Internet Engineering Task Force (IETF)
Request for Comments: 5872
Updates: 5191
Category: Standards Track
ISSN: 2070-1721

J. Arkko
Ericsson
A. Yegin
Samsung

May 2010

IANA Rules for the Protocol for Carrying Authentication for Network Access (PANA)

Abstract

This document relaxes the IANA rules for the Protocol for Carrying Authentication for Network Access (PANA).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5872.

1. Introduction

This document relaxes the IANA rules for the Protocol for Carrying Authentication for Network Access (PANA) [RFC5191]. Rules for the following protocol fields, all defined in [RFC5191], are affected:

- Message Types
- Message Flags
- Attribute-Value Pair (AVP) Flags
- Result-Code AVP Values
- Termination-Cause AVP Values

The rationale for this update is that there can be situations in which it makes sense to grant an allocation under special circumstances. At the time of this writing, the IETF is in the process of approving one such allocation. By changing the current IANA rules to allow for IESG Approval [RFC5226] as well, it has become possible for the Internet Engineering Steering Group (IESG) to consider an allocation request, even if it does not fulfill the default rule. For instance, an experimental protocol extension could perhaps deserve an allocation from a field of reserved bits, as long as a sufficient number of bits still remain for other purposes, and the PANA community is happy with such allocation.

2. IANA Considerations

IANA has updated the registries related to PANA Message Types, Message Flags, AVP Flags, Result-Code AVP Values, and Termination-Cause AVP Values, as specified below. All other PANA IANA registries are to remain unchanged.

2.1. Message Types

The Message Types namespace is used to identify PANA messages. Value 0 is not used and is not assigned by IANA. The range of values from 1 - 65,519 are for permanent, standard Message Types, allocated by IETF Review or IESG Approval [RFC5226]. Previously, the rule for this range was allocation by IETF Review only. [RFC5191] defined the range of values from 1 - 4. The same Message Type is used for both the request and the answer messages, except for type 1. The Request bit distinguishes requests from answers.

The range of values from 65,520 - 65,535 (hexadecimal values 0xfff0 - 0xffff) is reserved for experimental messages. As these codes are only for experimental and testing purposes, no guarantee is made for interoperability between the communicating PANA Client (PaC) and PANA Authentication Agent (PAA) using experimental commands, as outlined in [RFC3692].

2.2. Message Flags

There are 16 bits in the Flags field of the PANA message header. Section 6.2 of [RFC5191] assigned bit 0 ('R'), 1 ('S'), 2 ('C'), 3 ('A'), 4 ('P'), and 5 ('I'). Allocations from the remaining free bits in the PANA header Flag field are made via Standards Action or IESG Approval [RFC5226]. Previously, the rule for these bits was allocation by Standards Action only.

2.3. AVP Flags

There are 16 bits in the AVP Flags field of the AVP header, defined in Section 6.3 of [RFC5191]. That RFC also assigned bit 0 ('V'). The remaining bits are assigned via Standards Action or IESG Approval [RFC5226]. Previously, the rule for these bits was allocation by Standards Action only.

2.4. Result-Code AVP Values

As defined in Section 8.7 of [RFC5191], the Result-Code AVP (AVP Code 7) defines the values from 0 - 2.

All remaining values are available for assignment via IETF Review or IESG Approval [RFC5226]. Previously, the rule for these values was allocation by IETF Review only.

2.5. Termination-Cause AVP Values

As defined in Section 8.9 of [RFC5191], the Termination-Cause AVP (AVP Code 9) defines the values 1, 4, and 8.

All remaining values are available for assignment via IETF Review or IESG Approval [RFC5226]. Previously, the rule for these values was allocation by IETF Review only.

3. Security Considerations

This specification does not change the security properties of PANA.

However, a few words are necessary about the use of the experimental code points defined in Section 2.1. Potentially harmful side effects from the use of the experimental values need to be carefully evaluated before deploying any experiment across networks that the owner of the experiment does not entirely control. Guidance given in [RFC3692] about the use of experimental values needs to be followed.

4. References

4.1. Normative References

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", RFC 5191, May 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

4.2. Informative References

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

Appendix A. Changes from RFC 5191

This document changes the IANA rules for: Message Types, Message Flags, AVP Flags, Result-Code AVP Values, and Termination-Cause AVP Values.

Appendix B. Acknowledgments

The authors would like to thank Yoshihiro Ohba, Ralph Droms, Magnus Westerlund, and Alfred Hoenes for reviews and comments on this topic.

Authors' Addresses

Jari Arkko
Ericsson
Jorvas 02420
Finland

EMail: jari.arkko@piuha.net

Alper Yegin
Samsung
Istanbul
Turkey

EMail: alper.yegin@yegin.org