



Conformance Test Report

IEC 61851-1, DIN 70121 and ISO 15118 (SLAC & V2G message) test cases — SECC under test (VTB)

Report generated: 2026-10-11 07:59:37

Overall: FAIL

System Under Test

Manufacturer	-
Model / type	-
Software / firmware	Everest testing/main @ 2e710bc8191bd5a29c16a4d0815c6bcd9318c51d
Serial / identification	-
Notes	Nightly CI, all SECC stacks Evse15118D20. SUT config: config-test-conformance-ac-full-ocpp.yaml (one of the nightly's rig cycles, each with its own report)
Transfer mode	AC

Black-box DUT: the internal software stack is not observable by the test system; the identification above was entered by the test operator.

Declared capability profile (PICS/PIXIT)

Capability	PICS/PIXIT	Declared
Energy transfer mode	PICS_CMN_CMN_ChargingMode	ac
Payment options offered	PIXIT_SECC_CMN_PaymentOption / PICS_CMN_CMN_IdentificationMode	ExternalPayment, Contract
Certificate services offered	PIXIT_SECC_CMN_CertificateHandling	Install, Update
Certificate validity checked against current time	PICS_SECC_CertificateValidationCheck	yes
Tester CSMS is the DUT's OCPP backend	PIXIT_SECC_TesterCSMS	yes
Transport security accepted	PIXIT_SECC_CMN_TLS	tcp, tls
Value-added service list (VAS)	PIXIT_SECC_CMN_VAS == serviceDetail / PICS_SECC_VAS	no
Internet access service	PIXIT_SECC_CMN_InternetAccess == internetAccess	no
Metering receipts requested	PIXIT_SECC_CMN_ReceiptRequired	no

Capability	PICS/PIXIT	Declared
MeterInfo in charge-loop responses	PIXIT_SECC_CMN_MeterInfo == meterInfo	yes
MeteringConfirmation requested (ISO 15118-20)	PICS_CMN_MeteringConfirmationRequested	no
SalesTariff in schedules	PIXIT_SECC_CMN_SalesTariff == salesTariff	no
Control modes offered (ISO 15118-20)	PICS_CMN_ControlMode	Dynamic, Scheduled
Schedule initially unavailable (ISO 15118-20)	PIXIT_SECC_ScheduleRetrievalSuspended	no
DepartureTime considered	PICS_SECC_CMN_DepartureTime	yes
MaxEntriesSAScheduleTuple considered	PICS_SECC_CMN_MaxEntriesSAScheduleTuple	yes
Renegotiation supported	PICS_CMN_CMN_Renegotiation	no
CP State D (ventilation) during charging	PICS_SECC_CMN_EvStateInChargeProgress == D	no
Pause / resume supported	PICS_SECC_CMN_Pause	no
Welding detection supported	PICS_SECC_DC_WeldingDetection	n/a (DC-only)
ISO 15118-2 supported	PICS_SECC_CMN_ISO15118_2	yes
ISO 15118-20 supported	PICS_SECC_CMN_ISO15118_20	yes
DIN SPEC 70121 supported (DC)	PICS_SECC_DC_DIN70121	n/a (DC-only)
DC energy transfer mode(s) advertised	PIXIT_SECC_DC_SupportedEnergyTransferMode	n/a (DC-only)
CableCheck answers Ongoing	PIXIT_SECC_DC_CableCheckOngoing == ongoing	n/a (DC-only)
Authorization answers Ongoing	PIXIT_SECC_CMN_AuthorizationOngoing == ongoing	no
ChargeParameterDiscovery answers Ongoing	PIXIT_SECC_CMN_ChargeParameterDiscoveryOngoing == ongoing	no
CM_VALIDATE (BCB-toggle validation)	PIXIT_SECC_CMN_CmValidate == cmValidate	no
Architecture makes validation unnecessary	PIXIT_SECC_CMN_ArchitectureValidationNotRequired	no
CM_AMP_MAP supported	PIXIT_CMN_CMN_CmAmpMap	no
SECC initiates CM_AMP_MAP	PICS_CMN_CMN_InitiateCmAmpMap	no

Capability	PICS/PIXIT	Declared
Self-initiated wake-up from pause	PIXIT_CMN_CMN_WakeUp < PICS_CMN_CMN_WakeUp	no
AC connection-loss handling	PIXIT_SECC_AC_ConnectionLossHandling	optionA
AC CP duty cycle after plug-in	PIXIT_SECC_AC_InitialDutyCycle	dc5
IEC 61851-1 basic charging (AC)	PIXIT_SECC_IEC61851_1_BasicCharging	yes
Identification modes supported	PICS_CMN_CMN_IdentificationMode	ExternalPayment
Certificate services used	PIXIT_EVCC_CMN_CertificateHandling	none
Renegotiation supported	PICS_CMN_CMN_Renegotiation	no
Pause / resume (sleep mode) supported	PIXIT_EVCC_CMN_Pause	no
Optimises the charging profile against sales tariffs	PIXIT_EVCC_CMN_ChargingProfileOptimization	unknown
States MaxNumberOfPhasesInUse (AC)	PIXIT_EVCC_AC_MaxNumberOfPhasesInUse	no
Queries value-added services (ServiceDetail)	PIXIT_EVCC_CMN_VAS	no
Transport security requested	PIXIT_EVCC_CMN_TLS	none_
Welding detection performed (DC)	PIXIT_EVCC_DC_WeldingDetection	weldingDetection
Reaction to a Pmax=0 W schedule	PICS_EVCC_CMN_PmaxSchedulewithZeroPow	noSleep
SLAC validation (CM_VALIDATE / BCB toggle)	PIXIT_EVCC_CMN_CmValidate	unknown
AC connection-loss handling	PIXIT_EVCC_AC_ConnectionLossHandling	optionA
CM_AMP_MAP supported	PIXIT_CMN_CMN_CmAmpMap	no
EV initiates CM_AMP_MAP	PICS_CMN_CMN_InitiateCmAmpMap	no

Declared by the test operator (profile v1); the test-case selection of this run was derived from this declaration, mirroring the ISO 15118-4 ATS control part ([V2G4-018]/[V2G4-019]). Test cases the declaration marks not applicable were deselected by default; any that were explicitly force-run are annotated "declared N/A (operator force-run)" at their result.

Test families & variants

ISO 15118-3 SLAC (-5)	DUT (dut)
ISO 15118-2 message layer (-4)	DUT (dut)

ISO 15118-20 (ISO 15118-21 ATS)	DUT (dut)
PIONIX interop testing (vendor-defined)	DUT (dut)

Test Environment

Test suite version	-
Test suite git SHA	-
Test suite branch	-
Mode	HW (CHARGEBRIDGE, BLACK-BOX DUT)
Host	CI runner
Kernel	6.8.0-86-generic
PLC taps (EVSE / EV)	- / cb_plc_ev
MQTT broker	/tmp/everest-conformance-mqtt.sock:1883
EVerest prefix	-
Pause between TCs	3 s
EV BSP module id	ev_bsp

Totals

ISO 15118-3 SLAC (-5)

DUT (dut)
2 pass
4 fail
0 not run
1 inconclusive

ISO 15118-2 message layer (-4)

DUT (dut)
28 pass
1 fail
0 not run
0 inconclusive

ISO 15118-20 (ISO 15118-21 ATS)

DUT (dut)
117 pass
15 fail
0 not run
0 inconclusive

PIONIX interop testing (vendor-defined)**DUT** (dut)**2** pass**0** fail**0** not run**0** inconclusive

Verdict semantics: expected failures (author-flagged known deviations / non-deterministic cases) are reported as

FAIL EXPECTED — genuine reds that are not hidden and must be explicitly accepted by the operator. A FAIL (or FAIL EXPECTED) accepted by the operator is reported as **ACCEPTED FAIL** with the mandatory justification and does not count against the overall verdict. Overall verdict is PASS only if no test case FAILs (or is left FAIL EXPECTED without acceptance) on any variant.

Summary matrix — ISO 15118-3 SLAC (-5)

Test case	DUT (dut)	
	Verdict	Duration
CmSlacParm		
TC_SECC_AC_VTB_CmSlacParm_001	FAIL	17.19 s
TC_SECC_AC_VTB_CmSlacParm_002	FAIL	150.43 s
TC_SECC_AC_VTB_CmSlacParm_004	PASS	5.45 s
PLCLinkStatus		
TC_SECC_AC_VTB_PLCLinkStatus_001	FAIL	8.31 s
TC_SECC_AC_VTB_PLCLinkStatus_005	FAIL	17.90 s
TC_SECC_AC_VTB_PLCLinkStatus_006	INCONCLUSIVE precondition not established	7.23 s
TC_SECC_AC_VTB_PLCLinkStatus_008	PASS	14.44 s

Summary matrix — ISO 15118-2 message layer (-4)

Test case	DUT (dut)	
	Verdict	Duration
SupportedAppProtocol		
TC_SECC_AC_VTB_SupportedAppProtocol_001	PASS	6.71 s
ChargeParameterDiscovery		
TC_SECC_AC_VTB_ChargeParameterDiscovery_001	PASS	7.18 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_003	PASS	7.00 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_004	PASS	7.00 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_005	FAIL	7.60 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_006	PASS	7.40 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_012	PASS	7.00 s
TC_SECC_AC_VTB_ChargeParameterDiscovery_016	PASS	7.00 s
PowerDelivery		
TC_SECC_AC_VTB_PowerDelivery_001	PASS	7.80 s
TC_SECC_AC_VTB_PowerDelivery_005	PASS	9.80 s
TC_SECC_AC_VTB_PowerDelivery_006	PASS	7.60 s
TC_SECC_AC_VTB_PowerDelivery_007	PASS	8.60 s
TC_SECC_AC_VTB_PowerDelivery_008	PASS	7.80 s
TC_SECC_AC_VTB_PowerDelivery_009	PASS	9.20 s
TC_SECC_AC_VTB_PowerDelivery_010	PASS	7.80 s
TC_SECC_AC_VTB_PowerDelivery_011	PASS	8.00 s
TC_SECC_AC_VTB_PowerDelivery_012	PASS	50.07 s
TC_SECC_AC_VTB_PowerDelivery_013	PASS	72.82 s
TC_SECC_AC_VTB_PowerDelivery_014	PASS	7.21 s
ChargingStatus		
TC_SECC_AC_VTB_ChargingStatus_001	PASS	8.20 s
TC_SECC_AC_VTB_ChargingStatus_003	PASS	8.00 s
TC_SECC_AC_VTB_ChargingStatus_004	PASS	8.00 s
TC_SECC_AC_VTB_ChargingStatus_005	PASS	71.89 s
TC_SECC_AC_VTB_ChargingStatus_006	PASS	8.11 s
TC_SECC_AC_VTB_ChargingStatus_008	PASS	8.80 s

Test case	DUT (dut)	
	Verdict	Duration
SessionStop		
TC_SECC_AC_VTB_SessionStop_001	PASS	9.57 s
TC_SECC_AC_VTB_SessionStop_002	PASS	8.93 s
TC_SECC_AC_VTB_SessionStop_003	PASS	9.00 s
TC_SECC_AC_VTB_SessionStop_004	PASS	72.69 s

Summary matrix — ISO 15118-20 (ISO 15118-21 ATS)

