Frequently Asked Questions

Security Certification & Voluntary Security Certification (VSC)

1. **Whether the fees mentioned in MTCTE portal includes Security Certification too?**

   NCCS Comments: *No. MTCTE has 5 parameters out of which 4 parameters are dealt by TEC and 1 parameter of security testing is dealt by NCCS for which fee has to be paid separately in accordance with ComSec scheme.*

2. **Is there any regulation on the test fee charged by TSTL?**

   NCCS Comments: *No. There is no regulation or cap on the test fee charged by TSTL. The Fee structure is decided by the market forces. The fee may be arrived at through the mutual agreement between TSTL & OEM.*

3. **Has NCCS prescribed any standard tools to be used by TSTL in order to ensure uniform costing?**

   NCCS Comments: *No. NCCS does not prescribe or promote particular tools to be used by TSTL. However, tool used should be capable of performing tests to the required extent.*

4. **With respect to the Voluntary Security Certification, can OEM request TSTL for testing which is still in process of getting accreditation/designation by NCCS?**

   NCCS Comments: *No. An OEM can apply to TSTL for testing only after they get accredited/designated by NCCS. However, they are free to enter into agreement for testing to gain time.*

5. **Do OEMs need to pay for test evaluation fee on or after 1st Jan 2024, in case the conformance tests being carried out by TSTL does not conclude by 31st Dec 2023? (w.r.t VSC scheme)**

   NCCS Comments: *No payment is required for applications received & approved for testing before 1st Jan 2024.*

6. **Can testing be done for software alone?**

   NCCS Comments: *No. According to the Communication Security Certification (ComSec) scheme, security testing & certification is done for a product as a whole. Testing is not carried out for components i.e., software or hardware alone.*

7. **What's the difference between Main & Associated model?**

   NCCS Comments: *The model with full configuration of hardwares, interfaces and all software modules is called main model whereas, Associated models for the purpose of Security certification are those models which have identical software but having hardware which is a subset of the main model. The Associated models shall be certified without testing.*

8. **Does OEM need to provide ER certificate number in the VSC application form for all the sub models/associated models issued by TEC?**

   NCCS Comments: *No. The ER Certificate Number (issued by TEC) for the Main model shall suffice.*

9. **Source Code Security Assurance**: Keeping various points on IPR, sensitivity & Security into consideration, the Source Code of the node is not possible to be shared with DoT/TSTL. Internal Source code review reports are internal to the organization and hence cannot be shared. It has organization secret/confidential information which may harm the organization.

   NCCS Comments: *The source code has to be tested to identify the existing weaknesses in the code. The source code will not be copied to any device in the TSTL. The code brought by OEM will be tested as it is using the tool and the test reports are shared with OEMs to take action on the weaknesses. As per IP router ITSAR, only test document containing test results has to be shared by OEM.*

10. **Cryptographic Algorithms implementation Security Assurance:** Crypto modules are mostly third party. Third-Party crypto modules are implemented from OpenSSL. FIPS 140-2 or later compliance depends on Third-Party. Re-performing testing does not give any benefit, at the same time it is a time-consuming, cumbersome, and extensive exercise.

    NCCS Comments: *Only undertaking that "the crypto module implemented is in compliance with FIPS 140-2 standards" is required in this case. Third party modules can be got tested by OEM to ensure compliance in line with FIPS 140-2 standards. CDAC has necessary tools to conduct tests and provide results to OEMs.*

11. **Fuzz Testing -** A complete Fuzz testing requires a significant amount of compute resources and takes many days to complete, requires a true engineering expert in such a tool to operate, and the results can potentially indicate errors such as timing issues in stress/malformed packets, etc., which needs to analyse by the engineering expert for the specific area to analyse any potential impact and the next steps for each of them. Only OEM which owns the software is equipped and capable of doing this.

    NCCS Comments: *We agree that fuzz testing takes long time and also it needs good amount of expertise to resolve the fuzzing related issues. OEM may have to extend necessary help to TSTL to configure tools during the fuzz testing. To check the robustness of the protocols used in the network function, it is necessary to carry out fuzz testing.*
    Based on the query from Cisco regarding the time required for the fuzz testing, DDG(SAS) clarified that OEMs need not to deploy the R&D team member for the whole-time during fuzz testing. Wherever, any issue related to DUT access, configuration or interoperability between DUT & fuzz tool is required, then only the concerned person of the OEM is required to extend the necessary help to TSTL to carry out the testing expeditiously either in person or through necessary and sufficient documentation.

