC 5537](#), DOI 10.17487/RFC5537, November 2009, <<http://www.rfc-editor.org/info/rfc5537>>.
- [RFC6125] Saint-Andre, P. and J. Hodges, "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)", [RFC 6125](#), DOI 10.17487/RFC6125, March 2011, <<http://www.rfc-editor.org/info/rfc6125>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), DOI 10.17487/RFC7258, May

2014, <<http://www.rfc-editor.org/info/rfc7258>>.

- [RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", [RFC 7457](#), DOI 10.17487/RFC7457, February 2015, <<http://www.rfc-editor.org/info/rfc7457>>.
- [RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", [RFC 7465](#), DOI 10.17487/RFC7465, February 2015, <<http://www.rfc-editor.org/info/rfc7465>>.
- [RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", [BCP 195](#), [RFC 7525](#), DOI 10.17487/RFC7525, May 2015, <<http://www.rfc-editor.org/info/rfc7525>>.
- [RFC7590] Saint-Andre, P. and T. Alkemade, "Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)", [RFC 7590](#), DOI 10.17487/RFC7590, June 2015, <<http://www.rfc-editor.org/info/rfc7590>>.

## [Appendix A](#). Detailed Changes to [RFC 4642](#)

This section lists detailed changes this document applies to [\[RFC4642\]](#).

### [A.1](#). Related to TLS-level Compression

The second sentence in the Abstract of [\[RFC4642\]](#) is replaced with the following text:

The primary goal is to provide encryption for single-link confidentiality purposes, but data integrity, and (optional) certificate-based peer entity authentication are also possible.

The second sentence of the first paragraph in [Section 2.2.2 of \[RFC4642\]](#) is replaced with the following text:

The STARTTLS command is usually used to initiate session security, although it can also be used for client and/or server certificate authentication.

### [A.2](#). Related to Implicit TLS

The third and fourth paragraphs in [Section 1 of \[RFC4642\]](#) are replaced with the following text:

TCP port 563 is dedicated to NNTP over TLS, and registered in the IANA Service Name and Transport Protocol Port Number Registry for that usage. NNTP implementations using TCP port 563 begin the TLS negotiation immediately upon connection and then continue with the initial steps of an NNTP session. This immediate TLS negotiation on a separate port (referred to in this document as "implicit

TLS") is the preferred way of using TLS with NNTP.

If a host wishes to offer separate servers for transit and reading clients ([Section 3.4.1 of \[RFC3977\]](#)), TCP port 563 SHOULD be used for implicit TLS with the reading server, and an unused port of its choice different than TCP port 433 SHOULD be used for implicit TLS with the transit server. The ports used for implicit TLS should be clearly communicated to the clients, and specifically that no plain-text communication occurs before the TLS session is negotiated.

As some existing implementations negotiate TLS via a dynamic upgrade from unencrypted to TLS-protected traffic during an NNTP session on well-known TCP ports 119 or 433, this specification formalizes the STARTTLS command in use for that purpose. However,

Elie

Expires June 29, 2017

[Page 11]

---

Internet-Draft

Use of TLS in NNTP

December 2016

as already mentioned above, implementations SHOULD use implicit TLS on a separate port.

Note: a common alternative to protect NNTP exchanges with transit servers that do not implement TLS is the use of IPsec with encryption [[RFC4301](#)].

An additional informative reference to [[RFC4301](#)] is therefore added to [Section 7.2 of \[RFC4642\]](#).

#### [A.3.](#) Related to RC4 Cipher Suites

The third paragraph in [Section 5 of \[RFC4642\]](#) is removed. Consequently, NNTP no longer requires to implement any cipher suites, other than those prescribed by TLS ([Section 9 of \[RFC5246\]](#)) and Sections [4.2](#) and [4.2.1](#) of [[RFC7525](#)].

#### [A.4.](#) Related to Server Name Indication

The last two sentences of the seventh paragraph in [Section 2.2.2 of \[RFC4642\]](#) are removed. [Section 3.6 of \[RFC7525\]](#) apply.

#### [A.5.](#) Related to Certificate Verification

The text between "During the TLS negotiation" and "identity

bindings)." in [Section 5 of \[RFC4642\]](#) is replaced with the following text:

During TLS negotiation, the client MUST verify the server's identity in order to prevent man-in-the-middle attacks. The client MUST follow the rules and guidelines defined in [\[RFC6125\]](#), where the reference identifier MUST be the server hostname that the client used to open the connection (or the hostname specified in the TLS "server\_name" extension [\[RFC6066\]](#)). The following NNTP-specific consideration applies: DNS domain names in server certificates MAY contain the wildcard character "\*" as the complete left-most label within the identifier.

If the match fails, the client MUST follow the recommendations in [Section 6.6 of \[RFC6125\]](#) regarding certificate pinning and fallback.

