ACVP IANA Registry

Apostol Vassilev
Information Technology Laboratory
Computer Security Division

June 05, 2019

National Institute of
Standards and Technology
U.S. Department of Commerce

Abstract

This document defines a set of IANA registries for supported cryptographic algorithm test specifications in the Automated Cryptographic Validation Protocol (ACVP) [ACVP]. This document also shows how to extend the capabilities of ACVP with testing for new cryptographic algorithms.

Keywords

The following are keywords to be used by search engines and document catalogues.

ACVP; cryptography

Acknowledgements

Many thanks to David Waltermire for his helpful comments to get us started on the right path.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

Feedback

Feedback on this publication is welcome, and can be sent to: code-signing@nist.gov.

1. Introduction

The Automated Cryptographic Validation Protocol (ACVP) [ACVP] defines a mechanism to automatically validate the cryptographic algorithm implementations of software or hardware cryptographic modules. The ACVP specification defines how a cryptographic module communicates with a validation authority server, including cryptographic capabilities negotiation, session management, authentication, test vector processing and more. The ACVP specification does not define algorithm-specific JSON constructs for performing the cryptographic validation. A series of ACVP-related sub-specifications define the constructs for testing individual cryptographic algorithms, see for example [ACVP-Symmetric]. Each such sub-specification addresses a specific algorithm or a class of cryptographic algorithms. This document defines the IANA registry for the supported algorithm test specifications that work with ACVP. The registry defined here provides the binding between the protocol and the supported algorithm test extensions.

2. IANA namespaces

There are three namespaces envisioned for extensions to the ACVP:

- ACVP — the approved algorithms for testing with one or more validation authorities
- EXPERIMENTAL — candidate algorithms for approval.
- LOCAL — locally supported algorithms, not guaranteed for interoperability. Algorithms in this namespace cannot be registered with IANA.

TBD

3. Algorithm Registry

Each entry in the algorithm registry must record the following fields:

- Name: a URN segment that conforms to the pattern {namespace}-{algorithm}. The keywords are defined as follows:
  - {namespace}: one of the options from Section 2.
  - {algorithm}: a required US-ASCII string that conforms to the URN syntax requirements (see [RFC 8141]). This string must be unique within the corresponding namespace.
- Revision: the revision identifier for the test specification of a particular algorithm. A required US-ASCII string that conforms to the URN syntax requirements (see [RFC 8141]).
- Reference: A static link to the specification and section where the definition of the parameter can be found.

3.1. Initial Algorithm Registry Names

Table 1

Name	Revision	Reference
“ACVP-AES-ECB”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CBC”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-OFB”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CFB1”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CFB8”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CFB128”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CTR”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-GCM”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CCM”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-XPN”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-CMAC”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-GMAC”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-KW”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-KWP”	“1.0”	[ACVP-Symmetric]
“ACVP-AES-XTS”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-ECB”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-CBC”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-OFB”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-CFB1”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-CFB8”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-CFB64”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-CTR”	“1.0”	[ACVP-Symmetric]
“ACVP-TDES-KW”	“1.0”	[ACVP-Symmetric]

4. Requirements Language

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted in [RFC 2119].

5. IANA Considerations

This memo includes several requests to IANA.

5.1. ACVP URN Sub-namespace

IANA should add an entry to the "IETF URN Sub-namespace for Registered Protocol Parameter Identifiers" registry located at https://www.iana.org/assignments/params/ as per [RFC 3553].

The entry should be as follows:

- Registered Parameter Identifier: ACVP
- Specification: this document
- Repository: ACVP URN Parameters (see Section 5.2)

5.2. ACVP URN Parameters

A new top-level registry should be created, titled "Automated Cryptographic Validation Protocol (ACVP) URN Parameters". Registration in the "ACVP URN Parameters" registry is via the Specification Required policy [RFC 8126]. Registration requests must be sent to both the ACVP Working Group mailing list (acvp@ietf.org) and IANA. IANA will forward registration requests to the Designated Expert.

Each entry in this subregistry must record the following fields:

- Name: A required US-ASCII string that conforms to the URN syntax requirements (see [RFC 8141]). This string MUST be constructed according to the specification in Section 3. Note: entries from the namespace "LOCAL" SHALL be forbidden from this table.
- Revision: A required US-ASCII string that conforms to the URN syntax requirements (see [RFC 8141]). The combination {Name}-1 for each entry MUST be unique for the entire subregistry.
- Reference: A static link to the specification and section where the definition of the parameter can be found.

This repository SHALL have as initial values the entries in Section 3.1.

6. Security Considerations

Security considerations are addressed by the ACVP specification.

Appendix A — References

S. Bradner (March 1997) *Key words for use in RFCs to Indicate Requirement Levels* (Internet Engineering Task Force), BCP 14, March 1997. RFC 2119. RFC RFC2119. DOI 10.17487/RFC2119. https://www.rfc-editor.org/info/rfc2119.

M. Mealling, L. Masinter, T. Hardie, G. Klyne (June 2003) *An IETF URN Sub-namespace for Registered Protocol Parameters* (Internet Engineering Task Force), BCP 73, June 2003. RFC 3553. RFC RFC3553. DOI 10.17487/RFC3553. https://www.rfc-editor.org/info/rfc3553.

M. Cotton, B. Leiba, T. Narten (June 2017) *Guidelines for Writing an IANA Considerations Section in RFCs* (Internet Engineering Task Force), BCP 26, June 2017. RFC 8126. RFC RFC8126. DOI 10.17487/RFC8126. https://www.rfc-editor.org/info/rfc8126.

P. Saint-Andre, J. Klensin (April 2017) *Uniform Resource Names (URNs)* (Internet Engineering Task Force), RFC 8141, April 2017. RFC 8141. RFC RFC8141. DOI 10.17487/RFC8141. https://www.rfc-editor.org/info/rfc8141.

Fussell B, Vassilev A, Booth H, Celi C, Hammett R (July 01, 2019) *Automatic Cryptographic Validation Protocol* (National Institute of Standards and Technology, Gaithersburg, MD), July 01, 2019.

Celi C, Hammett R (December 10, 2020) *ACVP Symmetric Algorithm JSON Specification* (National Institute of Standards and Technology, Gaithersburg, MD), December 10, 2020.