Stream: Internet Engineering Task Force (IETF)
RFC: 9158
Updates: 7299
Category: Informational
Published: November 2021
ISSN: 2070-1721
Author: R. Housley
Vigil Security

RFC 9158
Update to the Object Identifier Registry for the PKIX Working Group

Abstract

RFC 7299 describes the object identifiers that were assigned by the Public Key Infrastructure using X.509 (PKIX) Working Group in an arc that was allocated by IANA (1.3.6.1.5.5.7). A small number of object identifiers that were assigned in RFC 4212 are omitted from RFC 7299, and this document updates RFC 7299 to correct that oversight.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9158.

Copyright Notice

Table of Contents

1. Introduction

When the Public Key Infrastructure using X.509 (PKIX) Working Group was chartered, an object identifier arc was allocated by IANA for use by that working group. After the PKIX Working Group was closed, RFC 7299 [RFC7299] was published to describe the object identifiers that were assigned in that arc. A small number of object identifiers that were assigned in RFC 4212 [RFC4212] are not included in RFC 7299, and this document corrects that oversight.

The PKIX Certificate Management Protocol (CMP) [RFC4210] allocated id-regCtrl-altCertTemplate (1.3.6.1.5.5.7.5.1.7), and then two object identifiers were assigned within that arc [RFC4212], which were intended to be used with either PKIX CMP [RFC4210] or PKIX Certificate Management over CMS (CMC) [RFC5272] [RFC5273] [RFC5274] [RFC6402].

This document describes the object identifiers that were assigned in that arc, establishes an IANA registry for that arc, and establishes IANA allocation policies for any future assignments within that arc.

2. IANA Considerations

IANA has created a new subregistry.

2.1. "SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats" Registry

Within the "Structure of Management Information (SMI) Numbers (MIB Module Registrations)" registry, IANA has created the "SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats" subregistry (1.3.6.1.5.5.7.5.1.7). The initial contents of this subregistry are as follows:

Decimal	Description	References
1	id-acTemplate	[RFC4212]
2	id-openPGPCertTemplateExt	[RFC4212]

Table 1: New SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats Subregistry

Future updates to the registry table are to be made according to the Specification Required policy defined in [RFC8126]. The expert is expected to ensure that any new values are strongly related to the work that was done by the PKIX Working Group. In particular, additional object identifiers should be needed for use with either the PKIX CMP or PKIX CMC to support alternative certificate formats. Object identifiers for other purposes should not be assigned in this arc.

3. Security Considerations

This document populates an IANA registry, and it raises no new security considerations. The protocols that specify these values include the security considerations associated with their usage.

4. References

4.1. Normative References

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, DOI 10.17487/RFC7299, July 2014, <https://www.rfc-editor.org/info/rfc7299>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

4.2. Informative References

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/info/rfc4210>.

[RFC4212] Blinov, M. and C. Adams, "Alternative Certificate Formats for the Public-Key Infrastructure Using X.509 (PKIX) Certificate Management Protocols", RFC 4212, DOI 10.17487/RFC4212, October 2005, <https://www.rfc-editor.org/info/rfc4212>.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, DOI 10.17487/RFC5272, June 2008, <https://www.rfc-editor.org/info/rfc5272>.

[RFC5273] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC): Transport Protocols", RFC 5273, DOI 10.17487/RFC5273, June 2008, <https://www.rfc-editor.org/info/rfc5273>.

[RFC5274] Schaad, J. and M. Myers, "Certificate Management Messages over CMS (CMC): Compliance Requirements", RFC 5274, DOI 10.17487/RFC5274, June 2008, <https://www.rfc-editor.org/info/rfc5274>.

[RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, DOI 10.17487/RFC6402, November 2011, <https://www.rfc-editor.org/info/rfc6402>.

Author's Address

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA 20170
United States of America
Email: housley@vigilsec.com