Test case	DUT (dut)	
	Verdict	Duration
SDP		
TC21_SECC_SDP_001	PASS	5.60 s
TC21_SECC_SDP_002	PASS	6.00 s
TC21_SECC_SDP_003	PASS	18.61 s
TC21_SECC_SDP_004	PASS	18.00 s
V2GTPSDP		
TC21_SECC_V2GTPSDP_001	PASS	5.97 s
TC21_SECC_V2GTPSDP_002	PASS	18.61 s
TC21_SECC_V2GTPSDP_003	PASS	18.00 s
TC21_SECC_V2GTPSDP_004	PASS	18.20 s
TC21_SECC_V2GTPSDP_005	PASS	18.80 s
TC21_SECC_V2GTPSDP_006	PASS	18.00 s
TC21_SECC_V2GTPSDP_007	PASS	18.20 s
V2GTPSupportedAppProtocol		
TC21_SECC_V2GTPSupportedAppProtocol_001	PASS	6.38 s
TC21_SECC_V2GTPSupportedAppProtocol_002	PASS	6.00 s
TC21_SECC_V2GTPSupportedAppProtocol_003	PASS	22.83 s
TC21_SECC_V2GTPSupportedAppProtocol_004	PASS	23.00 s
TC21_SECC_V2GTPSupportedAppProtocol_005	PASS	23.80 s
TC21_SECC_V2GTPSupportedAppProtocol_006	PASS	23.20 s
TC21_SECC_V2GTPSupportedAppProtocol_007	PASS	23.00 s
TC21_SECC_V2GTPSupportedAppProtocol_008	PASS	23.00 s
V2GTPCommonMessages		
TC21_SECC_V2GTPCommonMessages_001	PASS	6.00 s
TC21_SECC_V2GTPCommonMessages_002	PASS	6.00 s
TC21_SECC_V2GTPCommonMessages_003	PASS	22.82 s
TC21_SECC_V2GTPCommonMessages_004	PASS	23.00 s
TC21_SECC_V2GTPCommonMessages_005	PASS	23.00 s
TC21_SECC_V2GTPCommonMessages_006	PASS	23.00 s

Test case	DUT (dut)	
	Verdict	Duration
TC21_SECC_V2GTPCommonMessages_007	FAIL	10.78 s
TC21_SECC_V2GTPCommonMessages_008	PASS	23.22 s
SupportedAppProtocol		
TC21_SECC_SupportedAppProtocol_001	PASS	6.40 s
TC21_SECC_SupportedAppProtocol_002	PASS	6.60 s
TC21_SECC_SupportedAppProtocol_003	PASS	6.40 s
TC21_SECC_SupportedAppProtocol_004	FAIL	6.00 s
SessionSetup		
TC21_SECC_SessionSetup_002	PASS	6.00 s
TC21_SECC_SessionSetup_003	PASS	23.83 s
TC21_SECC_SessionSetup_004	PASS	6.17 s
TC21_SECC_SessionSetup_005	PASS	6.60 s
AuthorizationSetup		
TC21_SECC_AuthorizationSetup_001	PASS	6.00 s
TC21_SECC_AuthorizationSetup_002	PASS	6.00 s
TC21_SECC_AuthorizationSetup_003	PASS	6.00 s
TC21_SECC_AuthorizationSetup_004	PASS	69.89 s
TC21_SECC_AuthorizationSetup_005	PASS	6.12 s
CertificateInstallation		
TC21_SECC_CertificateInstallation_001	PASS	6.60 s
TC21_SECC_CertificateInstallation_002	PASS	7.80 s
TC21_SECC_CertificateInstallation_003	PASS	7.20 s
TC21_SECC_CertificateInstallation_004	PASS	7.00 s
TC21_SECC_CertificateInstallation_005	PASS	7.00 s
TC21_SECC_CertificateInstallation_006	PASS	6.40 s
TC21_SECC_CertificateInstallation_007	PASS	6.00 s
TC21_SECC_CertificateInstallation_008	PASS	6.40 s
TC21_SECC_CertificateInstallation_009	PASS	6.60 s
TC21_SECC_CertificateInstallation_010	PASS	6.00 s
TC21_SECC_CertificateInstallation_011	PASS	6.00 s

Test case	DUT (dut)	
	Verdict	Duration
TC21_SECC_CertificateInstallation_012	PASS	6.00 s
TC21_SECC_CertificateInstallation_013	PASS	6.00 s
TC21_SECC_CertificateInstallation_014	PASS	6.00 s
TC21_SECC_CertificateInstallation_015	PASS	6.00 s
TC21_SECC_CertificateInstallation_016	PASS	6.40 s
TC21_SECC_CertificateInstallation_017	PASS	7.00 s
TC21_SECC_CertificateInstallation_018	PASS	6.60 s
TC21_SECC_CertificateInstallation_019	PASS	6.00 s
TC21_SECC_CertificateInstallation_020	PASS	6.00 s
TC21_SECC_CertificateInstallation_021	PASS	6.00 s
Authorization		
TC21_SECC_Authorization_001	PASS	6.62 s
TC21_SECC_Authorization_003	PASS	7.00 s
TC21_SECC_Authorization_004	PASS	6.40 s
TC21_SECC_Authorization_005	PASS	6.00 s
TC21_SECC_Authorization_006	PASS	6.00 s
TC21_SECC_Authorization_007	PASS	6.00 s
TC21_SECC_Authorization_008	PASS	5.99 s
TC21_SECC_Authorization_009	PASS	6.00 s
TC21_SECC_Authorization_010	PASS	6.00 s
TC21_SECC_Authorization_011	PASS	6.00 s
TC21_SECC_Authorization_012	PASS	6.00 s
TC21_SECC_Authorization_013	PASS	6.00 s
TC21_SECC_Authorization_014	PASS	6.00 s
TC21_SECC_Authorization_015	PASS	6.00 s
TC21_SECC_Authorization_016	PASS	6.00 s
TC21_SECC_Authorization_017	PASS	6.00 s
TC21_SECC_Authorization_018	PASS	6.00 s
TC21_SECC_Authorization_021	PASS	6.00 s
TC21_SECC_Authorization_023	PASS	6.60 s

Test case	DUT (dut)	
	Verdict	Duration
TC21_SECC_Authorization_024	PASS	6.40 s
CertificateInstallationOrAuthorization		
TC21_SECC_CertificateInstallationOrAuthorization_001	PASS	6.00 s
TC21_SECC_CertificateInstallationOrAuthorization_002	PASS	70.48 s
ServiceDiscovery		
TC21_SECC_ServiceDiscovery_001	PASS	6.80 s
TC21_SECC_ServiceDiscovery_002	PASS	7.00 s
TC21_SECC_ServiceDiscovery_003	PASS	7.00 s
TC21_SECC_ServiceDiscovery_004	FAIL	16.41 s
TC21_SECC_ServiceDiscovery_005	PASS	6.59 s
ServiceDetail		
TC21_SECC_ServiceDetail_001	PASS	6.58 s
TC21_SECC_ServiceDetail_002	PASS	7.00 s
TC21_SECC_ServiceDetail_003	PASS	7.00 s
TC21_SECC_ServiceDetail_004	PASS	7.00 s
TC21_SECC_ServiceDetail_005	FAIL	16.21 s
TC21_SECC_ServiceDetail_006	PASS	6.78 s
ServiceSelection		
TC21_SECC_ServiceSelection_001	PASS	7.20 s
TC21_SECC_ServiceSelection_002	PASS	7.61 s
TC21_SECC_ServiceSelection_003	PASS	7.39 s
TC21_SECC_ServiceSelection_004	FAIL	7.00 s
TC21_SECC_ServiceSelection_006	FAIL	16.21 s
TC21_SECC_ServiceSelection_007	PASS	6.79 s
ChargeParameterDiscovery		
TC21_SECC_ChargeParameterDiscovery_001	PASS	7.51 s
TC21_SECC_ChargeParameterDiscovery_002	PASS	7.00 s
TC21_SECC_ChargeParameterDiscovery_003	FAIL	16.41 s
TC21_SECC_ChargeParameterDiscovery_004	PASS	7.59 s
ScheduleExchange		

Test case	DUT (dut)	
	Verdict	Duration
TC21_SECC_ScheduleExchange_002	PASS	8.00 s
TC21_SECC_ScheduleExchange_003	PASS	8.00 s
TC21_SECC_ScheduleExchange_004	PASS	7.60 s
TC21_SECC_ScheduleExchange_005	FAIL	16.01 s
TC21_SECC_ScheduleExchange_006	PASS	6.99 s
TC21_SECC_ScheduleExchange_008	PASS	7.00 s
PowerDelivery		
TC21_SECC_PowerDelivery_001	PASS	7.40 s
TC21_SECC_PowerDelivery_002	PASS	8.80 s
TC21_SECC_PowerDelivery_003	PASS	7.10 s
TC21_SECC_PowerDelivery_004	PASS	8.10 s
TC21_SECC_PowerDelivery_005	PASS	7.80 s
TC21_SECC_PowerDelivery_006	PASS	7.80 s
TC21_SECC_PowerDelivery_007	FAIL	7.20 s
TC21_SECC_PowerDelivery_008	FAIL	7.10 s
TC21_SECC_PowerDelivery_009	FAIL	15.90 s
TC21_SECC_PowerDelivery_010	PASS	72.29 s
TC21_SECC_PowerDelivery_011	FAIL	7.70 s
TC21_SECC_PowerDelivery_012	FAIL	7.10 s
TC21_SECC_PowerDelivery_013	FAIL	7.10 s
ChargeLoop		
TC21_SECC_ChargeLoop_001	PASS	7.72 s
TC21_SECC_ChargeLoop_002	PASS	71.28 s
SessionStop		
TC21_SECC_SessionStop_001	PASS	9.00 s
TC21_SECC_SessionStop_002	PASS	9.00 s
TC21_SECC_SessionStop_003	PASS	9.00 s
TC21_SECC_SessionStop_004	PASS	72.89 s
TC21_SECC_SessionStop_005	PASS	9.21 s
TC21_SECC_SessionStop_006	PASS	8.90 s

Test case	DUT (dut)	
	Verdict	Duration
TC21_SECC_SessionStop_007	FAIL	9.00 s

Summary matrix — PIONIX interop testing (vendor-defined)

Test case	DUT (dut)	
	Verdict	Duration
PionixInterop		
TC_SECC_AC_VTB_PionixInterop_005	PASS	11.20 s
TC_SECC_AC_VTB_PionixInterop_006	PASS	608.65 s

Test case details — ISO 15118-3 SLAC (-5)

TC_SECC_AC_VTB_CmSlacParm_001

TC_SECC_AC_VTB_CmSlacParm_001.

Test objective: Test System executes GoodCase procedure, indicates the initial CP State B, waits for 5 % duty cycle and executes successful EIM process. Test System then checks that a nominal duty cycle can be detected after SUT changes CP State to E or F for T_step_EF. Furthermore a successful SLAC matching process shall be performed afterwards.

