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/

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

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	☐	BGP	☐	Bluetooth (BLE)	☐	CAPWAP	☐	DHCP	☐	Diameter	☐	DNS	☐
DNS Sec	☐	DTLS	☐	Dynamic DNS	☐	EAP	☐	EoMPLS/ CESoPSN/ SAToP	☐	GLBP	☐	GTP	☐
HSRP	☐	ICMP	☐	IGMP	☐	IP v4	☐	IP v6	☐	ISAKMP/ IKEv2	☐	IS-IS	☐
L2VPN	☐	LDP	☐	LoRa	☐	LPWAP	☐	Mac sec	☐	MPLS FRR	☐	MPLS TE	☐
MPLS TP	☐	NFC	☐	NTP	☐	OSPF	☐	PIM	☐	PPOE/PPOA	☐	Proxy ARP	☐
PTP	☐	Radsec	☐	Radius	☐	RIP	☐	RSVP	☐	RTCP	☐	RTP	☐
SCTP	☐	SIP	☐	SSH	☐	TCP/ UDP/ SCTP	☐	TLS	☐	UPnP/SSDP	☐	VPLS/ H-VPLS	☐
VRRP	☐	WAP	☐	WPA2/3	☐	ZigBee	☐						
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 : 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.	☐
1. Available RBAC Support and list of such Roles 2. Process/Command to create User account in DUT	☐
List for pre-defined user and machine accounts and usage of authentication attributes supported by these accounts, as supported by DUT.	☐
Method to access root or highest privileged user account locally and remotely.	☐
Authorization policy of the users and their roles in the DUT	☐
Information about the unique identifier or user/machine accounts and group account policy of the DUT	☐
1. Method to Configure Password Policy in DUT 2. Confirmation from OEM if central authentication system is supported by DUT	☐
Information about pre-defined users or default authentication attributes (passwords, tokens, cryptographic keys etc.)	☐
Modes the DUT can support for software update and upgrade also.	☐
STD (For source code analysis) document/Internal Test Report of DUT software	☐
MTD (for malware test document) / Internal Test Report of DUT software	☐
List of all available software in the DUT required and their usage in DUT	☐
List of all required network protocols and services containing at least the following information: - protocol handlers and services needed for the operation of network product; - their open ports and associated services; - and a description of their purposes.	☐
List of Intended mode of boot of DUT.	☐
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.	☐
Undertaking from OEM as per ITSAR Clause 1.3.11	☐

Annexure A

List of available software and hardware function in the DUT and their usage in DUT	☐
List of logs storage location and their access methods.	☐
OEM undertaking for clause 1.6.2	☐
OEM undertaking for clause 1.6.3	☐
Details of Operational and the maintenance mode supported in the DUT.	☐
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	☐
List of outbound channels supported by the DUT	☐
List of security measures available in the DUT to handle overload situation.	☐
List of available features in DUT to protect against excessive overload.	☐
Details on Filtering IP options for the following is present in DUT or not: a) The support of filtering capability for IP packets with unnecessary options or extensions headers. – b) The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received. c) Guidelines on how to enable and configure this filtering capability.	☐
List of protocols supported by the DUT for fuzzing	☐
List of documented ports on Transport layer and associated services	☐
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.	☐
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	☐
List of commands for verifying User accounts and their privileges.	☐
List of commands for verifying User accounts present in DUT	☐

Annexure A

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	☐
List of removable media ports	☐
Information on log file location and procedure to access it	☐
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.	☐
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	☐
List of HTTP methods that are required for the web server's operation.	☐
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	☐
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	☐
Paths to the Upload directory, CGI, and scripting directories.	☐
Web server configuration settings for SSI if available.	☐
Path to the root directory and all accessible directories of the web server.	☐
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.	☐
Methodology of remote troubleshooting/alarm maintenance of the DUT	☐
Controlled network software rollback mechanisms deployed in the DUT.	☐