Beyond server identity checking, clients also MUST apply the procedures specified in [\[RFC5280\]](#) for general certificate validation (e.g., certificate integrity, signing, and path validation).

Additional normative references to [\[RFC5280\]](#) (replacing the one it obsoletes), [\[RFC6066\]](#), and [\[RFC6125\]](#) are therefore added to [Section 7.1 of \[RFC4642\]](#).

#### [A.6.](#) Related to Other Obsolete Wording

The first two sentences of the seventh paragraph in [Section 2.2.2 of \[RFC4642\]](#) are removed. There is no special requirement for NNTP with regards to TLS Client Hello messages. [Section 7.4.1.2](#) and [Appendix E of \[RFC5246\]](#) apply.

#### [Appendix B.](#) Acknowledgments

This document draws heavily on ideas in [\[RFC7590\]](#) by Peter Saint-Andre and Thijs Alkemade; a large portion of this text was borrowed from that specification.

The author would like to thank the following individuals for

contributing their ideas and support for writing this specification: Michael Baeuerle, Stephane Bortzmeyer, Viktor Dukhovni, Sabahattin Gucukoglu, Richard Kettlewell, Jouni Korhonen, David Eric Mandelberg, Matija Nalis, Chris Newman, and Peter Saint-Andre.

Many thanks to the Responsible Area Director, Alexey Melnikov, for reviewing and sponsoring this document.

## Appendix C. Document History (to be removed by RFC Editor before publication)

### C.1. Changes since -02

- o Use (and define) the "implicit TLS" terminology instead of "strict TLS". The language in [\[RFC7525\]](#) is unfortunate since "strict TLS" is not clearly defined in that document, and the name suggests that it is an alternative to "opportunistic TLS", rather than an alternative to STARTTLS. While STARTTLS is often used opportunistically, that is not always the case.
- o Mention SSL Stripping in [Section 3.6](#) with a reference to [Section 2.1 of \[RFC7457\]](#) because the intent of the related task may not have been clear enough. Reported by Matija Nalis.
- o Add [Section 3.4](#) about how to prevent SSL stripping, notably by an attempt to negotiate TLS even if STARTTLS is not advertised, when implicit TLS is not used.
- o Strengthen the requirements on hostname validation and certificate verification, by referencing [\[RFC6125\]](#) and [\[RFC5280\]](#).

Elie

Expires June 29, 2017

[Page 13]

---

Internet-Draft

Use of TLS in NNTP

December 2016

- o Ask IANA to add this document to the NNTP capability labels registry.
- o Reference the security considerations of [\[RFC6125\]](#).
- o Mention informative and normative references to add to [\[RFC4642\]](#).

### C.2. Changes since -01

- o Take into account all the remarks sent during IETF Last Call.

- o Move the part about [\[RFC4642\]](#) from Introduction to a new dedicated Section named "Updates/Changes to [RFC 4642](#)" so as to make the document a bit more structured.
- o The warning about lack of STARTTLS is expanded in scope to say "during any previous connection within a (possibly configurable) time frame" instead of "during the previous connection".
- o Remove Appendix about export restrictions on crypto. It is useless since [RFC 2804](#).
- o Add wording about the use of strict TLS for transit. Mention the use of a port other than 433 for strict TLS between two peers, and add a note about a possible use of IPsec [\[RFC4301\]](#) for transit. Do not only speak about port 563.
- o Explicitly mention the mandatory-to-implement cipher suite for TLS 1.2.
- o Do not keep the paragraph about TLS Client Hello messages and Server Name Indication (SNI) in [\[RFC4642\]](#). Support for SNI [\[RFC6066\]](#) is now a MUST, and not a SHOULD.
- o Reference [\[RFC7457\]](#) for the STARTTLS command injection vulnerability.
- o Add notes to RFC Editor to ask that [\[MUA-STX\]](#) and [\[NNTP-COMPRESS\]](#) references be changed to their [\[RFCxxxx\]](#) form, once published, and whether [\[BCP195\]](#) should be used instead of [\[RFC7525\]](#).
- o Move [\[RFC5246\]](#) (TLS) to a normative reference.
- o Minor other wording improvements.

### [C.3](#). Changes since -00

- o Clarify in the introduction of [Section 3](#) that NNTP implementations compliant with this document are REQUIRED to also comply with

[[RFC7525](#)].

- o Improve the wording of [Section 3.2](#) to mention that configuration is primarily intended for news servers. Also, be more consistent in the options to accept, and include signature algorithms and named groups.

#### Author's Address

Julien Elie  
10 allée Clovis  
Noisy-le-Grand 93160  
France

EMail: [julien@trigofacile.com](mailto:julien@trigofacile.com)

URI: <http://www.trigofacile.com/>