

Network Working Group  
Internet-Draft  
Updates: [7299](#) (if approved)  
Intended status: Informational  
Expires: 27 January 2022

R. Housley  
Vigil Security  
26 July 2021

Update to the Object Identifier Registry for the PKIX Working Group  
draft-ietf-lamps-rfc7299-update-00

## Abstract

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. [RFC 7299](#) describes the object identifiers that were assigned in that arc. A small number of object identifiers that were assigned in [RFC 4212](#) are not included in [RFC 7299](#), and this document corrects that oversight.

## 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 27 January 2022.

## Copyright Notice

Copyright (c) 2021 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.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	IANA Considerations . . . . .	<a href="#">2</a>
2.1.	"SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats" Registry . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">3</a>
<a href="#">4.</a>	References . . . . .	<a href="#">3</a>
<a href="#">4.1.</a>	Normative References . . . . .	<a href="#">3</a>
<a href="#">4.2.</a>	Informative References . . . . .	<a href="#">3</a>
	Author's Address . . . . .	<a href="#">4</a>

## [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, [\[RFC7299\]](#) 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, established an IANA registry for that arc, and establishes IANA allocation policies for any future assignments within that arc.

## [2.](#) IANA Considerations

IANA is asked to create one additional registry table.

Housley

Expires 27 January 2022

[Page 2]

---

Internet-Draft

CRMF Algorithm Requirements Update

July 2021

### [2.1.](#) "SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats" Registry

Within the SMI-numbers registry, an "SMI Security for PKIX CRMF Registration Controls for Alternate Certificate Formats (1.3.6.1.5.5.7.5.1.7)" table with three columns has been added:

Decimal	Description	References
-----	-----	-----
1	id-acTemplate	<a href="#">[RFC4212]</a>
2	id-openPGPCertTemplateExt	<a href="#">[RFC4212]</a>

Future updates to the registry table are to be made according to the Specification Required policy as 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>>.

Housley

Expires 27 January 2022

[Page 3]

---

Internet-Draft

CRMF Algorithm Requirements Update

July 2021

- [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

Housley

Expires 27 January 2022

[Page 4]