#

CIP Private Key Management

Table of contents

1. Objective
2. Assumptions
3. Scope
4. Roles
5. RACI

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-08-26	Draft RACI document in CIP	Yasin Demirci	To be reviewed by CIP Security WG members
002	2022-01-06	Changed to better reflect SM-2	Yasin User	To be reviewed by CIP Security WG members

---

---

1. Objective

The primary objective of this document is to show the roles in CIP with their responsibilities and accountabilities. It is also shown which roles should be consulted and/or informed for certain actions and which qualifications, if any, are needed to fulfill a role.

2. Scope

Scope of this document is to meet IEC-62443-4-1 SM-2 (Identification of Responsibilities) security requirement.

4. Roles

Abbreviation	Name	Description	Qualifications
SWG	Security Working Group	The SWG handles all IT security topics for CIP. This includes consulting other working groups and adding additional security features. All decisions are made via the security mailing list or meetings of the SWG.	>50% of the SWG members need to have at least 3 years of experience in IT security or proof their expertise via certifications.

Abbreviation	Name	Description	Qualifications
MNT	CIP Maintainer	CIP maintainers are usually members of the Kernel or Core working groups.	All CIP maintainers have to show evidence for at least 3 days of secure coding training.
TSC	Technical Steering Committee	The technical steering committee consists representatives of the member companies. They vote on changes suggested by the working groups.	TSC members do not need security qualifications as they are consulted by the security working group.
TST	CIP Tester	CIP maintainers are usually members of the Kernel, Core or Testing working groups.	All CIP testers have to show evidence for at least 3 days of secure coding training or a similar training for secure testing.

5. RACI

	SWG	MNT	TSC	TST
Update Secure Coding Standard	a r	c	i	i
Provide File Integrity	a r	i	i	-
Controls for Private Keys	a	r	i	r
Product Security Context	a r	-	i	-
Threat Model	a r	-	i	-
Product Security Requirements	a r	c	i	-
Product Security Requirements Content	a r	-	i	-
Security Requirements Review	a r	-	i	-
Secure Coding Standards	a r	c	i	-
Security Update Qualification	a c	r	i	r
Security Update Documentation	a c	r	i	-

Legend: - a = accountable - r = responsible - c = consulted - i = informed - - = not applicable

Note: Ultimately, The CIP governing board and the Linux Foundation are accountable for the whole CIP project. The RACI matrix above instead shows who is responsible and accountable from an everyday business perspective.