Network Working Group M. Garcia-Martin
Internet-Draft Nokia
Expires: November 1, 2004 May 3, 2004

Uniform Resource Identifier (URI) schemes for Authentication, Authorization and Accounting (AAA) protocols
draft-ietf-aaa-uri-01

Status of this Memo

Copyright Notice

Abstract

This memo provides an update for the "aaa" and "aaas" scheme definition originally specified in RFC 3588. The updated scheme is now compatible with the generic URI syntax specified in RFC 2396. This memo also updates the syntax and semantics of the "aaa" and "aaas" URI schemes and provides instructions to IANA to register them in the namespace of registered URI schemes.

Table of Contents

1. Introduction 3
2. Terminology 3
3. The aaa and aaas URI schemes 3
3.1 Syntax 4
3.2 Semantics 4
4. Examples 5
5. IANA Considerations 5
5.1 aaa and aaas URI scheme registration form 5
6. Security Considerations 6
7. Acknowledgements 6
8. References 7
8.1 Normative References 7
8.2 Informative References 7
Author's Address 8
A. Changes in the aaa/aaas URI schemes with respect RFC 3588 . . 8
Intellectual Property and Copyright Statements 9

1. Introduction

RFC 3588 [RFC3588] describes the Diameter base protocol for authentication, authorization and accounting purposes. The RFC provides for the existence of a DiameterURI AVP that contains a "aaa" or "aaas" URI. That definition of the "aaa" and "aaas" URI schemes follows the so-called hierarchical model specified in RFC 2396 [RFC2396], although aaa/aaas resources do not point to hierarchical resources. RFC 3588 [RFC3588] does not provide semantics for the "aaas" URI nor it provide instructions to IANA to register any of those URI schemes in the official IANA registry of URI schemes.

This memo updates the syntax of the "aaa" and "aaas" URI, originally defined in RFC 3588 [RFC3588]. The syntax is made compatible with the generic URI syntax specified in RFC 2396 [RFC2396] at the cost of making an incompatible change with respect RFC 3588. We provide semantics to the "aaas" URI. Additionally, this memo serves for the purpose of the registration of both URI schemes in the Official IANA Registry of URI schemes.

Appendix A provides a summary of the differences between the original definition of the aaa/aaas URI schemes in RFC 3588 and the update specified in this memo.

2. Terminology

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 [RFC2119] and indicate requirement levels for compliant implementations.

3. The aaa and aaas URI schemes

This section defines the syntax of the "aaa" and "aaas" URI schemes using the augmented Backus-Naur Form (BNF) defined in RFC 2234 [RFC2234]. The syntax of the "aaa" and "aaas" URI schemes follows the model of an "absoluteURI" that contains an "opaque_part" (see RFC 2396 [RFC2396] for details of the syntax). We import the definition of "hostport" from RFC 2396 [RFC2396] and their corresponding updates specified in RFC 2732 [RFC2732].

Both the "aaa" and the "aaas" URI schemes are used to identify resources related to authentication, authorization and accounting (AAA) functions that are accessed with AAA protocols such as RADIUS [RFC2865] or Diameter [RFC3588].

The "aaa" URI scheme indicates that transport layer security is not required. The "aaas" URI scheme indicates a requirement for the AAA

protocol to use security provided through TLS.

These URI schemes use the UTF-8 character encoding scheme specified in RFC 3629 [RFC3629].

3.1 Syntax

The "aaa" and "aaas" URI schemes have the following ABNF:

```
aaaURI             = "aaa:" hostport [ transport ]
                                     [ protocol ]
aaasURI            = "aaas:" hostport [ transport ]
                                      [ protocol ]
transport          = ";" "transport=" transport-protocol
transport-protocol = ( "tcp" / "sctp" / "udp" )
protocol           = ";" "protocol=" aaa-protocol
aaa-protocol       = ( "diameter" / "radius" / "tacacs+" )
```

The syntax of "hostport" is defined in RFC 2396 [RFC2396] and updated by RFC 2732 [RFC2732].

3.2 Semantics

According to RFC 2396 [RFC2396] and RFC 2732 [RFC2732] "hostport" is composed of a "host" and a "port" elements. If "host" is specified as a "hostname" (as opposed to an "IPv4address" or an "IPv6address") then it SHOULD contain a Fully Qualified Domain Name. If "port" is empty or not given implementations MUST first determine the AAA protocol associated to the URI by inspecting the "protocol" parameter value or select Diameter if the URI does not include a "protocol" parameter; then implementations MUST assume the default port number of such protocol (e.g., port 3868 for Diameter, 1812 for RADIUS, etc.).

TCP refers to the Transmission Control Protocol specified in RFC 793 [RFC0793]. SCTP refers to the Stream Control Transport Protocol specified in RFC 2960 [RFC2960]. UDP refers to the User Datagram Protocol specified in RFC 768 [RFC0768]. If the transport parameter is empty or not given, then implementations MUST assume that the transport protocol is SCTP.

A "aaas" URI indicates the requirement for using a TLS connection between any two nodes, including possible relays, proxies, etc. An implementation that uses a "aaas" URI scheme to access a AAA resource MUST use TLS over the specified transport protocol, meaning TLS over TCP (specified in RFC 2246 [RFC2246]), TLS over SCTP (specified in RFC 3436 [RFC3436]) or any other usage of TLS over a transport protocol that may be specified in the future.