DUT (dut) FAIL 17.19 s

FAILURE REASON

tests/test_secc_ac_cm_slac_parm.py:132

TimeoutError: CP E/F (duty 0) step not observed before the window closed (last duty=100.0)

Measurement	Measured	Target / range	Result
initial CP duty cycle (dc5)	5.0 %	5 ± 1.5 %	✓

Failure detail (excerpt):

E TimeoutError: CP E/F (duty 0) step not observed before the window closed (last duty=100.0)

TC_SECC_AC_VTB_CmSlacParm_002

TC_SECC_AC_VTB_CmSlacParm_002.

Test objective: Test System executes GoodCase procedure, indicates the initial CP State B transition and waits for 5 % duty cycle fallback if the TT_EVSE_SLAC_init timer has expired and no CM_SLAC_PARM.REQ messages was sent before. Test System then counts the number of fallback sequences. Test System then checks that a 5 % duty cycle can be detected after SUT changes CP State to E or F for T_step_EF and whether this sequence is limited to 2 retries by the SUT. When the repetition limit is reached, the Test System checks if the SUT is initiating an oscillator shutdown.

DUT (dut) **FAIL** 150.43 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT goes to X1 (oscillator shutdown, duty 100%) after 2 fallback retries with no residual 5% oscillation ([V2G3-M06-07]) – final duty 5.0 with 1 5%-duty period(s) after the window opened

Conformance check	Observed	Result
CP E/F step ends within T_step_EF max (8.0s) [T_step_EF (5% fallback #1)]		✓
CP E/F step within T_step_EF [4.0, 8.0]s [T_step_EF (5% fallback #1)]	E/F step 4.010s	✓
5%-fallback #1 E/F not before TT_EVSE_SLAC_init min (20s) after CP State B ([V2G3-A09-11]/[V2G3-M06-07])	E/F 40.06s after CP State B	✓
CP E/F step ends within T_step_EF max (8.0s) [T_step_EF (5% fallback #2)]		✓
CP E/F step within T_step_EF [4.0, 8.0]s [T_step_EF (5% fallback #2)]	E/F step 4.009s	✓
5%-fallback #2 E/F not before TT_EVSE_SLAC_init min (20s) after the E/F end (CP State B) ([V2G3-A09-11]/[V2G3-M06-07])	E/F 40.55s after the E/F end (CP State B)	✓
5% duty held across the full TT_EVSE_SLAC_init window (20s) after the last fallback retry ([V2G3-M06-07])	5% duty left after 40.55s	✓
SUT goes to X1 (oscillator shutdown, duty 100%) after 2 fallback retries with no residual 5% oscillation ([V2G3-M06-07])	final duty 5.0 with 1 5%-duty period(s) after the window opened	✗

Measurement	Measured	Target / range	Result
initial CP duty cycle (dc5)	5.0 %	5 ± 1.5 %	✓
T_step_EF (5% fallback #1)	4010.4 ms	-	info
5%-fallback #1 E/F after CP State B (TT_EVSE_SLAC_init)	40.06 s	[20.0, 50.0] s	✓
5% duty resume after fallback #1 E/F end	0.797 s	≤ 8.0 s	✓

Measurement	Measured	Target / range	Result
T_step_EF (5% fallback #2)	4008.9 ms	-	info
5%-fallback #2 E/F after the E/F end (CP State B) (TT_EVSE_SLAC_init)	40.55 s	[20.0, 50.0] s	✓
5% duty resume after fallback #2 E/F end	0.798 s	≤ 8.0 s	✓
final CP duty after 2 fallback retries (oscillator shutdown = X1)	5.0 %	100 ± 1.5 %	✗

Failure detail (excerpt):

E AssertionError: SUT goes to X1 (oscillator shutdown, duty 100%) after 2 fallback retries with no residual 5% oscillation ([V2G3-M06-07]) – final duty 5.0 with 1 5%-duty period(s) after the window opened

TC_SECC_AC_VTB_CmSlacParm_004

TC_SECC_AC_VTB_CmSlacParm_004.

Test objective: Test System executes successful EIM process before plug-in, the GoodCase procedure and indicates the initial CP State B. Test System then checks that a nominal duty cycle can be detected. Furthermore a successful SLAC matching process shall be performed afterwards.

DUT (dut) **PASS** 5.45 s

Conformance check	Observed	Result
nominal duty confirmed within par_T_conn_max_comm (8.0s) of CP State B	confirmed 0.507s after CP State B	✓
no transient 5% HLC duty between plug-in and the nominal duty (EIM beforePlugin)	0 transient 5% HLC duty period(s)	✓

Measurement	Measured	Target / range	Result
nominal duty after plug-in (par_T_conn_max_comm, EIM beforePlugin)	506.7 ms	-	info
nominal CP duty cycle (EIM beforePlugin)	26.7 %	[10.0, 96.0] %	✓
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC_SECC_AC_VTB_PLCLinkStatus_001

TC_SECC_AC_VTB_PLCLinkStatus_001.

Test objective: Test System executes GoodCase procedure, initiates an EIM authorization during the SLAC process, indicates the key at the local PLC node and then checks that the data link connection is established within 'TT_match_join'. Test System then checks if the SUT has changed from 5 % initial duty cycle to a nominal duty cycle during the matching process by detecting X2(5 %) to X1(100 %) to X2(nominal) transition after successful EIM process during the matching process.

DUT (dut)

FAIL

8.31 s

FAILURE REASON

tests/test_secc_ac_plc_link_status.py:216

TimeoutError: no matching CP duty period within 3.829933802000596s (periods: [(100.0, 83600.839), (5.0, 83601.347)])

Measurement	Measured	Target / range	Result
initial CP duty cycle (dc5)	5.0 %	5 ± 1.5 %	✓
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Failure detail (excerpt):

E TimeoutError: no matching CP duty period within 3.829933802000596s (periods: [(100.0, 83600.839), (5.0, 83601.347)])

TC_SECC_AC_VTB_PLCLinkStatus_005

TC_SECC_AC_VTB_PLCLinkStatus_005.

Test objective: Test System executes GoodCase procedure (5 % duty cycle), indicates the key at the local PLC node and then checks that the data link connection is established within 'TT_match_join'. Afterwards Test System initiates a connection loss by setting a new key at the local node. Test System then checks that the SUT performs a CP State X2 to X1 to E/F transition. Furthermore Test System checks that the SUT applies CP State E or F for T_step_EF and will switch to CP State X1 or X2 afterwards.

DUT (dut) **FAIL** 17.90 s

FAILURE REASON

tests/test_secc_ac_plc_link_status.py:216

TimeoutError: no matching CP duty period within 8.0s (periods: [(0.0, 83611.446), (100.0, 83615.455), (5.0, 83616.253)])

Conformance check	Observed	Result
SUT terminates the PLC link within TP_match_leave (1.25s) on connection loss (AC dc5)	left after 0.000s	✓
SUT performs the X1 (100%) step within par_T_conn_max_comm (8.0s) after connection loss (AC dc5)	X1 step 4.303s after loss	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CM_SET_KEY.CNF response time	0.3 ms	-	info
left logical network on connection loss (AC dc5)	0.0 s	≤ 1.25 s	✓
X1 (100%) step after connection loss (AC dc5)	4.303 s	≤ 8.0 s	✓

Failure detail (excerpt):

E TimeoutError: no matching CP duty period within 8.0s (periods: [(0.0, 83611.446), (100.0, 83615.455), (5.0, 83616.253)])

TC_SECC_AC_VTB_PLCLinkStatus_006

TC_SECC_AC_VTB_PLCLinkStatus_006.

Test objective: Test System executes GoodCase procedure (Nominal duty cycle), indicates the key at the local PLC node and then checks that the data link connection is established within 'TT_match_join'. Afterwards Test System initiates a connection loss by setting a new key at the local node. Test System then checks that the SUT performs a CP State X2 to X1 to E/F transition. Furthermore Test System checks that the SUT applies CP State E or F for T_step_EF and will switch to CP State X1 or X2 afterwards (Option A).

DUT (dut) **INCONCLUSIVE** precondition not established 7.23 s

FAILURE REASON

harness/test_ev.py:1034

`harness.verdict.PreconditionInconclusive: INCONCLUSIVE (StateB + nominal duty after afterPlugin EIM): nominal CP PWM duty in [10.0,96.0]% not observed within 3.25s (last=5.0)`

Failure detail (excerpt):

E TimeoutError: nominal CP PWM duty in [10.0,96.0]% not observed within 3.25s (last=5.0)

The above exception was the direct cause of the following exception:

E `harness.verdict.PreconditionInconclusive: INCONCLUSIVE (StateB + nominal duty after afterPlugin EIM): nominal CP PWM duty in [10.0,96.0]% not observed within 3.25s (last=5.0)`

TC_SECC_AC_VTB_PLCLinkStatus_008

TC_SECC_AC_VTB_PLCLinkStatus_008.

Test objective: Test System executes GoodCase procedure and initiates a terminated V2G communication session by sending a SessionStopReq message with the current SessionID, ChargingSession 'Terminate' and all additional mandatory parameters and waits for a SessionStopRes message with the current SessionID and all additional mandatory parameters. Furthermore Test System checks if the SUT terminates the TCP connection after. Test System then checks that the SUT leaves the logical network after 'TP_match_leave' by using the CM_NW_STATS message sequence.

DUT (dut) **PASS** 14.44 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends SessionStopRes(OK) on Terminate	got 'SessionStopRes'/'OK'	✓
SessionStopRes SessionID = current session id	got 'fb559f5611058301' vs 'fb559f5611058301'	✓
SUT sends no SLAC frame during par_TP_match_leave (leaving the network)	silent for 1s	✓
SUT has left the current logical network (CM_NW_STATS empty)	no stations	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
supportedAppProtocolRes response time	100.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.5 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.2 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
SessionStopRes response time	101.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	3999.6 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓
SUT node absent from tester-node AVLN after Terminate (CM_NW_STATS after TP_match_leave)	0 stations	= 0 stations	✓

Test case details — ISO 15118-2 message layer (-4)

TC_SECC_AC_VTB_SupportedAppProtocol_001

TC_SECC_AC_VTB_SupportedAppProtocol_001.

Test objective: GoodCase (eIM / no-TLS) against the AC SUT; Test System sends a valid SupportedAppProtocolReq including the ISO namespace urn:iso:15118:2:2013:MsgDef and all mandatory parameters, and checks the SUT replies SupportedAppProtocolRes with ResponseCode OK_SuccessfulNegotiation or OK_SuccessfulNegotiationWithMinorDeviation and a valid SchemaID. Primary happy-path handshake TC for the AC/eIM/TLS-off SUT.

DUT (dut) **PASS** 6.71 s

Conformance check	Observed	Result
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓
ResponseCode is an OK_* negotiation code	got 'OK_SuccessfulNegotiation'	✓
supportedAppProtocolRes carries the negotiated SchemaID	got 1	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
Negotiated SchemaID	1	-	info

TC_SECC_AC_VTB_ChargeParameterDiscovery_001

TC_SECC_AC_VTB_ChargeParameterDiscovery_001.

Test objective: GoodCase; the Test System sends a ChargeParameterDiscoveryReq with the current SessionID, a valid RequestedEnergyTransferType (AC) and a valid AC_EVChargeParameter, without MaxEntriesSAScheduleTuple and DepartureTime. Checks the SUT replies ChargeParameterDiscoveryRes with the current SessionID, ResponseCode OK, EVSEProcessing Finished and a valid scheduleList (looping while Ongoing). Primary happy-path AC CPD TC.

