Network Working Group
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

P. Wouters
Aiven
P. Hoffman
ICANN

3 March 2025

Documenting and Referencing Cryptographic Components in IETF Documents
draft-paulwh-crypto-components-04

Abstract

This document describes the history of how cryptographic components have been documented and referenced in the IETF, such as in RFCs, Internet Drafts, and exernal sources. It also gives guidance for how such specification should happen in the future.

%% (To be removed before publication as an RFC) This document is being developed in SAAG. There is a git repo for the document at https://github.com/paulehoffman/draft-paulwh-crypto-components (https://github.com/paulehoffman/draft-paulwh-crypto-components). %%

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 4 September 2025.

Table of Contents

1. Introduction 2
2. Referencing Cryptography in RFCs 3
2.1. External References for Specifying Cryptography 3
2.2. RFCs for Specifying Cryptography 3
3. Using Identifiers for Cryptography in Protocols 4
3.1. Per-Registry Requirements for Adding Code Points 5
3.2. Private-Use Code Points 5
3.3. Vendor Space Code Points 6
3.4. Recommendations in IANA Registries 6
3.5. OIDs 6
3.6. Identifiers and Intellectual Property 7
4. IANA Considerations 7
5. Security Considerations 7
6. References 7
6.1. Normative References 7
6.2. Informative References 7
Authors' Addresses 8

1. Introduction

The IETF has many diverse ways to document and reference cryptographic components that are used in protocols. These practices have changed over time, based on the IETF community, the IETF leadership, and the types of components needed by protocols.

The purpose of this document is to increase consistency and transparency in how the IETF handles cryptographic components. It provides input to IETF working groups that are defining new cryptographic components or updating the way they specify cryptographic components, such as in IANA registries. This document does not define any new policies, but instead describes the many practices that have been used, particularly the practices that are considered best current practices today.

In this document, items such as cryptographic algorithms, base primitives, functions, methods, and constructions are all lumped under the term "cryptographic components". Doing so avoids the conflicting definitions of what differentiates, for example, a method from a construction.

This document is informative, and thus does not prohibit exceptions from the current practices. Given the wide variety of historical practices, the difficulty of differentiating what is a base primitive and what is a cryptographic component, and the variety of needs in IETF working groups, the guidance in this document gives leeway for future specifications.

2. Referencing Cryptography in RFCs

RFCs that define secure protocols need to reference cryptographic components, or those RFCs define the components themselves. It is uncommon for IETF protocols to define cryptographic components; instead, those components are defined elsewhere and referenced in the protocol RFC.

There are many sources for cryptographic references for RFCs.

2.1. External References for Specifying Cryptography

There are many sources of references for cryptography other than RFCs. Such sources include:

* National standards development organizations (SDOs) such as the U.S. National Institute of Standards and Technology (NIST) and the German Federal Office for Information Security (BSI)

* International SDOs such as the International Standards Organization (ISO) and the International Telecommunications Union (ITU)

* Academic papers and articles

* Internet Drafts not meant to proceed to RFC status

* Web sites of individual cryptographers

2.2. RFCs for Specifying Cryptography

In order to be published as an RFC, an Internet Draft must be sponsored by one of the following:

* An IETF working group (and then the working group’s Area Director)

* A research group in the Internet Research Task Force (IRTF)

* An Area Director who is individually sponsoring the draft

* The Independent Submissions Editor (ISE)

* The Internet Architecture Board

RFCs describing cryptographic components have been published by the first four of those. Note, however, that Area Directors may not be willing to individually sponsor drafts for cryptographic components because other venues for RFC publication can garner better reviews, and because RFCs are often not required for specifying cryptographic components (see Section 2.1). Documents from working groups and those sponsored by Area Directors must get IETF consensus (as determined by the IESG) before publication as RFCs; see [RFC8789].

Many RFCs are specifications of cryptographic components, some are specific use cases of cryptography where additional operational constraints apply, and still others simply list cryptographic identifiers such as OIDs or IANA registration values.

An IETF protocol that uses cryptographic components does not need to refer to RFCs for those components; it can refer to external references as described in Section 2.1. Whenever possible, cryptographic components related to a specific protocol should be specified separately from the protocol itself. This allows better review of the cryptography by cryptographers, and better review of the protocol by protocol experts.

3. Using Identifiers for Cryptography in Protocols

IETF working groups often produce RFCs that create registries for cryptographic components. IRTF research groups, particularly the Crypto Forum Research Group (CFRG), also produce RFCs that create registries for cryptographic components. Cryptographic components that originate in the IRTF can appear in IETF protocols.

Although a proliferation of cryptographic components is a barrier to interoperability, the IETF encourages experimenting with new cryptographic components. Identifiers used in IETF protocols are meant to be easy to obtain, as the IETF encourages experimentation and operational testing. These identifiers are often called "code points" when they are listed in IANA registries, but might also be object identifiers (OIDs). OIDs are covered in Section 3.5.

IANA registries are described in depth in [RFC8126]. The following sections cover aspects of using IANA registries for cryptographic protocols; most of these aspects are the same for non-cryptographic protocols as well.

