#### IoT System Certification Scheme



P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024 Page : 10 of 34

The validity of the "Certificate of Approval" will be issued for three years from date of issue. **Essential Security Requirements** 

Sr. No.	Category	Testing Parameter	What to be tested	Documents Required	Implement ation Details	Comm ent by Develo per
						Yes/N o
1.	Hardware Level Security Parameter (supported by software)	1.1 Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	<ol> <li>Identification of the availability of debugging interfaces such as USB, UART, and other serial variants through the Datasheet of the SoC being used in the device under test</li> <li>Verification and validation of the ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same as declared in the vendor documentation</li> <li>Testing, in presence of OEM team, to verify the enabling/disablin g of all the ports</li> </ol>	The vendor shall provide the following: a. Datasheet of the SoC being used in the device. b. Documentation related to ports/interfaces enabled in the production devices and the related access control mechanism for protection of the same. c. Process flow of the Manufacturing/ Provisioning of the device		





#### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01

Date : 21-05-2024

Page : 12 of 34

	_	-		
	certificates	verification	and certificates	
	are unique	through:	being used in the	
	to each	<ul> <li>Testing, in</li> </ul>	device ecosystem	
	individual	presence		
	device.	of OEM	2. Key management	
	aevicei	team	life cycle (nurnose	
		Cada	anoration	
		• Code	generation,	
		review	storage,	
		<ul> <li>Process</li> </ul>	destruction/zeroiz	
		audit of	ation, validity, key	
		the key-	changeover/rotatio	
		life cycle	n)	
		process		
	1.3 Verify	1. Identification	The vendor shall	
	that on-chip	of the availability	provide the	
	dehugging	of debugging	following.	
	interfaces	interfaces such as	ionowing.	
	such ac	IISB IIABT and	a Datasheet of the	
	ITAC or	other corial	a. Datasneet of the	
	JIAG OI	oullel Sellal	soc being used in	
	SWD are	Variants	the device.	
	disabled or	through the		
	that	Datasheet of the	b. Documentation	
	available	SoC being used in	related to	
	protection	the device under	ports/interfaces	
	mechanism	test	enabled in the	
	is enabled		production devices	
	and	2. Verification	and the related	
	configured	and validation of	access control	
	appropriate	the	mechanism for	
	lv.	ports/interfaces	protection of the	
	5	enabled in the	same.	
		production	50000	
		devices and the	c Process flow of	
		related access	the	
		control	Manufacturing/Dro	
		control machanism for	Manufacturing/FIO	
			visioning of the	
		protection of the	uevice	
		same as declared		
		in the vendor		
		documentation		
		О		
		3. Testing, in		
		presence of OEM		
		team, to verify the		

СТОС	IoT System Certification Scheme					
				Issue : 01		
।। जागोः कर्षे चार्याप्र ।।।	P01 — Procedure	e for CCTV Testin	g	Date · 21	-05-2024	
।। गुणात्मव समृाद्धः ।।	Evaluation	n and Certificatio	n –	$D_{acc}$ · $21$	of 24	
				Page : 15	01 34	
		enabling/disablin g of all the ports and debugging interfaces such as USB, UART, and other serial variants using their relevant hardware based debuggers and access control mechanisms in case the interface is enabled. 4. Process audit of the manufacturing facility to validate				
		facility to validate the vendor's claim regarding the debugging interfaces which are closed/disabled during provisioning.				
		[For instance, through Block connection diagram depicting pin connections between the host microcontroller and its interactions with various sub components/peri pherals.]				
	1.4 Verify that trusted execution is	Identifying whether TEE/SE/TPM is	The vendor provide following:	shall the		



### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 14 of 34

implemente d and enabled, if available on the device SoC or CPU.	available or not in the device through the SoC datasheet and technical documentation submitted by the vendor.	<ol> <li>Datasheet of the SoC being used in the device.</li> <li>User manual/ Technical specifications of the device</li> </ol>	
	Further assessment is done on the basis of scenarios as applicable to device as defined below:	3. Code snippets of the TEE API call, wherever applicable	
	CASE1:TEE/SE/TPMisnot available:Nofurtherassessment		
	CASE 2: TEE/SE/TPM is available and enabled: Verification through code- review that crypto functions are called through TEE/SE/TPM APIs.		
	CASE 3: TEE/SE/TPM is available but not enabled by the vendor: Termed as non- conformance to the requirement.		



#### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 15 of 34

1.5 Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environme nt), or protected using strong cryptograp hy.	OEM is required to enable and implement the <u>TEE/SE/TPM.</u> Identifying all the keys and certificates being used in the device eco-system, sensitive data and their storage mechanism(s); and verification through: • Testing, in presence of OEM team • Code review • Process audit of the key- life cycle process	Vendor shall submit the following: 1. List of all keys and certificates being used in the device ecosystem 2. List of all the sensitive data with their intended usage and secure storage mechanism(s) as implemented along with secure configurations to be enabled in the device. 3. Key management life cycle (purpose, generation, storage, destruction/zeroiz ation, validity, key changeover/rotatio n) private keys and certificates.	
1.6Verify the presence of tamper resistance and/or	Testing, in presence of OEM team, to verify the measures implemented in the device to	Vendor shall submit the following: 1. Measures available in the	
tamper detection	prevent software and hardware	device to prevent software	



#### IoT System Certification Scheme

#### P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 16 of 34

features.	tampering.	tampering.	
		2. Measures available in the device to prevent hardware tampering.	
1.7 Verify that any available Intellectual Property protection technologie s provided by the chip manufactur er are enabled.	Testing, in presence of OEM team, to verify the enabling of the Intellectual Property protection technologies provided by the chip manufacturer, if available.	Vendorshallsubmitthefollowing:1. Datasheet of theSoC2. DocumentationregardingtheIntellectualPropertyprotectiontechnologiesprovidedby thechip manufacturerwhich have beenenabled.3. In case, noIntellectualPropertyprotectiontechnologiesarebeing provided bythechip manufacturer, thenadeclarationstating the same.	
1.8Verifythedevicevalidatestheboot	Testing, in presence of OEM team, to verify the following:	Vendor shall submit the following:	
image signature before loading.	1. Device boots up successfully with the documented	<ol> <li>Datasheet of the SoC</li> <li>Technical specifications of</li> </ol>	



Public

P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 17 of 34

	secure boot process when a valid boot image is provided. 2. Device does not boot up when a tampered boot image (like with missing signature, invalid signature) is provided.	the device regarding secure boot (should consist of keys involved and their management life cycle <sup>*</sup> , signature validation process and any other secure mechanisms if implemented.)	
1.9 Verify usage of cryptograp hically secure pseudo- random number generator on embedded device (e.g., using chip- provided random number generators)	Verification of the documentation provided by the vendor regarding the random number generators being used in the device. Verification through code- review that random number generators or related libraries as applicable are being used in the device.	Vendorshallsubmitthedocumentationregardingtherandom generators(eitherhardwarebased or softwarebased or softwarebased or both)being used in thedevice with theirintended usage.In case, hardwarebased randomnumber generatorsarebeingused, vendorsshallsubmitthefollowing:1. Datasheet of theSoC2.Technicalspecificationsofthedeviceregardingrandomgenerators	



### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 18 of 34

				In case, software based random number generators are being used, vendors shall provide the libraries being used for the same.	
2.	Software/Fir mware	2.1 Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/ IoT operating system, if applicable. 2.2 Verify that the firmware apps protect data-in- transit using transuport	Testing, in presence of OEM team, to verify the declared memory protection controls available and enabled in the device using command line based tools/commands or any other open source tool like DEP, EMET tool.	Vendor shall submit the declaration of the memory protection controls available and enabled in the device. The vendor shall submit the specifications and documentation related to the configurations available in the applications and	
		transport layer security.	<ol> <li>Verifying that device properly validates the server's TLS certificate to ensure that it is trusted and has not been tampered with.</li> <li>Testing for</li> </ol>	transport layer security.	





### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 20 of 34

	related to	signatures of the	
	secure	server connections.	
	server		
	connectio		
	ns and		
	digital		
	signature		
	validation		
	25		
	implemen		
	ted like		
	strong		
	cinher		
	suites		
	secure		
	TLS		
	version		
	SSL.		
	ninning		
	etc		
	sunnorted		
	by code		
	walkthrou		
	σh		
	8 <sup>11</sup>		
	Proper		
	certificate		
	validation		
	vandation		
	, certificate		
	chain		
	validation		
	and		
	certificate		
	revocatio		
	n checks		
	are		
	imnlemen		
	ted in the		
	device		
	2. Testing for		
	vulnerabilities		
	which can affect		
	vulnerabilities which can affect		



STOC	IoT System Certification Scheme						
गुणोत्कर्षे समृद्धि :	P01 — Procedure Evaluation	e for CCTV Testin n and Certificatio	CCTV TestingIssue : 01d CertificationDate : 21-05-2024Page : 21 of 34				
		<ul> <li>the security of TLS connection such as padding oracle attacks, or weak cipher suites.</li> <li>3. Using tools such as Nmap to identify open ports through which device can be accessed leading to unintended data retrieval.</li> <li>4. Verifying that TLS session(s) are resistant to attemptsof interception and decryption of network traffic using man-in-themiddle attacks using tools like Burpsuite.</li> </ul>					
	2.4 Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	Secure code review [both automated and manual], in presence of OEM team, using a licensed static analysis tool through any of the following approaches: 1. Visit to the evaluation agency by the vendor	Vendor provide : 1. F binaries f review. 2. Interna review rep	shall firmware for code al code orts			



P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01

Date : 21-05-2024

Page : 22 of 34

	with the		
	firmware code		
	and installing the		
	licensed static		
	analysis tool		
	available with the		
	evaluation agency		
	in their systems		
	[Recommended]		
	Incommented		
	2 Visit to the		
	evaluation agency		
	by the vendor		
	with the		
	firmware code		
	and any licensed		
	static analysis		
	tool available		
	with them and		
	demonstrating		
	the code review		
	activity in the		
	activity in the		
	presence of		
	representatives		
	of evaluation		
	agency.		
	2 Civing a romoto		
	5. Giving a remote		
	access of the		
	systems dl		
	ovaluation agongy		
	for installing their		
	licensed		
	analyzia ta -1		
	analysis tool		
	available with		
	uiem.		
	1. Civing a romoto		
	T. UIVING a TEINULE		
	access of the		
	systems at		
	venuor site to the		
	evaluation agency		
	containing the		

Public



### IoT System Certification Scheme

#### P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 23 of 34

	2.5 Verify that each firmware maintains a software bill of materials cataloging third party component s, versioning, and published vulnerabilit ies.	firmware code along with the licensed static analysis tool available with the vendors. Verification of the submitted list of third party components by running automated tools like FACT on the firmware. Identifying vulnerabilities in the third party component(s) through publically available vulnerability databases Verification and validation of the process defined by the vendor for	Vendor shall submit the following: 1. Documentation for information on software bill of materials, including third- party components and versions. 2. Organization process and policies for the following: • Addressing and patching any identified vulnerabilit	
	cataloging third party	firmware.	materials, including third-	
	component	Identifying	party components	
	S,	vulnerabilities in	and versions.	
	and	component(s)	2. Organization	
	published	through	process and	
	vulnerabilit	publically	policies for the	
	ies.	available	following:	
		vulnerability		
		databases	Addressing     and	
		Verification and	patching	
		validation of the	any	
		process defined	identified	
		by the vendor for	vulnerabilit	
		providing regular	ies in third-	
		and natches for	party	
		the firmware to	S.	
		address any	-	
		known	Informing	
		vulnerabilities in	the	
		third-party	customers	
		components.	about the	
			issues or	
			vulnerabilit	
			ies and	
			providing	
			security	



#### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 24 of 34

			updates and patches for the same. 3. Configuration management system and related policies for maintaining firmware and third party binaries, libraries and frameworks along with the patches/fixes issued to the devices.	
	2.6 Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors ).	Independent secure code review [both automated and manual] using a licensed static analysis tool through any of the following approaches: 1. Visit to the evaluation agency by the vendor with the firmware code and installing the licensed static analysis tool available with the evaluation agency in their systems. [Recommended] 2. Visit to the	<ul> <li>Vendor shall provide :</li> <li>1. Firmware binaries for code review.</li> <li>2. Internal code review reports</li> </ul>	



Public

STOC	C I System Certification Scheme				
			Issue :	01	
।। गणोत्कर्धे समध्दि :।।	P01 — Procedure	e for CCTV Testin	g Date :	21-05-2024	
3	Evaluatio	n and Certificatio	n Page :	25 of 34	
	2.7 Verify	evaluation agencyby the vendorwiththefirmwarecodeand any licensedstaticanalysistoolavailablewiththemanddemonstratingthe code reviewactivityinpresenceofrepresentativesofevaluationagency.3. Giving a remoteaccessofaystemsatvendor site to theevaluation agencyfor installing theirlicensedstaticanalysistoolavailablewiththem.4. Giving a remoteaccessofavailablewiththem.4. Giving a remoteaccessofavailablewiththem.4. Giving a remoteaccessofavailablewiththem.1. Identifying the	Vendor shall		
	that the	scenarios when	submit a document		
	firmware	the device	mentioning the		
	the digital	server	device establishes		



### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01

Date : 21-05-2024

Page : 26 of 34

	signature to	connec	tions with	server connections	
	signature to a trusted server(s).	connec the world verifyir followin	tions with external and ng the ng: Security features, related to secure server connectio ns and digital signature validation as implemen ted like strong cipher suites, secure TLS version, SSL pinning etc. supported by code walkthrou gh. Proper	server connections with the external world, with detailed information about the security measures in place while validating the digital signatures of the server connections.	
		•	supported by code walkthrou gh. Proper		
			validation , certificate chain validation		
			and certificate revocatio n checks are		



### IoT System Certification Scheme

#### P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 27 of 34

	implemen ted in the device.		
2.8 Verify security controls are in place to hinder firmware reverse engineering (e.g.remova l of verbose debugging symbols).	Testing, in presence of OEM team, to verify the security controls as provided by the vendor to hinder firmware reverse engineering.	Vendor shall submit the documentation regarding the security controls in place to hinder firmware reverse engineering.	
2.9 Verify that the firmware update process is not vulnerable to time-of- check vs time-of-use attacks.	Testing, in presence of OEM team, to verify the measures implemented in the device to make it resistant to time-of-check vs.time-of-use attacks.	Vendor shall submit the measures implemented in the device to make it resistant to time- of-check vs. time- of-use attacks.	
2.10 Verify the device uses code signing and validates firmware upgrade files before installing.	Testing,inpresenceof OEMteam, to verify thefollowing:1.Devicegetssuccessfullyupdated with thedocumentedsecureupgradeprocesswhen avalidupdatepackageisprovided.2.Device does notbootup when a	Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle <sup>*</sup> , signature validation process and any other secure mechanisms if implemented.	