DUT (dut) **PASS** 7.18 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargeParameterDiscoveryRes message	got 'ChargeParameterDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓
ChargeParameterDiscoveryRes(Finished) carries a SAScheduleList	SAScheduleList=[{'PMaxScheduleEntry': [{'PMax': {'multiplier': 1, 'unit': 'W', 'value': 1104}, 'duration': 86400, 'start': 0}], 'SAScheduleTupleID': 1}]	✓
ChargeParameterDiscoveryRes carries an AC_EVSEChargeParameter	got {'AC_EVSEStatus': {'EVSENotification': 'None', 'NotificationMaxDelay': 0, 'RCD': False}, 'EVSEMaxCurrent': {'multiplier': -2, 'unit': 'A', 'value': 1600}, 'EVSENominalVoltage': {'multiplier': -1, 'unit': 'V', 'value': 2300}}	✓
AC_EVSEChargeParameter carries an AC_EVSEStatus	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
AC_EVSEChargeParameter carries an EVSENominalVoltage	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
EVSENominalVoltage ~230 V (ac_nominal_voltage)	got 230.0 V	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
AC EVSENominalVoltage	230.0 V	230 ± 1.0 V	✓
AC EVSEMaxCurrent	16.0 A	-	info

TC_SECC_AC_VTB_ChargeParameterDiscovery_003

TC_SECC_AC_VTB_ChargeParameterDiscovery_003.

Test objective: GoodCase; the Test System sends a ChargeParameterDiscoveryReq with an invalid SessionID and a valid RequestedEnergyTransferType. Checks the SUT replies ChargeParameterDiscoveryRes with a valid SessionID, FAILED_UnknownSession, then closes TCP within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_UnknownSession	got FAILED_UnknownSession (name=ChargeParameterDiscoveryRes)	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.4 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ChargeParameterDiscoveryRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_ChargeParameterDiscovery_004

TC_SECC_AC_VTB_ChargeParameterDiscovery_004.

Test objective: GoodCase; the Test System sends a ChargeParameterDiscoveryReq with an invalid RequestedEnergyTransferType 'DC_extended' (a DC mode the AC SUT does not offer). Checks the SUT replies ChargeParameterDiscoveryRes with FAILED_WrongEnergyTransferMode, then closes TCP within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_WrongEnergyTransferMode	got FAILED_WrongEnergyTransferMode (name=ChargeParameterDiscoveryRes)	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	100.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ChargeParameterDiscoveryRes response time	101.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_ChargeParameterDiscovery_005

TC_SECC_AC_VTB_ChargeParameterDiscovery_005.

Test objective: GoodCase; the Test System sends a ChargeParameterDiscoveryReq with a valid RequestedEnergyTransferType but an invalid AC_EVChargeParameter (EVMaxCurrent -100). Checks the SUT replies ChargeParameterDiscoveryRes with FAILED_WrongChargeParameter, then closes TCP within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **FAIL** 7.60 s

FAILURE REASON

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_WrongChargeParameter – SUT accepted a negative EVMaxCurrent with OK instead of FAILED_WrongChargeParameter (no AC charge-parameter range validation; same class as the DC charge-parameter finding).

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_WrongChargeParameter	SUT accepted a negative EVMaxCurrent with OK instead of FAILED_WrongChargeParameter (no AC charge-parameter range validation; same class as the DC charge-parameter finding).	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
ChargeParameterDiscoveryRes response time	101.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

E `AssertionError: ResponseCode = FAILED_WrongChargeParameter – SUT accepted a negative EVMaxCurrent with OK instead of FAILED_WrongChargeParameter (no AC charge-parameter range validation; same class as the DC charge-parameter finding).`

TC_SECC_AC_VTB_ChargeParameterDiscovery_006

TC_SECC_AC_VTB_ChargeParameterDiscovery_006.

Test objective: GoodCase; CPDReq valid AC mode, without MaxEntries, WITH
DepartureTime, salesTariff expected → OK, Finished, valid scheduleList.
(salesTariff N/A on this free-service SUT.)

DUT (dut) **PASS** 7.40 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargeParameterDiscoveryRes message	got 'ChargeParameterDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓
ChargeParameterDiscoveryRes(Finished) carries a SAScheduleList	SAScheduleList=[{'PMaxScheduleEntry': [{'PMax': {'multiplier': 1, 'unit': 'W', 'value': 1104}, 'duration': 7200, 'start': 0}], 'SAScheduleTupleID': 1}]	✓
ChargeParameterDiscoveryRes carries an AC_EVSEChargeParameter	got {'AC_EVSEStatus': {'EVSENotification': 'None', 'NotificationMaxDelay': 0, 'RCD': False}, 'EVSEMaxCurrent': {'multiplier': -2, 'unit': 'A', 'value': 1600}, 'EVSENominalVoltage': {'multiplier': -1, 'unit': 'V', 'value': 2300}}	✓
AC_EVSEChargeParameter carries an AC_EVSEStatus	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
AC_EVSEChargeParameter carries an EVSENominalVoltage	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
EVSENominalVoltage ~230 V (ac_nominal_voltage)	got 230.0 V	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
AC EVSENominalVoltage	230.0 V	230 ± 1.0 V	✓
AC EVSEMaxCurrent	16.0 A	-	info

TC_SECC_AC_VTB_ChargeParameterDiscovery_012

TC_SECC_AC_VTB_ChargeParameterDiscovery_012.

Test objective: GoodCase; CPDReq valid AC mode, WITH MaxEntriesSAScheduleTuple, without DepartureTime → OK, Finished, valid scheduleList (MaxEntries considered).

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargeParameterDiscoveryRes message	got 'ChargeParameterDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓
ChargeParameterDiscoveryRes(Finished) carries a SAScheduleList	SAScheduleList=[{'PMaxScheduleEntry': [{'PMax': {'multiplier': 1, 'unit': 'W', 'value': 1104}, 'duration': 86400, 'start': 0}], 'SAScheduleTupleID': 1}]	✓
SAScheduleList honours MaxEntriesSAScheduleTuple (<= 3)	got 1 tuple(s)	✓
ChargeParameterDiscoveryRes carries an AC_EVSEChargeParameter	got {'AC_EVSEStatus': {'EVSENotification': 'None', 'NotificationMaxDelay': 0, 'RCD': False}, 'EVSEMaxCurrent': {'multiplier': -2, 'unit': 'A', 'value': 1600}, 'EVSENominalVoltage': {'multiplier': -1, 'unit': 'V', 'value': 2300}}	✓
AC_EVSEChargeParameter carries an AC_EVSEStatus	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
AC_EVSEChargeParameter carries an EVSENominalVoltage	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
EVSENominalVoltage ~230 V (ac_nominal_voltage)	got 230.0 V	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
AC EVSENominalVoltage	230.0 V	230 ± 1.0 V	✓
AC EVSEMaxCurrent	16.0 A	-	info

TC_SECC_AC_VTB_ChargeParameterDiscovery_016

TC_SECC_AC_VTB_ChargeParameterDiscovery_016.

Test objective: GoodCase; CPDReq valid AC mode, WITH MaxEntries and DepartureTime → OK, Finished, valid scheduleList (MaxEntries considered).

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargeParameterDiscoveryRes message	got 'ChargeParameterDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓
ChargeParameterDiscoveryRes(Finished) carries a SAScheduleList	SAScheduleList=[{'PMaxScheduleEntry': [{'PMax': {'multiplier': 1, 'unit': 'W', 'value': 1104}, 'duration': 7200, 'start': 0}], 'SAScheduleTupleID': 1}]	✓
SAScheduleList honours MaxEntriesSAScheduleTuple (<= 3)	got 1 tuple(s)	✓
ChargeParameterDiscoveryRes carries an AC_EVSEChargeParameter	got {'AC_EVSEStatus': {'EVSENotification': 'None', 'NotificationMaxDelay': 0, 'RCD': False}, 'EVSEMaxCurrent': {'multiplier': -2, 'unit': 'A', 'value': 1600}, 'EVSENominalVoltage': {'multiplier': -1, 'unit': 'V', 'value': 2300}}	✓
AC_EVSEChargeParameter carries an AC_EVSEStatus	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
AC_EVSEChargeParameter carries an EVSENominalVoltage	keys=['AC_EVSEStatus', 'EVSEMaxCurrent', 'EVSENominalVoltage']	✓
EVSENominalVoltage ~230 V (ac_nominal_voltage)	got 230.0 V	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
AC EVSENominalVoltage	230.0 V	230 ± 1.0 V	✓
AC EVSEMaxCurrent	16.0 A	-	info

TC_SECC_AC_VTB_PowerDelivery_001

TC_SECC_AC_VTB_PowerDelivery_001.

Test objective: GoodCase; PowerDeliveryReq (current SessionID, ChargeProgress=Start, valid charging profile and TupleID), signalling CP State C. Checks the SUT replies PowerDeliveryRes with the current SessionID, ResponseCode OK. Primary happy-path AC PowerDelivery TC (Start).

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = OK	got 'OK' (0.0s)	✓
Response echoes the current SessionID		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.6 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_PowerDelivery_005

TC_SECC_AC_VTB_PowerDelivery_005.

Test objective: GoodCase; PowerDeliveryReq (current SessionID, ChargeProgress=Stop); after the valid PowerDeliveryRes it signals CP State B.
Checks PowerDeliveryRes with the current SessionID, ResponseCode OK.

DUT (dut) **PASS** 9.80 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = OK	got 'OK' (0.1s)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	100.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.5 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
PowerDeliveryRes(Stop) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_PowerDelivery_006

TC_SECC_AC_VTB_PowerDelivery_006.

Test objective: GoodCase; the Test System sends a valid ServiceDiscoveryReq instead of a PowerDeliveryReq (ChargeProgress Start context, sequence error). Checks ServiceDiscoveryRes with the current SessionID, FAILED_SequenceError, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 7.60 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError' (name='ServiceDiscoveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_007

TC_SECC_AC_VTB_PowerDelivery_007.

Test objective: as _006 but in the Stop context -- GoodCase through the AC charge loop, then a valid ServiceDiscoveryReq instead of a PowerDeliveryReq (ChargeProgress Stop context) → ServiceDiscoveryRes FAILED_SequenceError + TCP close.

DUT (dut) **PASS** 8.60 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError' (name='ServiceDiscoveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ServiceDiscoveryRes response time	101.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_008

TC_SECC_AC_VTB_PowerDelivery_008.

Test objective: GoodCase; PowerDeliveryReq with an invalid SessionID, ChargeProgress=Start, valid charging profile and TupleID, signalling CP State C or D. Checks PowerDeliveryRes with a valid SessionID, FAILED_UnknownSession, then TCP close.

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession' (name='PowerDeliveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.5 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_009

TC_SECC_AC_VTB_PowerDelivery_009.

Test objective: as _008 but ChargeProgress=Stop -- GoodCase through the AC charge loop, then a PowerDeliveryReq with an invalid SessionID, ChargeProgress=Stop → PowerDeliveryRes FAILED_UnknownSession + TCP close.

DUT (dut) **PASS** 9.20 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession' (name='PowerDeliveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
PowerDeliveryRes(Start) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_010

TC_SECC_AC_VTB_PowerDelivery_010.

