#

Use of Cryptography

Table of contents

1. Objective
2. Use of Cryptography Requirement
3. Recommended NIST Standards
4. OpenSSL Support for FIPS-140-2
5. Guidelines for CIP Users
6. CIP Review frequency

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2022-03-29	Draft use of cryptography details for CIP	Dinesh K	To be reviewed and discuss with SWG

---

1. Objective

The primary objective of this document is to explain about the IEC-62443-4-2 CR-4.3 requirement.

Explain about recommended NIST standards to strengthen product security.

2. Use of Cryptography Requirement CR-4.3

This requirement has following expectations to meet by end product.

- Cryptography mechanisms should be used following internationally recognized standard
- Data in all forms, at rest, in transit or both should be protected
- Key management practices should be documented
- Only use established and tested hash and encryption algorithms
- Follow the best practices provided by NIST SP 800-57 part-1 to 3

3. Recommended NIST Standards

Following NIST standards are recommended to be followed by products owner.

NIST SP 800-57 Part-1

NIST SP 800-57 Part-2

NIST SP 800-57 Part-3

These NIST standards are updated periodically, hence CIP users are advised to review them periodically. Incorporate important security recommendations in the product.

4. OpenSSL Support for FIPS-140-2

Current CIP (bullseye based) uses OpenSSL 1.1.1. OpenSSL 1.1.1 has FIPS-140-2 recommended crypto algorithms supported for hashing, signing and encryption.

OpenSSL 3.0 have FIPS-140-2 compliant support. However, OpenSSL 3.0 is not supported by CIP.

Based on CIP end products security and compliance requirements, CIP users should select appropriate OpenSSL version or other crypto libraries.

5. Guidelines for CIP Users

CIP users are recommended to use FIPS-140-2 approved algorithms for all crypto operations. As now the successor of FIPS-140-2 is FIPS-140-3 which will be effective from 2022 onward. Hence CIP users should inquire the effective FIPS standard and follow the crypto algorithms.

In addition, guidelines related to following key topics should be followed using NIST standards listed in this document.

- Key usage
- Crypto periods
- Key compromise plan
- Key distribution methodologies
- Key-Size Selection
- Key-Management Functions
- Cryptographic Key Management Systems (CKMS)
- Key management planning
- Key Management Planning Process

6. CIP Review frequency

As NIST standards are revised periodically, CIP developers would set a review frequency of once in a year.

Based on the new recommendations CIP users would be advised accordingly and this document would remain subject to revision.