

File No. NCCS/SC/1-2/2024-25
भारत सरकार/ Government of India
संचार मंत्रालय/Ministry of Communications
दूरसंचार विभाग/Department of Telecommunications
राष्ट्रीय संचार सुरक्षा केंद्र / National Centre for Communication Security
बेंगलुरु - 560027/ Bengaluru - 560027

Dated: .12.2024

Subject: General instructions to the applicants for Security Certification applications in the MTCTE portal -reg.

It has been observed that while applying for the security certification some of the OEMs make incorrect and irrelevant entries which lead to problems in issuing certificates at the later stage. In addition, industry raised some practical issues concerning DUT. Hence, the following instructions are issued to address these points.

2. Regarding ITSAR BoM:

- a) It has been observed that many applicants are not using the sample ITSAR BoM file (available for download in during the application stage) as available in the MTCTE portal. Instead, they are using their own company's BoM file or modified sample file. Altering the format of sample ITSAR BoM file may result in errors at the time of certificate generation. Hence, the applicants are advised to edit/enter the details in the sample ITSAR BoM file downloaded from the portal and upload it to avoid such errors.
- b) Only the software which can be verified after power-on of device are to be listed in the ITSAR BoM. Only the information that needs to be captured in the Certificate need to be submitted at this stage. These may include - Firmware/BIOS/Bootloader, Operating system, Crypto module, preloaded Application software etc. If it is a single package (consisting of OS, Crypto algorithms, Applications software or any other software), only details of that package need to be entered. It has been observed that the applicants are uploading complete Software BoM (SBoM) in place of ITSAR BoM. The same may be avoided and instead, only the required

information as indicated above is to be mentioned in ITSAR BoM. The complete Software BoM is to be submitted to the selected TSTL at the time of submission of DUT and consolidated information sheet (Declaration) for testing purpose, which shall be verified as part of compliance of ITSAR Clauses, wherever applicable. The information provided in the ITSAR BoM will be used for certificate generation, hence, the same is to be filled with due diligence.

- c) Some of the applicants make typographical errors while entering software name and version number, hash values, serial number etc. in the ITSAR BoMs at the time of submitting the applications. Based on the requests from industry to allow such applications, as a one-time measure, it has been decided that an applicant may correct ITSAR BoM details by submitting an undertaking on the company's letterhead by the authorised signatory to the selected TSTL. It may be noted that only modification /and deletion of details will be permissible. Adding new details in the ITSAR BoM is not allowed. Such modification requests should be submitted within 15 days of acceptance of application or before submission of first test plan by the selected TSTL, whichever is earlier.
- d) In general, no change in DUT's software is allowed after the start of testing (submission of first test plan). During the testing, if DUT fails any test and a software upgrade/change is the remedy to make the DUT compliant to the ITSAR conditions, then the software change shall be allowed.

3. The timeline with milestones issued by NCCS for Security Certification process for completing the testing is to be strictly followed. The same is attached herewith as Annex-A. DUT, along with necessary documentation and complete consolidated information sheet/undertaking, vide letter No. NCCS/HQ/COMSEC/2021-22/III-Part-(2)/627 dated 14.10.2024 (enclosed as Annex-B), must be submitted to the selected TSTL as per the timeline (within 15 days after the acceptance of application by TSTL) for the start of testing. The same is also required for issuing *Pro Tem* certificate. The application is liable to

be rejected if there is delay in submission of DUT along with Consolidated DUT Information sheet/ documents/clarifications as sought by TSTL/NCCS beyond the timeline prescribed by NCCS.

4. The DUT's default configuration as submitted to the TSTL should be hardened for ITSAR compliance. Submission of hardened DUT to the TSTL shall be the responsibility of the applicant. The configuration should not change after device reboot or reset. If configuration changes after reboot it will be sole responsibility of the applicant to ensure that device is configured properly before taking up other tests.

This issues with the approval of competent authority.

