

Req ID	Requirement name	Supported by CIP	Need satisfied	Status	HW by	Reference	CIP recommendation
CR-1.1	Human identification and authentication	TRUE	FALSE	Completed	Adding	<a href="https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-passwd-testcases/TC_CR1.1_2">https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-passwd-testcases/TC_CR1.1_2</a>	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	Unique identification and authentication	TRUE	FALSE	Completed	Adding	<a href="https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-libpart-testcases/TC_CR1.1-RE1_1">https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-libpart-testcases/TC_CR1.1-RE1_1</a>	Same as CR-1.1
CR-1.1	Multi-factor authentication for all interfaces	TRUE	FALSE	Completed	Adding	pack-age libpam-google-authenticator	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.

ReqID	Requirement name	Supported by CIP	Need reported	Status if supported	By HW	IEC-62443-4-2 tests reference	CIP recommendation
CR-1.2	Software process and device identification and authentication	FALSE	TRUE	FALSE	EA	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. APP: All certificates/authentication ids for 1.2 need to be unique.
CR-1.3	Unique identification and authentication management	TRUE	FALSE	FALSE	EA	None	Default Action
CR-1.4	Identification management	TRUE	FALSE	FALSE	EA	None	Default Action

Req ID	Requirement name	Support	Need	Status	HW	By	CIP recommendation
CR-Authenticator content	1.5 authentication-initialize	TRUE	FALSE	Completed	None	As of	Default Action
CR-Authenticators on which the company rely shall be protected via hardware mechanism	1.5-authenticators on which the company rely shall be protected via hardware mechanism	TRUE	FALSE	Completed	None	As of	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.
ND-1.6 access management	1.6 wireless access management	TRUE	FALSE	None	progress	Wireless drivers to be included in CIP kernel	Default Action

ReqID	Requirement name	Supported by CIP	Need ap-plied	Status if supported	HW by IEC-62443-4-2 tests reference	CIP recommendation
NDR-1.6	Unique identification and authentication	TRUE	FALSE	SE	None progressWireless drivers to be in- cluded in CIP kernel	Default Action
CR-1.7	Strength of password-based authentication	TRUE	FALSE	SE	<a href="https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7_1">https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7_1</a>	Default Action
CR-1.7	Password generation and lifetime restrictions for human users	TRUE	FALSE	SE	<a href="https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7-RE1_1">https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7-RE1_1</a>	Default Action
CR-1.7	Password lifetime restrictions for all users (human, software process, or device)	FALSE	FALSE	SE	None	This is for SL-4

Req ID	Requirement name	Support by CIP	Need fulfilled	Status if supported	HW by IEC-62443-4-2 tests reference	CIP recommendation
CR-1.8	Public key infrastructure (PKI) certificates	TRUE	FALSE	Completed	<a href="https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR1.8_1">https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR1.8_1</a>	Default Action
CR-1.9	Strength of public key-based authentication - check validity of signature of a given certificate	TRUE	FALSE	Completed	<a href="https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR1.9_12">https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR1.9_12.</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_23">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_23.</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_34">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_34.</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_45">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_45.</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_56">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_56.</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_6">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-testcases/TC_CR1.9_6</a>	Default Action
CR-1.9	Hardware security (H) for public key-based authentication	TRUE	FALSE	Required		It requires HW support, should be met by CIP users
CR-1.10	Authentication feedback	TRUE	FALSE	Completed	<a href="https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR2.10_1">https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iecs-security-tests/singlenode-opensstestcases/TC_CR2.10_1</a>	Default Action

Req ID	Requirement name	Support by CIP	Need by HW	Status if supported	Reference	CIP recommendation
CR-1.11	Successful login attempts limit number	FALSE	FALSE	Implemented	<a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-pack-security-tests/singlenode-age_testcases/TC_CR1.11_1">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-pack-security-tests/singlenode-age_testcases/TC_CR1.11_1</a> <a href="https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-bin_testcases/TC_CR1.11_2">https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-bin_testcases/TC_CR1.11_2</a>	<b>Default Action</b>
CR-1.12	System use notification	FALSE	FALSE	SEA	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.
ND-1.13	Access via untrusted networks	FALSE	FALSE	SEA	None	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.

ReqID	Requirement name	Support	Need	Status	HW	By	IEC-62443-4-2 tests reference	CIP recommendation
ND-1.13	Explicit access request approval	FALSE	FALSE	EA	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.
CR-1.14	Symmetric key-based authentication	TRUE	FALSE	EA	None		<a href="https://github.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.8_1">https://github.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.8_1</a>	Default Action
CR-1.14	Hardware security for symmetric key-based authentication	TRUE	FALSE	EA	None			Requires HW support