    Also, NCCS has issued clarification for the kind of fuzz testing i.e., generation based or mutation-based fuzz test required for various protocols.

12. **Vulnerability Scanning -** As Vulnerability can occur at any point in time hence, it is not possible to define any exact date for no known vulnerability. It is an ongoing process that needs to be performed on regular basis and for identified vulnerabilities, appropriate actions are being taken or a mitigation plan is prepared.

    NCCS Comments: *As on the day of applying for certification, the network function has to be free from known critical and high vulnerabilities and the OEM has to submit remediation plan for medium and low vulnerabilities.*

13. **Software Upgrades/Patches/Bugs/Fixes:** Repetitive testing of every software patch or update on regular intervals should be exempted from the certification process under the integrated regime of MTCTE. This would significantly delay the time to deploy any technology/critical functionality in Indian network.

    NCCS Comments: *As per clause 7.1 of the certification scheme, in the event of Software patch/ bug fix/ update, the certificate holder is responsible for ascertaining the compliance of certified equipment, including deployed equipment, with ITSAR and apply for certificate modification. Whenever a patch/ bug fix/ update is released by OEM, it may be permitted to be deployed with a temporary certificate. OEM will submit the changed signature along with all the internal test reports demonstrating to compliance to all security requirements of applicable ITSAR along with an undertaking given in the Annexure. The modified signature of the said model will be incorporated in a temporary certificate with a validity period of up to one year from the date of release or for balance period of initial certificate whichever is earlier. Temporary certificate will be issued within 7 working days of Application normally. Any subsequent request for modification of temporary certificate will be allowed with a validity for balance period of that certificate.*

    During interactions with OEMs, NCCS has requested all OEMs, several times, to provide the software upgrade/update information. This data is yet to be received from OEMs. OEMs are requested to provide details of software update/upgrade for the last two years, so that NCCS may take a call on the issue, in the following format.

S No.	*Name of the product*	*Version and date of initial release*	*Details of software updates/upgrades for last two years*					
			Version No.	*Date*	*Version No.*	*Date*	*Version No.*	*Date*

14. **Different hardware models using the same software**: Software used across different Hardware's should go for integrated MTCTE certification only which will be applicable for 10 years from the issue date of certificate in order to avoid repetitive software testing. Since ITSAR is entirely about tests on Operating System (software) and very rarely on hardware, testing of any single member of family should suffice, for complete family's certification. We request this to be the guiding principle behind the ComSec certifications.

    NCCS Comments: *As per ComSec scheme,* ***'Model'*** *means a particular hardware/software design or version of a product/equipment bearing a unique model number assigned to the equipment. An equipment, which is different in either of hardware/ software/ design/ model/ version, shall be treated as a different model.*

*If OEMs want any change in the definition of the model, then supporting documents/ product brochure may be provided by OEMs **within 15 days** so that NCCS may take a call on specific cases, if required. It is not possible to make such decisions on security test requirements based on generic arguments/data and across the categories.*

15. **List of Cryptographic controls, Table 1**

a. In addition to listed ciphers, nodes support other weaker ciphers for compatibility reasons. Those cannot simply be removed since it would mean that some operators would lose the O&M connectivity to their nodes if we would disable or remove them. The operator has the freedom to disable these weak ciphers by configuration. Therefore, it is recommended to enforce this requirement to Indian operators if it is strictly required.

b. Further specific to SNMP, SNMP is not used as a management protocol in the node but only for the transfer of alarms. No sensitive data is carried over this interface. Today encryption and integrity are based on weak ciphers that shall be enhanced to support the strong ciphers in the future. However, SNMP servers do normally follow the old standard based on weak ciphers. Risk for the mismatch between Node and SNMP server.

c. Allow for use of weak ciphers until SNMP servers, in general, supports strong ciphers and use IPsec as the strong protection. Customers can disable other algorithms (other than Cryptographic Controls prescribed in Table1) by configuration at the time of installation.

NCCS Comments: *Weak ciphers cannot be allowed in the network elements. The cryptographic table of NCCS will be updated periodically to ensure that weak ciphers are not part of the cryptographic table.*

It was clarified that if weak ciphers are present in the product, then the OEMs must demonstrate that the same cannot be exploited by threat actors through changing configuration or any other parameters.

Disclaimer

In case of any variation between what has been produced in these FAQs and that contained in the NCCS documents/other relevant Acts/Rules/Regulations/Policy Statements etc., of the department, the latter shall only prevail.