Encl: As above

Digitally signed by
Sumit Singh
Date: 06-12-2024 12:56:41
Sumit Singh
ADG(SC-I)
NCCS

To,

1. All OEMs/Dealers/Importers/applicants/designated TSTLs- through NCCS website

Copy for kind information to:

1. Member(S), DCC
2. DDG(SA), DoT HQ

Timelines with Milestones for Security Certification process

S.N.	Milestone No.	Milestone Detail	Max. Timeline by which milestone is to be completed by
1.	Milestone 1	Acceptance of application by TSTL	T0
2.	Milestone 2	Appointment of Validator by NCCS	T0+1 week
3	Milestone 3	Receipt of DUT by TSTL from OEM along with complete documentation with filled product details in prescribed format as specified by NCCS, Commands list, required manuals, reports, Declarations, Undertakings as required by ITSAR	T0+2 week=T1
4	Milestone 4*	Completion of identification of DUT by TSTL and submission of First Test plan by TSTL	T1+1 week
5	Milestone 5*	DUT Verification by Validator and Completion of approval of First Test plan by Validator	T1+2 week
6	Milestone 6*	Completion of submission of all Test plans by TSTL to Validator	T1+3 week
7	Milestone 7*	Completion of approval of all Test plans by Validator	T1+7 week
8	Milestone 8	Completion of Testing by TSTL, submission of Test reports by TSTL, Validation of all test reports from Validator and submission of Technical Oversight report by Validator	T1+12 week
9	Milestone 9	Appointment of Evaluator by NCCS and completion of evaluation by Evaluator	T1+15 week
10	Milestone 10	Re-testing by TSTL based on inputs from Validators, Evaluators, if any and submission of revised reports	T1+19 week
11	Milestone 11	Completion of Final evaluation by Evaluator and submission of Evaluator report	T1+20 week=T2
12	Milestone 12	Processing of Case by Director(SC)	T2+1 week
13	Milestone 13	Processing of Case by DDG(SC)	T2+1 week

*- Testing shall start as soon as possible and first test plan is approved by validator. Testing will go on simultaneously with Test plan approval.

File No. NCCS/HQ/COMSEC/2021-22/III-Part-(2)/627
भारत सरकार/ Government of India
संचार मंत्रालय/Ministry of Communications
दूरसंचार विभाग/Department of Telecommunications
राष्ट्रीय संचार सुरक्षा केंद्र / National Centre for Communication Security
बेंगलुरु - 560027/ Bengaluru – 560027

Date: 14.10.2024

Sub: Declaration by OEM/Applicant, to be submitted to Designated TSTL along with the DUT – Reg.

Reference is invited to the subject cited above.

2. In this regard, in order to fast track the security testing and to streamline the necessary information required for identifying the DUT and to prepare Test Plans, it is requested that OEMs/Applicants must submit the information of DUT, in the enclosed format and documents to Designated TSTL while submitting the DUT, after acceptance of application by TSTL in portal.

This issues with approval of the Sr. DDG NCCS.

Encl: As Above

**Rama Krishna
Majety** Digitally signed by
Rama Krishna Majety
Date: 2024.10.14
18:29:21 +05'30'
(Rama Krishna Majety)
Director(SC&HQ), NCCS

To:

- (i) OEMs/Prospective Applicants- through NCCS website
- (ii) Designated TSTLs - through NCCS website

Copy to:

- (I) All officers of NCCS

Declaration by OEM/Applicant (To be submitted to Designated TSTL along with DUT)**(Please sign on each page)****A. General Information**

1. Name of the Product :
2. Application Id (copy from portal) :
3. ITSAR Ref (copy from ITSAR document) :
4. OEM Name :
5. Applicant Name :
6. Name and Contact Details of Authorized Signatory of Applicant :
7. Name and Address of TSTL :
8. Date of supply of DUT to TSTL :
9. ER Certificate details if already issued (Certificate copy to be provided) :
10. EoS and EoL dates (if declared) :
11. Any other details :

B. Product Related Details (Please strike out what is not applicable)

1. Product/ DUT Description, use and purpose (A network diagram showing the DUT with other connected entities to enable testing)	:
2. Deployment Scenario a. Standalone (Aggregated) b. Disaggregated (split) c. Is it cloud hosted	Yes/ No Yes/ No If disaggregated, pl furnish the details of the elements and their deployment locations Yes/ No If yes, furnish the following details Service Model: IaaS/ PaaS/ SaaS Deployment Model: Public/ Private/ Hybrid/