Test objective: GoodCase; PowerDeliveryReq (current SessionID, ChargeProgress=Start, invalid ChargingProfile whose ChargingProfileEntryMaxPower exceeds EVSEMaximumPowerLimit, valid TupleID), CP State C or D. Checks PowerDeliveryRes FAILED_ChargingProfileInvalid + TCP close.

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_ChargingProfileInvalid	got 'FAILED_ChargingProfileInvalid' (name='PowerDeliveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_011

TC_SECC_AC_VTB_PowerDelivery_011.

Test objective: GoodCase; PowerDeliveryReq (current SessionID, ChargeProgress=Start, valid ChargingProfile, invalid SAScheduleTupleID), CP State C or D. Checks PowerDeliveryRes FAILED_TariffSelectionInvalid + TCP close.

DUT (dut) **PASS** 8.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_TariffSelectionInvalid	got 'FAILED_TariffSelectionInvalid' (name='PowerDeliveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.4 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_PowerDelivery_012

TC_SECC_AC_VTB_PowerDelivery_012.

Test objective: GoodCase; after a ChargeParameterDiscoveryRes (current SessionID, OK, EVSEProcessing Finished) the Test System stays silent until V2G_Sequence_Timeout expires (sends no PowerDeliveryReq). Checks the SUT terminates the session by closing TCP within par_CMN_TCP_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **PASS** 50.07 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TCP connection after V2G_Sequence_Timeout (within 70s)	closed 42.3s after ChargeParameterDiscoveryRes	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	42344.5 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC_SECC_AC_VTB_PowerDelivery_013

TC_SECC_AC_VTB_PowerDelivery_013.

Test objective: GoodCase; after a valid ChargingStatusRes (or MeteringReceipt) the Test System stays silent until V2G_Sequence_Timeout expires (sends no PowerDeliveryReq). Checks the SUT terminates the session by closing TCP within par_CMN_TCP_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **PASS** 72.82 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TCP connection after V2G_Sequence_Timeout (within 70s)	closed 63.8s after ChargingStatusRes	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	100.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.2 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	63783.7 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC_SECC_AC_VTB_PowerDelivery_014

TC_SECC_AC_VTB_PowerDelivery_014.

Test objective: GoodCase; PowerDeliveryReq (current SessionID, ChargeProgress=Renegotiate) but no PowerDeliveryReq with ChargeProgress=Start was sent before. Checks PowerDeliveryRes with the current SessionID, ResponseCode FAILED, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 7.21 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED	got 'FAILED' (name='PowerDeliveryRes')	✓
SUT closes the TCP connection after the FAILED response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Renegotiate) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_ChargingStatus_001

TC_SECC_AC_VTB_ChargingStatus_001.

Test objective: GoodCase; the Test System sends a ChargingStatusReq with the current SessionID and all mandatory parameters. Checks the SUT sends a ChargingStatusRes with the current SessionID, ResponseCode OK, ReceiptRequired 'false' and all mandatory parameters.

DUT (dut) **PASS** 8.20 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargingStatusRes message	got 'ChargingStatusRes'	✓
ResponseCode = OK	got 'OK' (0.1s)	✓
ChargingStatusRes carries mandatory EVSEID	present	✓
ChargingStatusRes carries mandatory SAScheduleTupleID	present	✓
ChargingStatusRes carries mandatory AC_EVSEStatus	present	✓
AC_EVSEStatus carries EVSENotification and RCD	got ['EVSENotification', 'NotificationMaxDelay', 'RCD']	✓
ReceiptRequired is false (eIM free service)	ReceiptRequired=False	✓
Response echoes the current SessionID		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ChargingStatusRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ChargingStatus EVSEMaxCurrent	16.0 A	-	info
PowerDeliveryRes(Stop) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_ChargingStatus_003

TC_SECC_AC_VTB_ChargingStatus_003.

Test objective: GoodCase; the Test System sends a valid ServiceDiscoveryReq instead of a ChargingStatusReq (sequence error). Checks ServiceDiscoveryRes with the current SessionID, FAILED_SequenceError, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 8.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_SequenceError	got FAILED_SequenceError (name=ServiceDiscoveryRes)	✓
SUT closes the TCP connection within par_CMN_TCP_Connection_Termination_Timeout		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.5 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ServiceDiscoveryRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_ChargingStatus_004

TC_SECC_AC_VTB_ChargingStatus_004.

Test objective: GoodCase; the Test System sends a ChargingStatusReq with an invalid SessionID. Checks the SUT replies ChargingStatusRes with a valid SessionID, FAILED_UnknownSession, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 8.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_UnknownSession	got FAILED_UnknownSession (name=ChargingStatusRes)	✓
SUT closes the TCP connection within par_CMN_TCP_Connection_Termination_Timeout		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ChargingStatusRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_ChargingStatus_005

TC_SECC_AC_VTB_ChargingStatus_005.

Test objective: GoodCase; after a PowerDeliveryRes (current SessionID, ResponseCode OK) the Test System stays silent until V2G_Sequence_Timeout expires (sends no ChargingStatusReq). Checks the SUT terminates the session by closing TCP within par_CMN_TCP_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **PASS** 71.89 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TCP connection after V2G_Sequence_Timeout (within 70s)	closed 64.0s after PowerDeliveryRes	✓
SUT does not close before V2G_Sequence_Timeout expires (>= 55s)	closed after 64.0s	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	64031.3 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC_SECC_AC_VTB_ChargingStatus_006

TC_SECC_AC_VTB_ChargingStatus_006.

Test objective: GoodCase; ChargingStatusReq (current SessionID). Checks ChargingStatusRes OK, ReceiptRequired 'false', a MeterInfo and all mandatory parameters. (MeterInfo is PIXIT-driven; this free-service SUT may omit it -- the reachable OK + mandatory AC_EVSEStatus assertion is checked, MeterInfo presence is N/A.)

DUT (dut) **PASS** 8.11 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargingStatusRes message	got 'ChargingStatusRes'	✓
ResponseCode = OK	got 'OK' (0.1s)	✓
ChargingStatusRes carries mandatory EVSEID	present	✓
ChargingStatusRes carries mandatory SAScheduleTupleID	present	✓
ChargingStatusRes carries mandatory AC_EVSEStatus	present	✓
AC_EVSEStatus carries EVSENotification and RCD	got ['EVSENotification', 'NotificationMaxDelay', 'RCD']	✓
ReceiptRequired is false (eIM free service)	ReceiptRequired=False	✓
Response echoes the current SessionID		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	100.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ChargingStatusRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ChargingStatus EVSEMaxCurrent	16.0 A	-	info
PowerDeliveryRes(Stop) response time	101.5 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_ChargingStatus_008

TC_SECC_AC_VTB_ChargingStatus_008.

Test objective: GoodCase; ChargingStatusReq (current SessionID). Checks ChargingStatusRes OK, ReceiptRequired 'false', a MeterInfo including MeterReading and all mandatory parameters. (MeterInfo/MeterReading are PIXIT-driven; N/A on this free-service SUT -- the reachable OK + AC_EVSEStatus assertion is checked.)

DUT (dut) **PASS** 8.80 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ChargingStatusRes message	got 'ChargingStatusRes'	✓
ResponseCode = OK	got 'OK' (0.1s)	✓
ChargingStatusRes carries mandatory EVSEID	present	✓
ChargingStatusRes carries mandatory SAScheduleTupleID	present	✓
ChargingStatusRes carries mandatory AC_EVSEStatus	present	✓
AC_EVSEStatus carries EVSENotification and RCD	got ['EVSENotification', 'NotificationMaxDelay', 'RCD']	✓
ReceiptRequired is false (eIM free service)	ReceiptRequired=False	✓
Response echoes the current SessionID		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ChargingStatusRes response time	101.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ChargingStatus EVSEMaxCurrent	16.0 A	-	info
PowerDeliveryRes(Stop) response time	101.0 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_SessionStop_001

TC_SECC_AC_VTB_SessionStop_001.

Test objective: GoodCase; after PowerDelivery(Stop) the Test System sends a SessionStopReq with the current SessionID and ChargingSession= Terminate. Checks the SUT replies SessionStopRes with the current SessionID, ResponseCode OK, and, once the Test System has closed its TCP connection, terminates the data link within par_TP_match_leave + par_CMN_Transmission_Delay. Primary happy-path AC SessionStop TC.

DUT (dut) **PASS** 9.57 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK' (0.1s)	✓
SUT terminates the data link within par_TP_match_leave	left the logical network after 0.10s (bound 1.25s)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.4 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.2 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
SessionStopRes response time	101.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC_SECC_AC_VTB_SessionStop_002

TC_SECC_AC_VTB_SessionStop_002.

Test objective: GoodCase; the Test System sends a valid ServiceDiscoveryReq instead of a SessionStopReq (sequence error). Checks ServiceDiscoveryRes with the current SessionID, FAILED_SequenceError, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 8.93 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError' (name='ServiceDiscoveryRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.3 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ServiceDiscoveryRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_SessionStop_003

TC_SECC_AC_VTB_SessionStop_003.

Test objective: GoodCase; the Test System sends a SessionStopReq with an invalid SessionID and ChargingSession=Terminate. Checks SessionStopRes with a valid SessionID, FAILED_UnknownSession, then TCP close within par_CMN_TCP_Connection_Termination_Timeout.

DUT (dut) **PASS** 9.00 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession' (name='SessionStopRes')	✓
SUT closes the TCP connection after the error response		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
PaymentServiceSelectionRes response time	100.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	150.6 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
SessionStopRes response time	101.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
TCP connection close after failure/ timeout	0.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

TC_SECC_AC_VTB_SessionStop_004

TC_SECC_AC_VTB_SessionStop_004.

Test objective: GoodCase; after a PowerDeliveryRes (current SessionID, ResponseCode OK) the Test System stays silent until V2G_Sequence_Timeout expires (sends no SessionStopReq). Checks the SUT terminates the session by closing TCP within par_CMN_TCP_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **PASS** 72.69 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TCP connection within V2G_Sequence_Timeout+termination (70s) with no SessionStopReq	closed 63.7s after PowerDeliveryRes(Stop)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
PowerDeliveryRes(Start) response time	101.8 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
PowerDeliveryRes(Stop) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
TCP connection close after failure/ timeout	63737.7 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Test case details — ISO 15118-20 (ISO 15118-21 ATS)

TC21_SECC_SDP_001

TC21_SECC_SDP_001.

Test objective: once the data link is established, send an SDP request built from the default parameter set (Security=TLS, TransportProtocol=TCP) up to 50 times, waiting up to the SDP_Msg_Timeout (0.25 s) between attempts and stopping at the first response. Passes if an SDP response is received before the retries are exhausted, with Security=TLS, TransportProtocol=TCP and a usable SECC IP address + port.

DUT (dut)

PASS

5.60 s

Conformance check	Observed	Result
SDP response Security = 0x00 (TLS)	got 0x00	✓
SDP response TransportProtocol = 0x00 (TCP)	got 0x00	✓
SDP response carries a valid SECC IP address + port	got port=50000 addr='fe80::3c4b:c4ff:fed8:1845'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SDP advertised TLS port	50000	-	info

TC21_SECC_SDP_002

TC21_SECC_SDP_002.