#### IoT System Certification Scheme

#### P01 — Procedure for CCTV Testing Evaluation and Certification

Issue : 01

Date : 21-05-2024

Page : 28 of 34

2.11 Verify that the device cannot be d to old versions (anti- rolback) of valid firmware.Testing, in presence of OEM team, to verify that the device cannot be that the device cannot be downgraded to old versions (anti- rolback) of valid firmware.Vendor shall submit the process of achieving secure trimware upgrade consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.2.12 Verify that that firmware.Verification shall be done as per the applicable scenario:Vendor shall provide the following:2.12 Verify that firmware upon a perform automatic firmware upon a procedure schedule.Verification shall procedure for issuing automatic operating procedure for issuing automatic updates validspreade s to the in-field devices is required to beVendor shall process and process and process and process and process and process and process and process to the devices is required to be				
2.11 Verify thatTesting, presence of OEM team, to verify that the device downgrade d to old versions (anti- rollback) of valid firmware.Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.2.12 Verify that that firmware.Verification shall be done as per the applicable scenario: perform automatic firmware automatic firmwareVerification shall provide the applicable scenario: 1. Modes of updates are available: a schedule.2.12 Verify that firmware updates upon a predefined schedule.Verification shall be done as per the applicable scenario: the applicable scenario:Vendor shall provide the scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable scenario: the applicable 		tampered update package (like with missing signature, invalid signature) is provided.		
2.12 VerifyVerification shallVendorshallthatbe done as perprovidethefirmwaretheapplicablefollowing:canscenario:-perform1.ModesofautomaticCase1:updatesavailablefirmwareAutomatic OTAi.e.automatic,updatesupdatesaremanual or both.uponaavailable:-predefinedAstandard2.schedule.operatingprocessandprocedureforupdates to thei.e.schedule.stondardicites regardingi.e.uponastandardistondardischedule.operatingprocessandprocedureforupdates to thei.e.s to the in-fielddevicesisqupdatesisto thes to the in-fielddevices.devicesisrequired to beis	2.11 Verify that the device cannot be downgrade d to old versions (anti- rollback) of valid firmware.	Testing, in presence of OEM team, to verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.	Vendor shall submit the process of achieving secure firmware upgrade which should consist of keys involved and their management life cycle*, signature validation process and any other secure mechanisms if implemented.	
submitted by the vendor which can then be evaluated by the evaluation agency as per	2.12 Verify that firmware can perform automatic firmware updates upon a predefined schedule.	Verification shall be done as per the applicable scenario: Case 1: Automatic OTA updates are available: A standard operating procedure for issuing automatic updates/upgrade s to the in-field devices is required to be submitted by the vendor which can then be evaluated by the evaluation agency as per	Vendorshallprovidethefollowing:1.Modes1.Modesofupdatesavailablei.e.automatic,manual or both.2.Organizationalprocessandpoliciesregardingtheissuingofupdatestothedevices.of	



P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Public

Page : 29 of 34

			security requirement.		
			Case2:AutomaticOTAupdatesareavailableandvendorprovidesmanualupdates:Astandardoperatingprocedureprocedureforissuingmanualupdates/upgradestotothein-fielddevicesis		
			required to be submitted by the vendor which can then be evaluated by the evaluation agency as per C20, C21 and C22 security requirement.		
3.	Secure Process Conformance	3.1 Verify that wireless communica tions are mutually authenticat ed.	Testing, in presence of OEM team, to verify the process of mutual authentication as laid down in the documentation by the vendor.	Vendors shall provide the documentation regarding the process of mutual authentication as implemented in the device when wireless communications are initiated.	
				In case, the device does not support wireless communications, the vendor shall provide a declaration for the	



### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01

Date : 21-05-2024

Page : 30 of 34

			same.	
-	3.2 Verify	Identifying all the	Vendors shall	
	that	security	provide the	
	wireless	mechanisms	documentation	
	communica	heing used in the	regarding the	
	tions are	communication	socurity mossures	
	uons are	communication	implemented in the	
	sent over	process		
	an	verification	device to prevent	
	encrypted	through:	tampering of the	
	channel.	<ul> <li>Testing, in</li> </ul>	data being sent	
		presence	through wireless	
		of OEM	mode of	
		team	communication.	
		Code		
		review	In case, the device	
		<ul> <li>Process</li> </ul>	does not support	
		audit of	wireless	
		the key-	communications,	
		life cycle	the vendor shall	
		process	provide a	
		process	declaration for the	
			same.	
			buille	
-	3.3 Verify		Vendor shall	
	that		submit Bill of	
	whether		materials for	
	trusted		critical hardware	
	sources are		components	
	heing used		(related to security	
	for sourcing		functions libe So()	
	the		runctions like 500J.	
	component			
	component			
	s oi the			
	uevice i.e.			
	trusted			
	supply			
	chain			
	through a			
	managed			
	Bill of			
	materials			
	for critical			
	hardware			
	component			



### IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 31 of 34

	s (related to		
	security		
	functions		
	like SoC) is		
	in use.		
	3.4 Supply	Vendor shall	
	chain risk	submit the	
	idontificatio	following:	
	n	Supply shain rick	
	11, 	Supply chain lisk	
	assessment,	identification,	
	prioritizatio	assessment,	
	n, and	prioritization, and	
	mitigation	mitigation	
	shall be	documents.	
	conducted.		
	Supply	Supply chain	
	chain	risk/business	
	risk/busine	continuity planning	
	SS	policy documents,	
	continuity	playbooks	
	planning	reflecting how to	
	policy	handle supply	
	documents,	chain disruption,	
	playbooks	post-incident	
	reflecting	summary	
	how to	documents.	
	handle		
	supply		
	chain		
	disruption		
	nost-		
	incident		
	summary		
	documents		
	nood to bo		
	submitted		
	and		
	domonstrat		
	a the same		
		 De sum ent	
	3.5 Verify	Document for	
	tne no	Network protocols	
	proprietary	used in the device.	
	network		
	protocols		



#### **IoT System Certification Scheme**

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 32 of 34

		are being			
		used in the			
		device. If			
		ves. then			
		complete			
		implementa			
		tion details			
		and the			
		source code			
		for the			
		same shall			
		bo			
		provided			
1	Socurity	4.1 Design		Docign and	
т.	Conformanco	and		architactura	
	at product	anu		documents till the	
	development	a dotaile till		DCDA and SoC	
	atago	the DCPA		PUDA allu SOU	
	Stage	ule FCDA		level.	
		land SOL			
		level to be			
		ald in			
		counterfeit			
		mitigation			
		and			
		malware			
		detection.			
		4.2 Threat	Process and		
		mitigation	method artifacts		
		strategies	need to be		
		for tainted	submitted and		
		and	demonstrate the		
		counterfeit	same.		
		products			
		shall be			
		implemente			
		d as part of			
		product			
		developme			
		nt.			
		4.3 One or	List of		
		more up-to-	components that		
		date	have been		
		malware	identified as		



P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01

Date : 21-05-2024

Page : 33 of 34

	detection	requiring		
	tools shall	tracking targets		
	be	of		
	deployed as	tainting/counterf		
	nart of the	eiting CM tool		
	code	Quality assurance		
	accentance	nrocess need to		
	and	he submitted and		
	developmo	demonstrate the		
	nt	come		
	nrocassas	Same.		
	processes. Malwara			
	dotaction			
	tochniquos			
	chall ha			
	silali De			
	useu belore			
	nackaging			
	раскадінд			
	and			
	delivery			
	(e.g.,			
	Scanning			
	finished			
	products			
	and			
	component			
	s for			
	malware			
	using one			
	or more up-			
	to-date			
	malware			
	detection			
	tools).			
	4.4 Supply		Supply chain	
	chain risk		risk/business	
	identificatio		continuity planning	
	n,		policy documents,	
	assessment,		playbooks	
	prioritizatio		reflecting how to	
	n, and		handle supply	
	mitigation		chain disruption,	
	shall be		post-incident	

Public



# STCC ।। गुणोत्कर्धे समृध्दि ः।।

## IoT System Certification Scheme

P01 — Procedure for CCTV Testing Evaluation and Certification Issue : 01 Date : 21-05-2024

Page : 34 of 34

conducted.	summary	
	documents need to	
	be submitted and	
	demonstrate the	
	same.	