	<p>Mixed If non-private, the details of CSP CSP Name: Location of DC and DR: DC at DR at.....</p> <p>Is the cloud security certified: Yes/ No If yes, please furnish Cloud Security certification details</p>
<p>3. Main Model</p> <p>-(Same as per ER Certificate/ER Application and also, should match with the Security Certification application applied for) -No Grouping with Different ER Certificates</p>	<p>:</p>
<p>4. Associated Model(s)</p> <p>-(Same as per ER Certificate/ER Application and also, should match with the Security Certification application applied for) -No Grouping with Different ER Certificates</p>	<p>:</p>

C. Technical Details

1) Identification of Main Model (DUT)

- a) Hardware
 - i) Make :
 - ii) Model Name :
 - iii) Model Number :
 - iv) Serial Number :
 - v) Any other physical Identifier :

- b) Main Software
 - i) Software Name :
 - ii) Version/ Release :
 - iii) Hash Value :
- c) Firmware
 - i) Firmware Identifier :
 - ii) Version/ Release :
- d) Any logical Identifier
 - i) Certificate Id (X.509) :
 - ii) Trusted Platform Module or similar :

2) Debug interfaces (if available, please specify)

Sl. No.	Name of debug interface	Tick the relevant interfaces
1	JTAG	
2	SWD	
3	SPI	
4	Any other	

3) OAM Access supported by DUT

a) Local

i) Console : Yes/ No

If yes, Pl specify, the type of console interface

ii) If any other, pl specify

b) Remote

i) SSH : Yes/ No If Yes, Versions....

ii) IPsec : Yes/ No If Yes, Versions....

iii) SNMP : Yes/ No If Yes, Versions....

iv) Web interface : Yes/ No If Yes, Versions....

v) gRPC/gNMI : Yes/ No If Yes, Versions....

vi) TLS(https) : Yes/ No If Yes, Versions....

vii) VPN : Yes/ No If Yes, Versions....

viii) Any other

4) Features/ Functionality

a) NAT/ PAT : Yes/ No

b) DHCP : Yes/ No

c) Firewall : Yes/ No

d) VPN : Yes/ No

e) DNS : Yes/ No

f) ZTP : Yes/ No

g) MPLS : Yes/ No

h) MPLS-TP : Yes/ No

i) SDN : Yes/ No

j) Segmented Routing : Yes/ No

k) IPsec : Yes/ No

l) SCP/SFTP : Yes/ No

m) If any other, please specify the features/ functionalities

5) Network and related Protocols (Please tick all the protocols supported by DUT)

ARP/RARP	<input type="checkbox"/>	BGP	<input type="checkbox"/>	Bluetooth (BLE)	<input type="checkbox"/>	CAPWAP	<input type="checkbox"/>	DHCP	<input type="checkbox"/>	Diameter	<input type="checkbox"/>	DNS	<input type="checkbox"/>
DNS Sec	<input type="checkbox"/>	DTLS	<input type="checkbox"/>	Dynamic DNS	<input type="checkbox"/>	EAP	<input type="checkbox"/>	EoMPLS/ CESoPSN/ SAToP	<input type="checkbox"/>	GLBP	<input type="checkbox"/>	GTP	<input type="checkbox"/>
HSRP	<input type="checkbox"/>	ICMP	<input type="checkbox"/>	IGMP	<input type="checkbox"/>	IP v4	<input type="checkbox"/>	IP v6	<input type="checkbox"/>	ISAKMP/ IKEv2	<input type="checkbox"/>	IS-IS	<input type="checkbox"/>
L2VPN	<input type="checkbox"/>	LDP	<input type="checkbox"/>	LoRa	<input type="checkbox"/>	LPWAP	<input type="checkbox"/>	Mac sec	<input type="checkbox"/>	MPLS FRR	<input type="checkbox"/>	MPLS TE	<input type="checkbox"/>
MPLS TP	<input type="checkbox"/>	NFC	<input type="checkbox"/>	NTP	<input type="checkbox"/>	OSPF	<input type="checkbox"/>	PIM	<input type="checkbox"/>	PPOE/PPOA	<input type="checkbox"/>	Proxy ARP	<input type="checkbox"/>
PTP	<input type="checkbox"/>	Radsec	<input type="checkbox"/>	Radius	<input type="checkbox"/>	RIP	<input type="checkbox"/>	RSVP	<input type="checkbox"/>	RTCP	<input type="checkbox"/>	RTP	<input type="checkbox"/>
SCTP	<input type="checkbox"/>	SIP	<input type="checkbox"/>	SSH	<input type="checkbox"/>	TCP/ UDP/ SCTP	<input type="checkbox"/>	TLS	<input type="checkbox"/>	UPnP/SSDP	<input type="checkbox"/>	VPLS/ H-VPLS	<input type="checkbox"/>
VRRP	<input type="checkbox"/>	WAP	<input type="checkbox"/>	WPA2/3	<input type="checkbox"/>	ZigBee	<input type="checkbox"/>						
Proprietary/Any Other protocols (please state, if any)													

