

Requirement ID	Name	Category	Priority	Status	By	Why	CIP recommendation
CR-1.1	Human identification and authentication	Human	High	Implemented	IEC-62443-4-2	tests reference	The CIP platform complies with this requirement. Users can login through various interfaces (e.g. serial console, http etc). CIP based products may use variety of interfaces, this requirement mandates on each interface user or process or device should be uniquely identified and authenticated.
CR-1.1-RE1	Unique identification and authentication	Unique	High	Implemented	IEC-62443-4-2	tests reference	Same as CR-1.1

ReqID	Requirement name	Support	Need	Status	HW	By	CIP recommendation
CR-1.1	Multi-factor authentication for all interfaces	TRUE	FALSE	None	Adding	IEC-62443-4-2 tests reference	The CIP platform complies with this requirement by adding google MFA Debian package. However, CIP users can use their own way to achieve this MFA.
CR-1.2	Software and device identification and authentication	FALSE	FALSE	None			The CIP platform can't meet this requirement, CIP users should use their applications to meet this requirement. All components need to identify themselves. We recommend the usage of TPM generated id or certificates for device id, a process pid and the addition of the active user account. The pid must be logged in the processes lifetime as it changes after a process restart.

Req ID	Requirement name	Support	Need	Status	HW	By	CIP recommendation
CR1.2	Unique authentication and authentication	FALSE	FALSE	None		IEC-62443-4-2 tests reference	APP: All certificates/authentication ids for 1.2 need to be unique.
CR1.3	Account management	FALSE	FALSE	Implemented	As of	https://gitlab.com/cip-user-project/cip-testing/cip-security-mod-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_12 https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_23 https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_3	Default Action
CR1.4	Identification management	FALSE	FALSE	Implemented	As of	https://gitlab.com/cip-pack-project/cip-testing/cip-security-age-tests/-/tree/master/iec-security-add-tests/singlenode-testcases/TC_CR1.4_1	Default Action

Req ID	Requirement name	Priority	Support	Need	Status	HW	By	CIP recommendation
CR1.5-authentication-tactors on which the company rely shall be protected via hardware mechanism	Authentication-tactors on which the company rely shall be protected via hardware mechanism	High	True	True	Open	None	IEC-62443-4-2 tests reference	Default Action
CR1.5-authentication-tactors on which the company rely shall be protected via hardware mechanism	Authentication-tactors on which the company rely shall be protected via hardware mechanism	High	True	True	Open	None	IEC-62443-4-2 tests reference	This requirement expects a secure storage, CIP added TPM tools. However, secure storage and any other tools needed should be met by CIP users based on their requirements.

Req ID	Requirement name	Supported	Need	Status	HW	By	IEC-62443-4-2 tests reference	CIP recommendation
ND1.6	Wireless access management	TRUE	FALSE	None	progress	Wireless drivers to be included in CIP kernel		Default Action
ND1.6	Unique identification and authentication	TRUE	FALSE	None	progress	Wireless drivers to be included in CIP kernel		Default Action
CR1.7	Strengthening of password-based authentication	TRUE	FALSE	None	Completed	https://github.com/cip-pack-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7_1		Default Action
CR1.7	Password restriction for human users	TRUE	FALSE	None	Completed	https://github.com/cip-pack-project/cip-testing/cip-security-ages-tests/-/tree/master/iec-security-tests/singlenode-login-testcases/TC_CR1.7-RE1_1		Default Action

Req ID	Requirement name	Support	Need	Status	HW by	Tests reference	CIP recommendation
CR-1.7	Password 1.7 life-cycle restrictions for all users (human, software process, or device)	FALSE	FALSE	None			This is for SL-4
CR-1.8	Public key infrastructure (PKI) certificates	TRUE	FALSE	None		https://github.com/cip-pack-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.8_1	Default Action

Req ID	Requirement name	Support	Need	Status	Why	CIP recommendation
CR1.9	Strength of public key-based authentication - check validity of signature of a given certificate	CR1.9	CR1.9	Not supported	IEC-62443-4-2 tests reference	Default Action
					https://gitlab.com/cip-pack-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_12 . https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_23 . https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_34 . https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_45 . https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_56 . https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_6	

Requirement ID	Requirement Name	Support	Need	Status	By	CIP recommendation
CR-1.9	Hardware support for public key-based authentication	True	False	Not Implemented	IEC-62443-4-2 tests	It requires HW support, should be met by CIP users
CR-1.10	Authentication feedback	True	False	Implemented	https://gitlab.com/cip-pack-project/cip-testing/cip-security-age-tests/-/tree/master/iec-security-opensds/singlenode-testcases/TC_CR2.10_1	Default Action
CR-1.11	Unsuccessful login attempts - limit number	True	False	Implemented	https://gitlab.com/cip-pack-project/cip-testing/cip-security-age-tests/singlenode-libpan-testcases/TC_CR1.11_1 https://gitlab.com/cip-pack-project/cip-testing/cip-security-bin-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.11_2	Default Action

Req ID	Requirement name	System	Support	Need	Status	By HW	IEC-62443-4-2 tests reference	CIP recommendation
1.12	use notification	FALSE	FALSE	None				CIP does not support this requirement, CIP users should implement notifications based on their requirements. Following are some guidelines APP: If the device has a HMI for an application requiring authentication, the application shall be able to display a configurable use notification message before the credentials are requested from the user.

Req ID	Requirement name	Support	Need	Status	HW	By	CIP recommendation
NDR1.13	Access via untrusted networks	FALSE	FALSE	A	None	IEC-62443-4-2 tests reference	CIP does not support this requirement. Access of networks should be monitored using network security software and tools, only used ports should be open and unused ports should be blocked to avoid unauthorized access.
NDR1.13a	Access request approval	FALSE	FALSE	A	None		CIP does not support this requirement. Application based security policies, explicit request should be raised to access blocked URLs or ports to monitor them closely. Requests need to be approved by an assigned role. This can be done by a human or machine user.

Req ID	Requirement name	Need	Status	HW by	CIP recommendation
CR1.14	Strength of symmetric key-based authentication	Security for symmetric key-based authentication	Not supported	IEC-62443-4-2 tests reference	Default Action
CR1.14e	Hardware security for symmetric key-based authentication	Security for symmetric key-based authentication	Not supported	None	Requires HW support