Test objective: once the data link is established, send a default-parameter-set SDP request from a client UDP port drawn from the dynamic range (49152-65535) to the well-known SDP destination port, retrying up to 50 times at the SDP_Msg_Timeout (0.25 s) cadence and stopping at the first response. Passes if the response datagram's own UDP source port is the fixed SDP server port (15118) -- distinct from the SECC TCP endpoint port carried inside the response payload, which _001 already checks.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
SDP response received within the SDP_Msg_Timeout retry window (≤ 50 requests)	SdpResponse(addr=fe80::3c4b:c4ff:fed8:1845, port=50000, security=0x00, transport=0x00, header=0x01/0xfe/0x9001, len=20)	✓
SDP response UDP source port = V2G_UDP_SDP_SERVER (15118)	got src port=15118	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TS SDP request client-side (V2G_UDP_SDP_CLIENT) port	59063	-	info

TC21_SECC_SDP_003

TC21_SECC_SDP_003.

Test objective: once the data link is established, send the default-parameter-set SDP request 50 times from the SAME fixed client UDP port (drawn from the dynamic range 49152-65535), ignoring every response and always waiting the full SDP_Msg_Timeout (0.25 s) before the next retransmission -- unlike _001/_002, the sequence never stops early on the first response. Passes if more than one SDP response datagram is observed on that fixed client port over the whole sequence (fewer than 50, even though 50 requests are sent, is expected and acceptable given UDP's unreliable delivery).

DUT (dut) **PASS** 18.61 s

Conformance check	Observed	Result
more than one SDP response received on the re-used V2G_UDP_SDP_CLIENT port across the full retry sequence	count=50	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SDP responses received on the re-used client port	50	-	info

TC21_SECC_SDP_004

TC21_SECC_SDP_004.

Test objective: once the data link is established, send the default-parameter-set SDP request 50 times, each retransmission from a FRESH, distinct client UDP port drawn from the dynamic range (49152-65535), ignoring every response and always waiting the full SDP_Msg_Timeout (0.25 s) before switching to the next port -- the sequence never stops early. Passes if more than one SDP response is observed; each one is inherently addressed back to the exact client port its corresponding request was sent from (a UDP socket only ever receives datagrams sent to the port it is bound to), so counting responses across all per-request sockets already proves the per-request port match. Fewer than 50 responses, even though 50 requests are sent, is expected and acceptable given UDP's unreliable delivery.

DUT (dut) **PASS** 18.00 s

Conformance check	Observed	Result
more than one SDP response received, each on the distinct V2G_UDP_SDP_CLIENT port its request was sent from, across the full retry sequence	count=50	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SDP responses received across the 50 distinct client ports	50	-	info

TC21_SECC_V2GTPSDP_001

TC21_SECC_V2GTPSDP_001.

Test objective: with the data link already established, the Test System sends a fully default SDP request and checks that the SUT answers, within SDP_Msg_Timeout, with an SDP response carrying the standard V2GTP framing: ProtocolVersion 0x01 and InvProtocolVersion 0xFE (PayloadType 0x9001 is implicit -- see below). The request is retransmitted on every timeout, up to the retry ceiling, until a response arrives.

DUT (dut) **PASS** 5.97 s

Conformance check	Observed	Result
SDP response V2GTP ProtocolVersion = 0x01	got 0x01	✓
SDP response V2GTP InvProtocolVersion = 0xFE	got 0xfe	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SDP response V2GTP PayloadLength	20 byte	-	info

TC21_SECC_V2GTPSDP_002

TC21_SECC_V2GTPSDP_002.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but sets the V2GTP header's ProtocolVersion field to the invalid value 0xFF, repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) **PASS** 18.61 s

Conformance check	Observed	Result
SUT does not respond to an SDP request with an invalid V2GTP ProtocolVersion (0xFF)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSDP_003

TC21_SECC_V2GTPSDP_003.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but sets the V2GTP header's InvProtocolVersion field to the invalid value 0xFF, repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) **PASS** 18.00 s

Conformance check	Observed	Result
SUT does not respond to an SDP request with an invalid V2GTP InvProtocolVersion (0xFF)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info

TC21_SECC_V2GTPSDP_004

TC21_SECC_V2GTPSDP_004.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but sets the V2GTP header's PayloadType field to the invalid value 0x7001 (neither the SDP request nor any known application payload type), repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) **PASS** 18.20 s

Conformance check	Observed	Result
SUT does not respond to an SDP request with an invalid V2GTP PayloadType (0x7001)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSDP_005

TC21_SECC_V2GTPSDP_005.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but declares the V2GTP header's PayloadLength field as 0 (the actual SDP request payload is 2 bytes), repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) **PASS** 18.80 s

Conformance check	Observed	Result
SUT does not respond to an SDP request with V2GTP PayloadLength = 0x00000000		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSDP_006

TC21_SECC_V2GTPSDP_006.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but declares the V2GTP header's PayloadLength field as one byte smaller than the actual SDP request payload (2 bytes, so 1 is declared), repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) PASS 18.00 s			
Conformance check		Observed	Result
SUT does not respond to an SDP request whose V2GTP PayloadLength is one byte smaller than the actual payload			✓
Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSDP_007

TC21_SECC_V2GTPSDP_007.

Test objective: with the data link already established, the Test System sends an otherwise-default SDP request but declares the V2GTP header's PayloadLength field as one byte larger than the actual SDP request payload (2 bytes, so 3 is declared), repeating the send on every SDP_Msg_Timeout up to the retry ceiling. The SUT must never answer an SDP response to this malformed request.

DUT (dut) PASS 18.20 s			
Conformance check		Observed	Result
SUT does not respond to an SDP request whose V2GTP PayloadLength is one byte larger than the actual payload			✓
Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_001

TC21_SECC_V2GTPSupportedAppProtocol_001.

Test objective: with the data link and TLS 1.3 connection already established, the Test System sends a default-parameter-set SupportedAppProtocolReq and checks that a SupportedAppProtocolRes arrives within the message response window, framed with the standard V2GTP header: ProtocolVersion 0x01, InvProtocolVersion 0xFE and PayloadType 0x8001.

DUT (dut) **PASS** 6.38 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
response V2GTP ProtocolVersion = 0x01	got 0x01	✓
response V2GTP InvProtocolVersion = 0xFE	got 0xfe	✓
response V2GTP PayloadType = 0x8001	got 0x8001	✓
framed response is a SupportedAppProtocolRes	got 'supportedAppProtocolRes'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SupportedAppProtocolRes response time	103.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_V2GTPSupportedAppProtocol_002

TC21_SECC_V2GTPSupportedAppProtocol_002.

Test objective: with the data link and TLS 1.3 connection already established, the Test System sends a default-parameter-set SupportedAppProtocolReq and checks that the SECC's SDP-advertised V2G data port -- the TCP destination port the whole V2G connection (and hence the SupportedAppProtocolRes) rides on -- lies in the Dynamic Ports range (49152-65535), rather than a well-known/reserved port.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓
SECC-advertised V2G data TCP destination port is in the Dynamic Ports range (49152-65535)	got 50000	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SECC-advertised (V2G_DST_TCP_DATA) TCP port	50000	-	info

TC21_SECC_V2GTPSupportedAppProtocol_003

TC21_SECC_V2GTPSupportedAppProtocol_003.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header carries an invalid ProtocolVersion (0xFF). Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget -- the malformed frame is dropped, the session is not.

DUT (dut) **PASS** 22.83 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq with an invalid V2GTP ProtocolVersion (0xFF) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_004

TC21_SECC_V2GTPSupportedAppProtocol_004.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header carries an invalid InvProtocolVersion (0xFF). Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq with an invalid V2GTP InvProtocolVersion (0xFF) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_005

TC21_SECC_V2GTPSupportedAppProtocol_005.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header carries an invalid PayloadType (0x7001, neither the SAP payload type nor any known application payload type). Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget.

DUT (dut) **PASS** 23.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq with an invalid V2GTP PayloadType (0x7001) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_006

TC21_SECC_V2GTPSupportedAppProtocol_006.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header declares a PayloadLength of 0, although the actual EXI payload is longer. Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget.

DUT (dut) **PASS** 23.20 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq with V2GTP PayloadLength = 0x00000000 within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_007

TC21_SECC_V2GTPSupportedAppProtocol_007.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header declares a PayloadLength one byte smaller than the actual EXI payload (Annex D function setSmallerV2GTPPayloadLength). Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq whose V2GTP PayloadLength is one byte smaller than the actual payload within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info

TC21_SECC_V2GTPSupportedAppProtocol_008

TC21_SECC_V2GTPSupportedAppProtocol_008.

Test objective: with the TLS 1.3 connection already established, the Test System sends a SupportedAppProtocolReq whose V2GTP header declares a PayloadLength one byte larger than the actual EXI payload (Annex D function setLargerV2GTPPayloadLength). Checks that the SUT neither answers within the message response window nor tears down the TLS connection within the CommunicationSetup performance budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SupportedAppProtocolReq whose V2GTP PayloadLength is one byte larger than the actual payload within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_001

TC21_SECC_V2GTPCommonMessages_001.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends a fully default SessionSetupReq and checks that the SUT answers, within the message observation window, with a SessionSetupRes carrying the standard V2GTP framing for a mainstream CommonMessages payload: ProtocolVersion 0x01, InvProtocolVersion 0xFE and PayloadType 0x8002.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a SessionSetupRes message	got 'SessionSetupRes'	✓
SessionSetupRes V2GTP ProtocolVersion = 0x01	got 0x01	✓
SessionSetupRes V2GTP InvProtocolVersion = 0xFE	got 0xfe	✓
SessionSetupRes V2GTP PayloadType = 0x8002	got 0x8002	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_002

TC21_SECC_V2GTPCommonMessages_002.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends a fully default SessionSetupReq and checks that a SessionSetupRes arrives, then checks that the TCP destination port used for the whole V2G data connection (established earlier from the SDP response and reused for every CommonMessages exchange) falls within the dynamic port range (49152-65535).

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a SessionSetupRes message	got 'SessionSetupRes'	✓
V2G data connection TCP destination port is in the dynamic port range (49152-65535)	port=50000	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionSetupRes response time	99.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_V2GTPCommonMessages_003

TC21_SECC_V2GTPCommonMessages_003.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but sets the V2GTP header's ProtocolVersion field to the invalid value 0xFF. Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **PASS** 22.82 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with an invalid V2GTP ProtocolVersion (0xFF) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with an invalid V2GTP ProtocolVersion (0xFF)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_004

TC21_SECC_V2GTPCommonMessages_004.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but sets the V2GTP header's InvProtocolVersion field to the invalid value 0xFF. Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with an invalid V2GTP InvProtocolVersion (0xFF) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with an invalid V2GTP InvProtocolVersion (0xFF)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_005

TC21_SECC_V2GTPCommonMessages_005.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but sets the V2GTP header's PayloadType field to the invalid value 0x7001 (neither the mainstream CommonMessages id nor any other known application payload type). Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with an invalid V2GTP PayloadType (0x7001) within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with an invalid V2GTP PayloadType (0x7001)		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_006

TC21_SECC_V2GTPCommonMessages_006.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but declares the V2GTP header's PayloadLength field as 0 (the actual EXI payload is longer). Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **PASS** 23.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with V2GTP PayloadLength = 0x00000000 within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with V2GTP PayloadLength = 0x00000000		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_V2GTPCommonMessages_007

TC21_SECC_V2GTPCommonMessages_007.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but declares the V2GTP header's PayloadLength field as one byte smaller than the actual EXI payload. Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **FAIL** 10.78 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with a V2GTP PayloadLength one byte smaller than the actual payload – connection was closed

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with a V2GTP PayloadLength one byte smaller than the actual payload within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with a V2GTP PayloadLength one byte smaller than the actual payload	connection was closed	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
TCP connection close after failure/ timeout	997.0 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✓

Failure detail (excerpt):

E `AssertionError: SUT does not terminate the TLS connection within
V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with a V2GTP PayloadLength
one byte smaller than the actual payload – connection was closed`

TC21_SECC_V2GTPCommonMessages_008

TC21_SECC_V2GTPCommonMessages_008.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends an otherwise-default SessionSetupReq but declares the V2GTP header's PayloadLength field as one byte larger than the actual EXI payload. Checks the SUT neither answers nor tears down the TLS connection for the whole CommunicationSetup budget.