*This is an inexhaustive list and does not contain protocols supported by every telecom/ ICT equipment. The OEM may supply the details which are specific to their products.

6) Miscellaneous

a) Logging

- i) Local : Yes/ No
-Default Capacity of local log buffer (in MB) :
Is the buffer circular or Linear
- ii) External log server support : Yes/ No
-Supported client and version :
- iii) Is the log transfer to external log server occurs in real time: Yes/ No
(If not., pl specify the periodicity)
- iv) Streaming : Yes/ No
- v) If any other, pl specify :

b) Time Synchronization

- i) Is GNSS supported : Yes/ No
If so, pl specify the capability of GNSS to supply phase/ frequency/ ToD references
- ii) If any other is supported, pl specify

c) Method of Authentication

- i) Method of authentication supported
Local: Yes/ No
External: Yes/ No

d) Any default accounts

- i) : Yes/ No
(if yes, give details of default machine / system/ user/ debug/ group accounts)

- e) Group accounts supported : Yes/ No
 f) Any Machine Accounts : Yes/No
 (if yes, give details of machine accounts)

- 7) Cryptography supported by DUT
 a) OAM Access

Sl. No.	Security Services	Security Mechanisms	Protocol and its versions	Key size or relevant details	Is it implemented as per FIPS (Yes/ No)
1	Confidentiality	Encryption			
2	Integrity	Hash			
3	Authentication				
.	Access				
	Non-repudiation	Digital Signature			
n					

Note: All supported cryptographic algorithms shall be listed.

- b) Any other (for communicating to the connected entities)

Sl. No.	Security Services	Security Mechanisms	Protocol and its versions	Key size or relevant details	Is it implemented as per FIPS (Yes/ No)
1	Confidentiality	Encryption			
2	Integrity	Hash			
3	Authentication				
.	Access				
	Non-repudiation	Digital Signature			
n					

8) Manual(s) of DUT containing information required for creating the test document as given in annexure A

D. The following documentation has been submitted along with DUT.

- a) Undertaking /declaration required as per the concerned ITSARs.
- b) Test Reports/ Results (e.g. Static Source Code Internal Test Document, Malware Test Document)
- c) Documents required to enable TSTLs to power on DUT and execute test cases like User Manuals, Security Manual, Security architecture description document MML/ Command set document (including Methods of accessing file systems and other internal systems for conducting tests), configuration manuals etc.

The above stated information is correct and complete to the best of my knowledge.

(Name & Signature of Authorized Signatory of Applicant)

Annexure A

Manual(s) need to cover the following information	Tick the availability of the information
List of all the management and OAM protocols supported by DUT and the details of authentication mechanism used for each one.	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. Available RBAC Support and list of such Roles 2. Process/Command to create User account in DUT 	<input type="checkbox"/>
List for pre-defined user and machine accounts and usage of authentication attributes supported by these accounts, as supported by DUT.	<input type="checkbox"/>
Method to access root or highest privileged user account locally and remotely.	<input type="checkbox"/>
Authorization policy of the users and their roles in the DUT	<input type="checkbox"/>
Information about the unique identifier or user/machine accounts and group account policy of the DUT	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. Method to Configure Password Policy in DUT 2. Confirmation from OEM if central authentication system is supported by DUT 	<input type="checkbox"/>
Information about pre-defined users or default authentication attributes (passwords, tokens, cryptographic keys etc.)	<input type="checkbox"/>
Modes the DUT can support for software update and upgrade also.	<input type="checkbox"/>
STD (For source code analysis) document/Internal Test Report of DUT software	<input type="checkbox"/>
MTD (for malware test document) / Internal Test Report of DUT software	<input type="checkbox"/>
List of all available software in the DUT required and their usage in DUT	<input type="checkbox"/>
<p>List of all required network protocols and services containing at least the following information:</p> <ul style="list-style-type: none"> - protocol handlers and services needed for the operation of network product; - their open ports and associated services; - and a description of their purposes. 	<input type="checkbox"/>
List of Intended mode of boot of DUT.	<input type="checkbox"/>
List of commands for self-test and methods implemented by OEM to verify the methods applied for firmware, software, cryptographic modules used in the DUT to check the same is not tampered.	<input type="checkbox"/>
Undertaking from OEM as per ITSAR Clause 1.3.11	<input type="checkbox"/>