The use of the "aaas" URI is restricted by the support of TLS provided by the AAA protocol and the transport protocol. For instance, RADIUS only supports UDP as a transport protocol. Since TLS does not support UDP as transport protocol, implementations MUST NOT use "aaas" URIs in conjunction with RADIUS. On the other hand, TACACS does not offer support for TLS, therefore, implementations SHOULD NOT use "aaas" URIs in conjunction with TACACS.

The token "diameter" refers to the Diameter base protocol specified in RFC 3588 [RFC3588]. The token "radius" refers to the RADIUS protocol specified in RADIUS [RFC2865]. The token "tacacs+" refers to the TACACS protocol defined in RFC 1492 [RFC1492]. If the protocol parameter is not given or empty, implementations MUST assume that the AAA protocol is Diameter.

Diameter does not provide support for UDP as a transport protocol, therefore, implementations MUST NOT set the "transport" parameter to "udp" when the "protocol" is set to "diameter" or not specified.

4. Examples

The following are examples of valid "aaa" and "aaas" URIs:

```
aaa:host.example.com;transport=tcp
aaas:host.example.com;transport=tcp;protocol=diameter
aaa:host.example.com;protocol=diameter
aaa:host.example.com:6666;protocol=diameter
aaa:host.example.com:6666;transport=tcp;protocol=diameter
aaa:host.example.com:1813;transport=udp;protocol=radius
```

5. IANA Considerations

This memo instructs IANA the following actions:

- To include "aaa" and "aaas" in the Official IANA Registry of URI Schemes
- To create a new "transport" sub-registry under the registry of AAA parameters, whose values are as per Section 3.1.
- To create a mew "protocol" sub-registry under the registry of AAA parameters, whose values are as defined Section 3.1.

5.1 aaa and aaas URI scheme registration form

URI scheme names: "aaa" and "aaas"

URI scheme syntax: specified in Section 3.1 of RFC XXXX. [Note to the RFC editor: Replace XXXX by the RFC number allocated to this

memo].

Character encoding considerations: The "aaa" and "aaas" URIs support the UTF-8 encoding scheme.

Intended use: common within Authentication, Authorization and Accounting protocols.

Applications and/or protocols which use these URI scheme: Diameter [RFC3588], RADIUS [RFC2865] and TACACS [RFC1492].

Interoperability considerations: none known.

Security considerations: the "aaas" URI scheme indicates a requirement to use TLS between every two nodes to access the AAA resource. However, only Diameter provides support for TLS.

Relevant publications: RFC XXXX [Note to the RFC editor: Replace XXXX by the RFC number allocated to this memo].

Contact information: the IETF AAA Working group. In case the WG does no exist anymore, any person appointed by the IETF Operations and Management Area Director.

Registered-by: Miguel Garcia, miguel.an.garcia@nokia.com

Change control: extensions, new parameters, and new values to these URIs have to be documented in an RFC. The IETF AAA Working Group or, in case the WG does no exist anymore, any person appointed by the IETF Operations and Management Area Director, will provide expert review and advise to the change control process.

6. Security Considerations

This memo does not specify a protocol, but the syntax and semantics of the "aaa" and "aaas" URI schemes. A "aaas" URI scheme indicates a requirement to use TLS over the specified transport protocol to provide security functions. Each AAA protocol (e.g., Diameter), provides additional normative behaviour on the usage of the AAA protocol over TLS. Diameter provides the normative behavior of the TLS usage in Section 13.2 of RFC 3588 [RFC3588]. At the time of writing this memo neither RADIUS nor TACACS provide support for TLS, therefore, there are no semantics associated with a "aaas" URI scheme when the "protocol" parameter is set to "radius" or "tacacs+".

7. Acknowledgements

The author would like to thank Pasi Eronen, John Loughney and Pete

McCann for providing valuable comments.

8. References

8.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC2396] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2732] Hinden, R., Carpenter, B. and L. Masinter, "Format for Literal IPv6 Addresses in URL's", RFC 2732, December 1999.

8.2 Informative References

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC1492] Finseth, C., "An Access Control Protocol, Sometimes Called TACACS", RFC 1492, July 1993.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[RFC3436] Jungmaier, A., Rescorla, E. and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, December 2002.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

Author's Address

Miguel A. Garcia-Martin
Nokia
P.O. Box 407
NOKIA GROUP, FIN 00045
Finland

Phone: +358 50 480 4586
EMail: miguel.an.garcia@nokia.com

Appendix A. Changes in the aaa/aaas URI schemes with respect RFC 3588

- RFC 3588 defined a aaa/aaas URI schemes that follow the hierarchical model defined in RFC 2396 (e.g., including double slashes "//" and slashes "/"). However, aaa/aaas URI schemes are not hierarchical in nature. The slashes have been removed and the URI follows the opaque_part model defined in RFC 2396. This change seems to be incompatible with the definition of the aaa/aaas URI scheme in RFC 3588.
- The "FQDN" definition in RFC 3588 replaced by "host", which is imported from RFC 2396. "host" allows an FQDN or an IP address.
- The "port" parameter defined in RFC 3588 is now embedded into the "hostport" portion of the URI. This does not represent a syntactical change.
- In RFC 3588 the absence of a "port" parameter indicated port 3868 irrespective of the AAA protocol. This memo makes the default port number dependent on the AAA protocol. Therefore, the absence of port in the URI indicates the default port number for the AAA protocol (e.g., port 3868 for Diameter, 1812 for RADIUS).
- Semantics are added so that a "aaas" URI scheme indicates a mandatory requirement to use TLS over the specified transport protocol.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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