DUT (dut) **PASS** 23.22 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT does not respond to a SessionSetupReq with a V2GTP PayloadLength one byte larger than the actual payload within V2G_EVCC_Msg_Timeout		✓
SUT does not terminate the TLS connection within V2G_SECC_CommunicationSetup_Performance_Time after a SessionSetupReq with a V2GTP PayloadLength one byte larger than the actual payload		✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_SupportedAppProtocol_001

TC21_SECC_SupportedAppProtocol_001.

Test objective: happy-path SupportedAppProtocol handshake. With the TLS 1.3 connection already established, the Test System offers the default single-entry AppProtocol list (the -20 namespace matching the configured energy-transfer type, at its default version/schema/priority values) and checks that a SupportedAppProtocolRes arrives before the message observation window elapses. Neither the ResponseCode nor the SchemaID value is constrained by this TC (the ATS format leaves both as wildcards here) -- only the message type and its timeliness are graded.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SupportedAppProtocolRes response time	103.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ResponseCode	OK_SuccessfulNegotiation	-	info
SchemaID	1	-	info

TC21_SECC_SupportedAppProtocol_002

TC21_SECC_SupportedAppProtocol_002.

Test objective: negative SupportedAppProtocol handshake. The Test System offers a single AppProtocol whose namespace names the -20 CommonMessages schema directly -- not a valid energy-transfer-service namespace -- and checks that the SUT rejects the offer with ResponseCode FAILED_NoNegotiation, in time, and omits SchemaID from the response.

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓
ResponseCode = FAILED_NoNegotiation for a CommonMessages namespace offer	got 'Failed_NoNegotiation'	✓
SupportedAppProtocolRes omits SchemaID	got None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SupportedAppProtocolRes response time	103.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SupportedAppProtocol_003

TC21_SECC_SupportedAppProtocol_003.

Test objective: SupportedAppProtocol priority selection. The Test System offers two AppProtocol entries in one request -- a legacy namespace at the lower priority (Priority 2, listed first) and the -20 energy-transfer namespace at the highest priority (Priority 1, listed second) -- and checks that the SUT negotiates the highest-priority entry (the -20 namespace) rather than simply the first list entry, replying OK_SuccessfulNegotiation and echoing that entry's SchemaID. Note that a lower Priority number means a higher priority: Priority 1 is the numerically lowest value and thus the highest priority.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓
ResponseCode = OK_SuccessfulNegotiation	got 'OK_SuccessfulNegotiation'	✓
SUT selects the highest-priority protocol's SchemaID (2), not the first list entry's	got 2	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_SupportedAppProtocol_004

TC21_SECC_SupportedAppProtocol_004.

Test objective: SupportedAppProtocol minor-version tolerance. The Test System offers the default single-entry AppProtocol list but with a VersionNumberMinor that deliberately differs from the SUT's, and checks that the SUT still negotiates successfully -- replying OK_SuccessfulNegotiation and echoing back the SchemaID of the offered (and only) entry.

DUT (dut) **FAIL** 6.00 s

FAILURE REASON

harness/test_ev.py:378

AssertionError: ResponseCode = OK_SuccessfulNegotiation – got 'OK_SuccessfulNegotiationWithMinorDeviation'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
SUT sends a supportedAppProtocolRes message	got 'supportedAppProtocolRes'	✓
ResponseCode = OK_SuccessfulNegotiation	got 'OK_SuccessfulNegotiationWithMinorDeviation'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info

Failure detail (excerpt):

E AssertionError: ResponseCode = OK_SuccessfulNegotiation – got 'OK_SuccessfulNegotiationWithMinorDeviation'

TC21_SECC_SessionSetup_002

TC21_SECC_SessionSetup_002.

Test objective: GoodCase up to the SupportedAppProtocol handshake (TLS connected, no session yet); the Test System then sends a valid ServiceDiscoveryReq (SessionID all-zero) in place of the expected SessionSetupReq. Checks the SUT answers with a ServiceDiscoveryRes within the message response window, carrying ResponseCode FAILED_SequenceError, no Header signature and no VASList.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓
ServiceDiscoveryRes omits the VASList	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	99.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionSetup_003

TC21_SECC_SessionSetup_003.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System then withholds the SessionSetupReq entirely. Checks the SUT terminates the TLS connection between the CommunicationSetup performance time and the following TLS connection termination timeout -- distinguishing an SUT that enforces the tighter CommunicationSetup budget from one that only reacts to the much longer general sequence timeout.

DUT (dut) **PASS** 23.83 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT terminates the TLS connection between V2G_SECC_CommunicationSetup_Performance_Time and TLS_Connection_Termination_Timeout (17-24s)	closed 18.1s after TLS establishment	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	17980.6 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗
TLS termination after V2G_SECC_CommunicationSetup_Performance_Time	18.1 s	-	info

TC21_SECC_SessionSetup_004

TC21_SECC_SessionSetup_004.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends a SessionSetupReq built from the default parameter set. Checks a SessionSetupRes is received within the message response window and that it carries a syntactically valid (non-empty) EVSEID; the ResponseCode value itself is not constrained by this TC.

DUT (dut) **PASS** 6.17 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a SessionSetupRes message	got 'SessionSetupRes'	✓
SessionSetupRes carries a syntactically valid EVSEID	got 'DE*PNX*E12345*1'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionSetupRes response time	100.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionSetup_005

TC21_SECC_SessionSetup_005.

Test objective: GoodCase up to the SupportedAppProtocol handshake; the Test System sends a SessionSetupReq built from the default parameter set. Checks a SessionSetupRes is received in time carrying ResponseCode OK_NewSessionEstablished and a newly assigned, non-zero SessionID.

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT sends a SessionSetupRes message	got 'SessionSetupRes'	✓
ResponseCode = OK_NewSessionEstablished	got 'OK_NewSessionEstablished'	✓
SessionSetupRes carries a new non-zero SessionID	got 461fb0f1209b88c3	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionSetupRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_AuthorizationSetup_001

TC21_SECC_AuthorizationSetup_001.

Test objective: GoodCase up to a received SessionSetupRes; the Test System then sends an AuthorizationSetupReq built from the default parameter set. Checks an AuthorizationSetupRes is received within the message response window, carrying ResponseCode OK, the list of advertised authorization services, the certificate-installation-service flag, and -- because the SUT offers PnC -- a PnC authorization-mode block whose GenChallenge is a present, 16-byte value.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
AuthorizationSetupRes received within V2G_EVCC_Msg_Timeout (2 s)	100 ms	✓
SUT sends an AuthorizationSetupRes message	got 'AuthorizationSetupRes'	✓
ResponseCode = OK	got 'OK'	✓
AuthorizationSetupRes advertises the authorization services	got ['EIM', 'PnC']	✓
AuthorizationSetupRes carries the CertificateInstallationService flag	got True	✓
PnC offered: PnC_ASResAuthorizationMode carries a GenChallenge	got '44b36d801c447845b119b4cdd52aa73c'	✓
GenChallenge is 16 bytes long [V2G20-2110]	got 16 byte(s)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
AuthorizationSetupRes response time	99.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
advertised authorization services	['EIM', 'PnC']	-	info

TC21_SECC_AuthorizationSetup_002

TC21_SECC_AuthorizationSetup_002.

Test objective: GoodCase up to a received SessionSetupRes; the Test System then sends an AuthorizationSetupReq whose SessionID is a freshly generated nonce not matching the established session. Checks an AuthorizationSetupRes is received within the message response window, carrying ResponseCode FAILED_UnknownSession and no Header signature.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
AuthorizationSetupRes received within V2G_EVCC_Msg_Timeout (2 s)	100 ms	✓
SUT sends an AuthorizationSetupRes message	got 'AuthorizationSetupRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
AuthorizationSetupRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_AuthorizationSetup_003

TC21_SECC_AuthorizationSetup_003.

Test objective: GoodCase up to a received SessionSetupRes; the Test System then sends a valid ServiceDiscoveryReq in place of the expected AuthorizationSetupReq. Checks the SUT answers with a ServiceDiscoveryRes within the message response window, carrying ResponseCode FAILED_SequenceError, no Header signature and no VASList.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
ServiceDiscoveryRes received within V2G_EVCC_Msg_Timeout (2 s)	100 ms	✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓
ServiceDiscoveryRes omits the VASList	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_AuthorizationSetup_004

TC21_SECC_AuthorizationSetup_004.

Test objective: GoodCase up to a received SessionSetupRes; the Test System then withholds the AuthorizationSetupReq entirely. Checks the SUT reacts to the V2G sequence timeout by terminating the TLS connection between the sequence timeout and the following TLS connection termination timeout (i.e. the connection comes down no earlier than the sequence timeout and within the termination budget on top of it).

DUT (dut) **PASS** 69.89 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59-66s)	closed 64.0s after SessionSetupRes	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/ timeout	64005.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗
TLS termination after V2G_SECC_Sequence_Timeout	64.0 s	-	info

TC21_SECC_AuthorizationSetup_005

TC21_SECC_AuthorizationSetup_005.

Test objective: GoodCase up to a received SessionSetupRes; the Test System then sends a SessionStopReq built from the default parameter set, modelling an EV-initiated shutdown for a non-critical reason (Terminate). Checks a SessionStopRes is received within the message response window carrying ResponseCode OK.

DUT (dut) **PASS** 6.12 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
SessionStopRes received within V2G_EVCC_Msg_Timeout (2 s)	100 ms	✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	100.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_001

TC21_SECC_CertificateInstallation_001.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq built from the default parameter set but with MaximumContractCertificateChains raised to 2, with more than one contract available at the backend for this vehicle's provisioning identity. Checks the SUT answers a CertificateInstallationRes in time, ultimately with EVSEProcessing Finished, ResponseCode OK, a verifiable SignedInstallationData signature, and RemainingContractCertificateChains == 1 (two available, one delivered). Requires more than one contract at the backend (PIXIT_CMN_MultipleContracts).