Annexure A

List of available software and hardware function in the DUT and their usage in DUT	<input type="checkbox"/>
List of logs storage location and their access methods.	<input type="checkbox"/>
OEM undertaking for clause 1.6.2	<input type="checkbox"/>
OEM undertaking for clause 1.6.3	<input type="checkbox"/>
Details of Operational and the maintenance mode supported in the DUT.	<input type="checkbox"/>
List of the sensitive data/files present in the DUT (e.g.: startup-configuration, crypto keys, dB) along with list of authorized users with their privilege rights	<input type="checkbox"/>
List of outbound channels supported by the DUT	<input type="checkbox"/>
List of security measures available in the DUT to handle overload situation.	<input type="checkbox"/>
List of available features in DUT to protect against excessive overload.	<input type="checkbox"/>
<p>Details on Filtering IP options for the following is present in DUT or not:</p> <p>a) The support of filtering capability for IP packets with unnecessary options or extensions headers. –</p> <p>b) The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received.</p> <p>c) Guidelines on how to enable and configure this filtering capability.</p>	<input type="checkbox"/>
List of protocols supported by the DUT for fuzzing	<input type="checkbox"/>
List of documented ports on Transport layer and associated services	<input type="checkbox"/>
List of storage sources that are susceptible to being exhausted and measures to prevent by the OEM such as a) Usage of dedicated file systems or quotas for dynamic or growing contents b) File system monitoring.	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. List of ICMP message types which are allowed in addition to permitted ICMP types as per ITSAR. 2. OEM declaration regarding expected DUT behaviour for those ICMP message types that are leading to response from DUT or causing configuration changes 	<input type="checkbox"/>
List of commands for verifying User accounts and their privileges.	<input type="checkbox"/>
List of commands for verifying User accounts present in DUT	<input type="checkbox"/>

Annexure A

<ol style="list-style-type: none"> 1. Declaration from the OEM that OS is sufficiently hardened, and Kernel based applications / functions not needed for the operation of the Network product are deactivated. 2. List of kernel-based applications/functions needed for operation. 3. Procedure to identify kernel-based applications/functions 	<input type="checkbox"/>
List of removable media ports	<input type="checkbox"/>
Information on log file location and procedure to access it	<input type="checkbox"/>
Procedure for how a session is maintained, where the session ID is stored, how it is communicated, the expiration duration of sessions and algorithm used to generate the session ID.	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. List of web server processes run with system-level privileges (e.g., root or administrator). 2. List of user account and its privilege under which the web server is operating 	<input type="checkbox"/>
List of HTTP methods that are required for the web server's operation.	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. List of add-ons or scripting tools for Web server components needed for system operation, 2. The path of the configuration file of web server 	<input type="checkbox"/>
<ol style="list-style-type: none"> 1. List of Supported scripting technology or CGI used in web server and paths to the directories offered for these CGI or scripting technology used/supported. 2. Path of the installed compiler/interpreter 	<input type="checkbox"/>
Paths to the Upload directory, CGI, and scripting directories.	<input type="checkbox"/>
Web server configuration settings for SSI if available.	<input type="checkbox"/>
Path to the root directory and all accessible directories of the web server.	<input type="checkbox"/>
Path to the web server's MIME configuration file and a list of file types required for the operation of the web server and web applications.	<input type="checkbox"/>
Methodology of remote troubleshooting/alarm maintenance of the DUT	<input type="checkbox"/>
Controlled network software rollback mechanisms deployed in the DUT.	<input type="checkbox"/>