

Network Working Group  
Internet-Draft  
Updates: [4211](#) (if approved)  
Intended status: Standards Track  
Expires: 26 April 2021

R. Housley  
Vigil Security  
23 October 2020

Algorithm Requirements Update to the Internet X.509 Public Key  
Infrastructure Certificate Request Message Format (CRMF)  
draft-housley-lamps-crmf-update-algs-00

## Abstract

This document updates the cryptographic algorithm requirements for the Password-Based Message Authentication Code in the Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) specified in [RFC 4211](#).

## 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 <https://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 26 April 2021.

## Copyright Notice

Copyright (c) 2020 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 (<https://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 the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

CRMF Algorithm Requirements Update

October 2020

## Table of Contents

|                      |  |                   |
|----------------------|--|-------------------|
| <a href="#">1.</a>   | Introduction . . . . .                               | <a href="#">2</a> |
| <a href="#">2.</a>   | Terminology . . . . .                                | <a href="#">2</a> |
| <a href="#">3.</a>   | Password-Based Message Authentication Code . . . . . | <a href="#">2</a> |
| <a href="#">3.1.</a> | One-Way Function . . . . .                           | <a href="#">2</a> |
| <a href="#">3.2.</a> | MAC Algorithm . . . . .                              | <a href="#">3</a> |
| <a href="#">4.</a>   | IANA Considerations . . . . .                        | <a href="#">3</a> |
| <a href="#">5.</a>   | Security Considerations . . . . .                    | <a href="#">3</a> |
| <a href="#">6.</a>   | Normative References . . . . .                       | <a href="#">3</a> |
|                      | Author's Address . . . . .                           | <a href="#">4</a> |

[1.](#) Introduction

This document updates the cryptographic algorithm requirements for the Password-Based Message Authentication Code (MAC) in the Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) [[RFC4211](#)]. The algorithms specified in [[RFC4211](#)] were appropriate in 2005; however, these algorithms are no longer considered the best choices. This update specifies algorithms that are more appropriate today.

[2.](#) Terminology

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 [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[3.](#) Password-Based Message Authentication Code

[Section 4.4 of \[\[RFC4211\]\(#\)\]](#) specifies a Password-Based MAC that relies on a one-way function to compute a symmetric key from the password and a MAC algorithm. This section specifies algorithm requirements for the one-way function and the MAC algorithm.

[3.1.](#) One-Way Function

Change the paragraph describing the "owf" as follows:

OLD:

owf identifies the algorithm and associated parameters used to compute the key used in the MAC process. All implementations MUST support SHA-1.

NEW:

Housley

Expires 26 April 2021

[Page 2]

---

Internet-Draft

CRMF Algorithm Requirements Update

October 2020

owf identifies the algorithm and associated parameters used to compute the key used in the MAC process. All implementations MUST support SHA-256 [[SHS](#)].

### [3.2.](#) MAC Algorithm

Change the paragraph describing the "mac" as follows:

OLD:

mac identifies the algorithm and associated parameters of the MAC function to be used. All implementations MUST support HMAC-SHA1 [HMAC]. All implementations SHOULD support DES-MAC and Triple-DES-MAC [PKCS11].

NEW:

mac identifies the algorithm and associated parameters of the MAC function to be used. All implementations MUST support HMAC-SHA256 [HMAC]. All implementations SHOULD support AES-CMAC [[CMAC](#)] with a 128 bit key.

## [4.](#) IANA Considerations

This document makes no requests of the IANA.

## [5.](#) Security Considerations

Cryptographic algorithms age; they become weaker with time. As new cryptanalysis techniques are developed and computing capabilities improve, the work required to break a particular cryptographic algorithm will reduce, making an attack on the algorithm more feasible for more attackers. While it is unknown how cryptoanalytic attacks will evolve, it is certain that they will get better. It is unknown how much better they will become or when the advances will happen. For this reason, the algorithm requirements for CRMF are

updated by this specification.

When a Password-Based MAC is used, implementations must protect the password and the MAC key. Compromise of either the password or the MAC key may result in the ability of an attacker to undermine authentication.

## 6. Normative References

- [AES] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", FIPS Publication 197, November 2001.

Housley

Expires 26 April 2021

[Page 3]

---

Internet-Draft

CRMF Algorithm Requirements Update

October 2020

- [CMAC] M., D., "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST Special Publication 800-38B, May 2005.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", [RFC 4211](#), DOI 10.17487/RFC4211, September 2005, <<https://www.rfc-editor.org/info/rfc4211>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [SHS] National Institute of Standards and Technology (NIST), "Secure Hash Standard", FIPS Publication 180-4, August 2015.

## Author's Address

Russ Housley  
Vigil Security, LLC  
516 Dranesville Road  
Herndon, VA, 20170  
United States of America

Email: [housley@vigilsec.com](mailto:housley@vigilsec.com)

Housley

Expires 26 April 2021

[Page 4]