

Req ID	Requirement name	Need	Status	ap- pli- ca- tion	if sup- ported	by HW	Why	CIP recommendation
Req ID	Requirement name	Need	Status	ap- pli- ca- tion	if sup- ported	by HW	Why	CIP recommendation
CR-1.1	Human user identification and authentication	TRUE	FALSE	Completed	Added	gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-passwordtestcases/TC_CR1.1_12. login https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.1_2		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	Added	gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-libpartestcases/TC_CR1.1-RE1_1 cracklib		Same as CR-1.1
CR-1.1	Multi-factor authentication for all interfaces	TRUE	FALSE	Completed	Added	gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-libpartestcases/TC_CR1.1-RE1_1 cracklib		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.

Req ID	Requirement name	CIP support	Need application support	Status if supported	Why not IEC-62443-4-2 tests reference	CIP recommendation
CR-Software 1.2	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 requirementAll 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-Unique ID 1.1	Identification and authentication	FALSE	TRUE	FALSE	EA. None	
CR-Account 1.3	management	TRUE	FALSE	FALSE	Completed https://gitlab.com/cip-project/cip-user-testing/cip-security-tests/-/tree/master/iec-mod-security-tests/singlenode-packages/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
CR-Identification 1.4	management	TRUE	FALSE	FALSE	Completed https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-age-security-tests/singlenode-addustestcases/TC_CR1.4_1	Default Action

Req ID	Requirement name	Need ap- pli- Support	Status if sup- ported	by HW	Why	CIP recommendation
Req ID	Requirement name	CIP support	Policy	On IEC-62443-4-2 tests	reference	
CR-1.5	Authentication management - initialize authentication content	TRUE	FALSE	Completed	https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-tpm2testcases/TC_CR1.5_22. tools,https://gitlab.com/cip-project/cip-tpm2testing/cip-security-tests/-/tree/master/iec-abrmdecurity-tests/singlenode-testcases/TC_CR1.5_3	Default Action
CR-1.5	Authentication on which the company rely shall be protected via hardware mechanism	TRUE	FALSE	Completed		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	Wireless access management	TRUE	FALSE	None	progressWireless drivers to be included in CIP kernel	Default Action

Req ID	Requirement name	Need by CIP	ap- plic- ation	Status if supported	HW by IEC-62443-4-2 tests	reference	CIP recommendation
ND-1.6	Unique identification and authentication	TRUE	FALSE	SE	None		Default Action
CR-1.7	Strength of password-based authentication	TRUE	FALSE	SE	progressWireless drivers to be included in CIP kernel	https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7_1	Default Action
CR-1.7	Password generation and life-time restrictions for human users	TRUE	FALSE	SE	pack-testing/cip-security-tests/-/tree/master/iec-ages security-tests/singlenode-passwordtestcases/TC_CR1.7-RE1_1 login	https://github.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-ages security-tests/singlenode-passwordtestcases/TC_CR1.7-RE1_1	Default Action
CR-1.7	Password life-time restrictions for all users (human, software process, or device)	FALSE	FALSE	SE	None		This is for SL-4

Req ID	Requirement name	Need applicability	Status if supported	Why HW by IEC-62443-4-2 tests reference	CIP recommendation
CR-1.8	Public key infrastructure (PKI) certificates	TRUE	FALSE	Completed https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-opensstestcases/TC_CR1.8_1	Default Action
CR-1.9	Strength of public key-based authentication - check validity of signature of a given certificate	TRUE	FALSE	Completed https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-opensstestcases/TC_CR1.9_12 . https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_23 . https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_34 . https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_45 . https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_56 . https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_6	Default Action
CR-1.9 RE(1)	Hardware security for public key-based authentication	TRUE	FALSE	Completed https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-opensstestcases/TC_CR1.9_6	It requires HW support, should be met by CIP users
CR-1.10	Authentication feedback	TRUE	FALSE	Completed https://gitlab.com/cip-project/cip-pack-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-opensstestcases/TC_CR2.10_1	Default Action

		Need	Status					
		ap-	if					
		pli-	sup-					
		Support	Not supported					
Req	Requirement	by HW	by HW					
ID	name	CIP support	IEC-62443-4-2 tests reference					CIP recommendation
CR-1.11	Unsuccessful login attempts - limit number	FALSE	FALSE	Completed	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iecpack-security-tests/singlenode-age	testcases/TC_CR1.11_1	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-bin	testcases/TC_CR1.11_2
CR-1.12	System use notification	FALSE	TRUE	SEA	None			
ND-1.13	Access via untrusted networks	FALSE	TRUE	SEA	None			

Default Action
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.
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.

Req ID	Requirement name	Need ap- pli- Support	Status if sup- ported	Why not supported	IEC-62443-4-2 tests reference	CIP recommendation
ND-1.13	Explicit access request approval	FALSE	FALSE	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	Complete	https://github.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.8_1	Default Action
CR-1.14	Hardware security for symmetric key-based authentication	TRUE	FALSE	None		Requires HW support