#

CIP Private Key Management

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-08-17	Draft private key management document in CIP	Dinesh Kumar	To be reviewed by CIP Security WG members

---

---

1. Objective

The primary objective of this document is to explain about how various private keys used in CIP development are maintained and kept secure and confidential.

Moreover, subsequent revisions of this document may consider to add details of keys which are added or used in future.

2. Assumptions

Assumption	Impact
All private keys used in CIP are only for reference and CIP users need to re-generate these keys again and use in the end product	Re-using CIP keys will make the end product vulnerable

3. Scope

Scope of this document is to meet IEC-62443-4-1 SM-8 (Control of Private Keys) security requirement. This document will explain about various private keys used during CIP development, including generation, usage, storage, password change, key rotation and protection of these keys.

4. Security Requirement

CIP shall place procedural and technical control to protect all private keys used in CIP development or needed at run time.

Since private keys are root of trust, they require extra protection so that they are not stolen or compromised.

5. General Private Key Management Steps

Following diagram illustrates steps fo private key management.

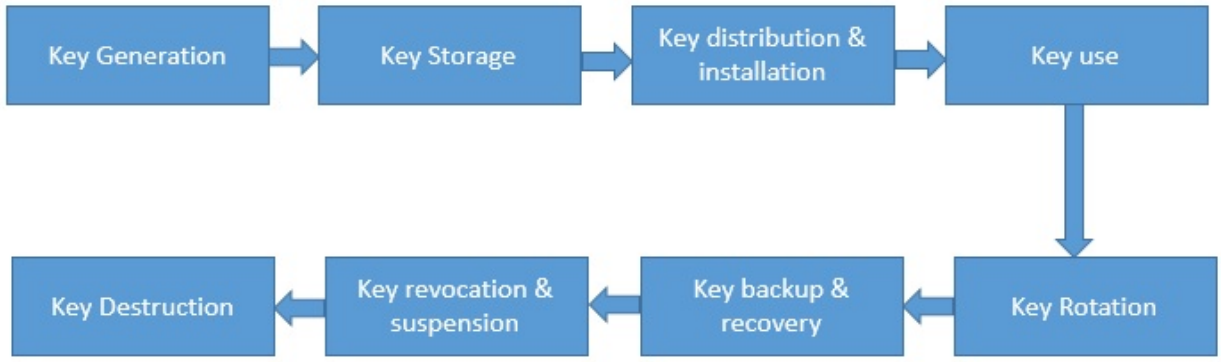

Figure 1: Private Key Management Life Cycle

6. About CIP Private Keys

Currently CIP does not use any private keys which is expected to be used by CIP based end products.

In future if any private key is used which would be used by CIP based end products, it will added here.

7. Private Key Management Best Practices

CIP Security work group members did investigation to find best practices for private key management which are recommnded to be followed by CIP users.

Following best practices have been taken from [1], [2], [3].

1. According to NIST, in general, a single key should be used for only one purpose (e.g., encryption, authentication, key wrapping, random number generation, or digital signatures
2. Limiting the use of a key limits the damage that could be done if the key is compromised.
3. Keys should never be stored in plaintext format.
4. Ensure all keys are stored in cryptographic vault, such as a hardware security module (HSM) or isolated cryptographic service.

5. If you are planning on storing keys in offline devices/databases, then encrypt the keys using Key Encryption Keys (KEKs) prior to the export of the key material.
6. Ensure that keys and cryptographic operation is done inside the sealed vault
7. Centralize Your Encryption Key Management Systems
8. Centralize User Roles & Access
9. Support Multiple Encryption Standards
10. Implement Robust Logging & Auditing
11. Implement the Principle of Least Privilege
12. Back Up Your Encryption Keys
13. Protection of the Key Manager & Recovery of Deleted Keys
14. Rotate Your Keys: No Decryption/Re-Encryption
15. Keep backup plan in case of key compromise/stolen

8. References

1. https://www.thesslstore.com/blog/12-enterprise-encryption-key-management-best-practices/
2. https://www.snia.org/sites/default/education/tutorials/2008/fall/security/WaltHubis-Best_Practices_Secure_Sto
3. https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html