3.1. Per-Registry Requirements for Adding Code Points

In the past, some working groups allowed only a narrow ability to add cryptographic component code points to IANA registries for their protocols, by requiring an RFC. Recently, the rules for many registries have been updated to make it easier to get code points. Registry rules with looser requirement may reduce the likelihood that vendors will just take unallocated codepoints (also known as "squatting") because they can create a stable document for their uses; this also leads to more well-documented experimentation. While the specific registration conditions for "Expert Review" and "Specification Required" are a matter for the WG to specify when creating or updating a registry, overall IETF policies do not require that these specifications be RFCs; they should, however, be stable references.

Stable specifications are important references for developers who rely on a registry with code points. Individual web sites are probably the least-used references for cryptographic components for good reasons: the URLs for them might change or disappear, the content of the web sites might change in ways that would affect the components' definition, and so on.

Although there is no IETF-wide consensus at the time of this writing as to whether an Internet Drafts are appropriate for all registries as stable references, they have been used in the past. Most RFCs do not define whether drafts are acceptable a stable reference, but some do give guidance to designated experts on this topic.

There are some IANA registries where the limited allocation space does not allow for handing out many experimental code points, such as those where the number of code points is limited to 256 or fewer. This necessitates a more conservative approach to code point allocation, and might instead force experiments to use private use code points instead of having allocations for code points that might only be used occasionally.

3.2. Private-Use Code Points

Every IANA registry for cryptographic components should reserve some code points for "private use". These private-use code points can be used by protocol implementers to indicate components that do not have their own code points. Generally, the RFC describing the protocol will define how the private-use code points can be used in practice.

3.3. Vendor Space Code Points

Some IANA registries use an allocation scheme that allows for unlimited code points based on "vendor strings". This allows for wide experimentation in a "vendor space" that acts as a private-use registration. Such registrations might later be converted to an allocation not based on vendor names if the cryptographic component achieves IETF-wide consensus.

3.4. Recommendations in IANA Registries

%% This section needs major work. It needs to incorporate different models for recommendations in registries, such the differences between TLS and DNSSEC algorithm registries. It might have suggestions for models. %%

3.5. OIDs

Some IETF cryptographic protocols (notably CMS, CMP, S/MIME, and PKIX) use OIDs as code points instead of values in IANA registries. A few IANA registries list OIDs, but currently most OIDs are only listed in RFCs. OIDs are a hierarchical numbering system, normally stored in ASN.1 DER or BER encoding, and displayed as a series of positive integers separated by period (".") characters.

In IETF standards, many OIDs for cryptographic components normally are based on a part of the OID tree that was established in the early 1990s. However, many OIDs come from other parts of the OID tree, and no particular part of the OID tree is better or worse than any other for unique identification of cryptographic components. In fact, individuals who want to control part of the OID tree (called "private enterprise numbers") can get their own OID prefix directly from IANA as described in [RFC9371]. The ASN.1 prefix for the IANA PEN tree is 1.3.6.1.4.1.

There is no definitive central source for OID assignments like the IANA registries. This means that OIDs that are assigned in RFCs are only visible to readers of those RFCs, which can cause authors of Internet Drafts to accidentally assign OIDs that are already assigned elsewhere.

Assigning OIDs for cryptographic components in RFCs does not have the flexibility and semantic richness available in IANA registries. Because of this, OIDs are rarely used for cryptographic identifiers in new protocols unless those new protocols are closely aligned with protocols that already use OIDs.

3.6. Identifiers and Intellectual Property

Assigning code points for proprietary cryptographic components or cryptographic components that have known intellectual property rights (IPR) is acceptable as long as any IETF protocol using those code points also allow the protocol to be run without using those components. The IETF policy on IPR can be found in [RFC8179].

4. IANA Considerations

This document contains no actions for IANA. However, it discusses the use of IANA registries in many places.

5. Security Considerations

This document is about the use of cryptography in IETF protocols, and how that cryptography is referenced in those protocols.

Reusing cryptographic components that have already been reviewed and approved in the IETF is usually better than creating new cryptography that must be reviewed before it is used in protocols.

6. References

6.1. Normative References

[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>.

6.2. Informative References

[RFC8179] Bradner, S. and J. Contreras, "Intellectual Property Rights in IETF Technology", BCP 79, RFC 8179, DOI 10.17487/RFC8179, May 2017, <https://www.rfc-editor.org/info/rfc8179>.

[RFC8789] Halpern, J., Ed. and E. Rescorla, Ed., "IETF Stream Documents Require IETF Rough Consensus", BCP 9, RFC 8789, DOI 10.17487/RFC8789, June 2020, <https://www.rfc-editor.org/info/rfc8789>.

[RFC9371] Baber, A. and P. Hoffman, "Registration Procedures for Private Enterprise Numbers (PENs)", RFC 9371, DOI 10.17487/RFC9371, March 2023, <https://www.rfc-editor.org/info/rfc9371>.

Authors' Addresses

Paul Wouters
Aiven
Email: paul.wouters@aiven.io

Paul Hoffman
ICANN
Email: paul.hoffman@icann.org