TaSK Report

1. General Information

Report Generated:	2023-11-13T17:30:32
Start of Execution:	2023-11-13T17:30:28
End of Execution:	2023-11-13T17:30:31
Tester in Charge:	test user
Execution Machine:	ubunutusrv
Execution Type:	Executed via the MICS file

2. Information about the Device Under Test

Title:	Test Application - TLS Server
Application Type:	TR-03116-4-SERVER
Version:	1.0.0
Input Filepath:	/home/toor/tools/TasK/task/com.achelos.task.commandlineinterface/target/ServerMICS.xml
SHA-256 Fingerprint of Inputfile:	F988089938CF543F91DB8E7E041E6B6A283A7EDF25ACD646AF65BD6BE68E00DE

3. Conformity

The MICS of the Device Under Test is not conform with TR-03116-TS.
The Certificates of the Device Under Test are not conform with TR-03116-TS.

4. Summary

4.1 Executed Test Suite Modules

Identifier	Total	Executed	Passed	With warnings	Failed	Start time	End time
ICS Checklist	12	12	9	1	2	2023-11-13 17:30:30	2023-11-13 17:30:30
Certificate Checks	1	1	0	0	1	2023-11-13 17:30:31	2023-11-13 17:30:31

4.2 Summaries of Test Suite Modules

4.2.1 Summary of Module "ICS Checklist"

Identifier	Result
TLS_ICS_01	PASSED_WITH_WARNINGS
TLS_ICS_02	PASSED
TLS_ICS_03	PASSED
TLS_ICS_04	PASSED
TLS_ICS_05	PASSED
TLS_ICS_06	PASSED
TLS_ICS_07	FAILED
TLS_ICS_08	PASSED
TLS_ICS_09	FAILED
TLS_ICS_10	PASSED
TLS_ICS_11	PASSED
TLS_ICS_12	PASSED

4.2.2 Summary of Module "Certificate Checks"

Identifier	Result
Check Certificates for TLS_CERT	FAILED

TaSK Report

5. Test Case Collection Details

5.1 Details of Collection "ICS Checklist"

TLS_ICS_01

Purpose:	The vendor has submitted a current ICS for the implementation to be tested. It covers the exact version of the submitted software.
Result:	PASSED_WITH_WARNINGS
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30
Additional Information:	MICS Verifier: The MICS file is submitted for the version: 1.0.0 The version of the MICS file has to be manually checked against the exact version of the submitted software.

TLS_ICS_02

Purpose:	Table 4 of the ICS contains all mandatory TLS versions according to the application-specific requirement.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_03

Purpose:	Table 4 of the ICS does not contain any TLS version which is not recommended according to the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_04

Purpose:	Table 5 of the ICS contains all mandatory cipher suites according to the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_05

Purpose:	The DUT does not support any cipher suite not recommended according to the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_06

Purpose:	Table 7 of the ICS contains only named groups according to IANA.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_07

Purpose:	Table 7 of the ICS contains all mandatory named groups according to the application-specific requirements.
Result:	FAILED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30
Additional Information:	MICS is missing required named curves for TLSv1.3: brainpoolP256r1tls13

TaSK Report

TLS_ICS_08

Purpose:	Table 6 of the ICS contains only conformant key lengths according to the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_09

Purpose:	Table 8 of the ICS contains all mandatory signature algorithms according to the application-specific requirements.
Result:	FAILED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30
Additional Information:	MICS is missing required Handshake Signature Algorithm for TLSv1.3: ecdsa_brainpoolP256r1tls13_sha256

TLS_ICS_10

Purpose:	Table 9 of the ICS contains all mandatory signature algorithms for certificates according to the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_11

Purpose:	Table 14 provides a maximum session duration not exceeding the maximum session duration defined by the application-specific requirements.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

TLS_ICS_12

Purpose:	The order of the cipher suites as specified in Table 5 represents the correct priority: the less preferred cipher suites (e.g. due to a transitional rule) are put at the end of the list.
Result:	PASSED
Start time:	2023-11-13T17:30:30
End time:	2023-11-13T17:30:30

5.2 Details of Collection "Certificate Checks"

Check Certificates for TLS_CERT

Purpose:	Check whether Certificates are provided.
Result:	FAILED
Start time:	2023-11-13T17:30:31
End time:	2023-11-13T17:30:31
Additional Information:	X509CertificateVerifier: Not enough certificate files have been provided. Required: 3 X509CertificateVerifier: Unable to parse the certificate chain. Certificate missing for Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1 X509CertificateVerifier: Unable to parse the certificate chain. Certificate missing for Subject: C = US, O = Let's Encrypt, CN = R3 X509CertificateVerifier: Unable to parse the certificate chain. Certificate missing for Subject: CN = www.tls-check.de