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = OK	got 'OK'	✓
RemainingContractCertificateChains == 1	got 1	✓
SignedInstallationData signature verifies against the CPS leaf	SignedInstallationData signature verified against CPS leaf	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	98.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:18:02.278	CS ↔ CSMS	StatusNotification	{"connectorId": 1, "connectorStatus": "Occupied", "evseId": 1, "timestamp": "2026-10-11T07:18:02.277Z"}
07:18:02.279	CSMS ↔ CS	StatusNotification (response)	{}
07:18:04.619	CS ↔ CSMS	Get15118EVCertificate	{"action": "Install", "exiRequest": "<3080 base64 chars>", "iso15118SchemaVersion": "urn:iso:std:iso:15118:-20:CommonMessages"}
07:18:04.628	CSMS ↔ CS	Get15118EVCertificate (response)	{"exiResponse": "<6368 base64 chars>", "remainingContracts": 1, "status": "Accepted"}

TC21_SECC_CertificateInstallation_002

TC21_SECC_CertificateInstallation_002.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq from the default parameter set with exactly one contract available at the backend for this provisioning identity. Checks the SUT answers a CertificateInstallationRes in time, ultimately with EVSEProcessing Finished, ResponseCode OK, a verifiable SignedInstallationData signature, and RemainingContractCertificateChains == 0 (the single available contract delivered). Requires a single contract at the backend (PIXIT_CMN_MultipleContracts = False).

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = OK	got 'OK'	✓
RemainingContractCertificateChains == 0	got 0	✓
SignedInstallationData signature verifies against the CPS leaf	SignedInstallationData signature verified against CPS leaf	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:18:09.278	CS → CSMS	StatusNotification	{ "connectorId": 1, "connectorStatus": "Occupied", "evseId": 1, "timestamp": "2026-10-11T07:18:09.277Z" }
07:18:09.279	CSMS → CS	StatusNotification (response)	{ }
07:18:11.616	CS → CSMS	Get15118EVCertificate	{ "action": "Install", "exiRequest": "<3080 base64 chars>", "iso15118SchemaVersion": "urn:iso:std:iso:15118:-20:CommonMessages" }
07:18:11.624	CSMS → CS	Get15118EVCertificate (response)	{ "exiResponse": "<6368 base64 chars>", "remainingContracts": 0, "status": "Accepted" }

TC21_SECC_CertificateInstallation_003

TC21_SECC_CertificateInstallation_003.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose PrioritizedEMAIDs list names an EMAID whose eMSP is not registered at the backend. Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_eMSPUnknown. Backend condition PIXIT_SECC_UnknownEMAID.

DUT (dut) **PASS** 7.20 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_eMSPUnknown	got 'WARNING_eMSPUnknown'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:18:17.277	CS → CSMS	StatusNotification	{"connectorId": 1, "connectorStatus": "Occupied", "evseId": 1, "timestamp": "2026-10-11T07:18:17.277Z"}
07:18:17.278	CSMS → CS	StatusNotification (response)	{}
07:18:19.617	CS → CSMS	Get15118EVCertificate	{"action": "Install", "exiRequest": "<3100 base64 chars>", "iso15118SchemaVersion": "urn:iso:std:iso:15118:-20:CommonMessages"}
07:18:19.619	CSMS → CS	Get15118EVCertificate (response)	{"exiResponse": "<224 base64 chars>", "remainingContracts": 0, "status": "Accepted"}

TC21_SECC_CertificateInstallation_004

TC21_SECC_CertificateInstallation_004.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq for a provisioning identity (PCID) for which the backend has no registered contract. Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_NoContractMatchingPCIDFound. The "no contract for this PCID" condition is realised by the backend / SA configuration (PIXIT_SECC_UnknownPCID); the wire request uses the default OEM provisioning chain.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_NoContractMatchingPCIDFound	got 'WARNING_NoContractMatchingPCIDFound'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	96.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:18:24.279	CS ↔ CSMS	StatusNotification	{"connectorId": 1, "connectorStatus": "Occupied", "evseId": 1, "timestamp": "2026-10-11T07:18:24.278Z"}
07:18:24.280	CSMS ↔ CS	StatusNotification (response)	{}
07:18:26.619	CS ↔ CSMS	Get15118EVCertificate	{"action": "Install", "exiRequest": "<3080 base64 chars>", "iso15118SchemaVersion": "urn:iso:std:iso:15118:-20:CommonMessages"}
07:18:26.622	CSMS ↔ CS	Get15118EVCertificate (response)	{"exiResponse": "<224 base64 chars>", "remainingContracts": 0, "status": "Accepted"}

TC21_SECC_CertificateInstallation_005

TC21_SECC_CertificateInstallation_005.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq while the SUT cannot retrieve a new contract certificate from the backend within the message performance time. Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_NoCertificateAvailable. The unreachable-backend condition is realised by the SA configuration (PIXIT_SECC_CommunicationToSA = False); the wire request uses the default OEM provisioning chain.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_NoCertificateAvailable	got 'WARNING_NoCertificateAvailable'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:18:31.278	CS ↔ CSMS	StatusNotification	{"connectorId": 1, "connectorStatus": "Occupied", "evseId": 1, "timestamp": "2026-10-11T07:18:31.278Z"}
07:18:31.279	CSMS ↔ CS	StatusNotification (response)	{}
07:18:33.619	CS ↔ CSMS	Get15118EVCertificate	{"action": "Install", "exiRequest": "<3080 base64 chars>", "iso15118SchemaVersion": "urn:iso:std:iso:15118:-20:CommonMessages"}
07:18:33.620	CSMS ↔ CS	Get15118EVCertificate (response)	{"exiResponse": "<0 base64 chars>", "status": "Failed", "statusInfo": {"reasonCode": "BackendUnreachable"}}

TC21_SECC_CertificateInstallation_006

TC21_SECC_CertificateInstallation_006.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired leaf certificate (sub-CAs valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_007

TC21_SECC_CertificateInstallation_007.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired SubCA2 certificate (leaf and SubCA1 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
CertificateInstallationRes response time	97.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_008

TC21_SECC_CertificateInstallation_008.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired SubCA1 certificate (leaf and SubCA2 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_009

TC21_SECC_CertificateInstallation_009.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired leaf and expired SubCA2 (SubCA1 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_010

TC21_SECC_CertificateInstallation_010.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired leaf and expired SubCA1 (SubCA2 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	98.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_011

TC21_SECC_CertificateInstallation_011.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has an expired SubCA2 and expired SubCA1 (leaf valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
CertificateInstallationRes response time	96.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_012

TC21_SECC_CertificateInstallation_012.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose entire OEM provisioning chain (leaf, SubCA2 and SubCA1) is expired. Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateExpired.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_013

TC21_SECC_CertificateInstallation_013.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid leaf certificate (sub-CAs valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_014

TC21_SECC_CertificateInstallation_014.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid SubCA2 certificate (leaf and SubCA1 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	96.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_015

TC21_SECC_CertificateInstallation_015.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid SubCA1 certificate (leaf and SubCA2 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_016

TC21_SECC_CertificateInstallation_016.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid leaf and not-yet-valid SubCA2 (SubCA1 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	98.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_017

TC21_SECC_CertificateInstallation_017.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid leaf and not-yet-valid SubCA1 (SubCA2 valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_018

TC21_SECC_CertificateInstallation_018.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose OEM provisioning chain has a not-yet-valid SubCA2 and not-yet-valid SubCA1 (leaf valid). Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	98.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_019

TC21_SECC_CertificateInstallation_019.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq whose entire OEM provisioning chain (leaf, SubCA2 and SubCA1) is not yet valid. Checks the SUT answers a CertificateInstallationRes in time with EVSEProcessing Finished and ResponseCode WARNING_CertificateNotYetValid.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 97 ms	✓
EVSEProcessing = Finished	got 'Finished'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_020

TC21_SECC_CertificateInstallation_020.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq from the default parameter set but with an unknown SessionID. Checks the SUT answers a CertificateInstallationRes in time with ResponseCode FAILED_UnknownSession.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallation_021

TC21_SECC_CertificateInstallation_021.

Test objective: GoodCase up to AuthorizationSetupRes; the Test System sends a CertificateInstallationReq from the default parameter set whose Header signature is computed with a private key other than the OEM provisioning leaf's -- the ATS's f_setSignature(toBeSigned_value, contractPrivateKey_value): a well-formed signature over the correct content, made with the MO contract leaf key instead. Checks the SUT answers a CertificateInstallationRes in time with ResponseCode FAILED_SignatureError.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a CertificateInstallationRes message	got 'CertificateInstallationRes'	✓
every CertificateInstallationRes received within V2G_EVCC_Msg_Timeout (5 s)	slowest 98 ms	✓
ResponseCode = FAILED_SignatureError	got 'FAILED_SignatureError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
CertificateInstallationRes response time	97.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_Authorization_001

TC21_SECC_Authorization_001.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends the AuthorizationReq from the ATS Annex C default parameter set for the authorization service the SUT offers: when the SUT offered PnC, the signed PnC request (Id "ram_id", the SUT's GenChallenge, the valid contract chain, signed with the contract private key); otherwise the bare EIM request after an external-identification token was presented at the charger. Checks every AuthorizationRes arrives within the message response window and that, following the Ongoing → Finished repetition, the final one carries ResponseCode OK with EVSEProcessing Finished.

DUT (dut) **PASS** 6.62 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 94 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 2 poll(s)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
authorization service used (Annex C default set)	PnC	-	info
PnC Authorization polls to EVSEProcessing=Finished	2	-	info

TC21_SECC_Authorization_003

TC21_SECC_Authorization_003.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends the default signed PnC AuthorizationReq (valid contract chain). The eMAID of that contract leaf is one the SUT's secondary actor does not know -- an SUT-side precondition (ATS PIXIT_SECC_UnknownEMAID = True), not a wire-level fault: the chain and signature verify. The TC therefore needs the tester's CSMS as the DUT's backend (PIXIT_SECC_TesterCSMS, marker requires_csms, SUT config config-test-conformance-iso20-pnc-ocpp.yaml); there the condition is produced by the backend itself: the OCPP Authorize for the eMAID is answered idTokenInfo.status Unknown ("identifier is unknown") with the certificate accepted, which is the OCPP rendering of [V2G20-2211]. Checks the AuthorizationRes carries ResponseCode WARNING_eMSPUnknown with EVSEProcessing Finished.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 97 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_eMSPUnknown	got 'WARNING_eMSPUnknown' after 2 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info

OCPP (DUT ↔ tester CSMS)	Direction	Message	Payload
07:14:32.277	CS ↔ CSMS	StatusNotification	{"connectorId":1,"connectorStatus":"Occupied","evseId":1,"timestamp":"2026-10-11T07:14:32.276Z"}
07:14:32.277	CSMS ↔ CS	StatusNotification (response)	{}
07:14:34.651	CS ↔ CSMS	Authorize	{ "idToken": { "idToken": "UKSWI123456791A", "type": "eMAID" }, "iso15118CertificateHashData": [{ "hashAlgorithm": "SHA256", "issuerKeyHash": "2a25071abd4fc18b270897506f488d0a0cdb442872fe6da9020bbb03b6945e2d", "issuerNameHash": "efc5a55e6e1e59c7605b48d7f260f2321aba004f97f5872986c3388f8756dce5", "responderURL": "https://www.example.com/", "serialNumber": "3044" }, { "hashAlgorithm": "SHA256", "issuerKeyHash": "7f306ad7add158c26f05ee0e35d0f120988ecf1caa5c64a81aa90959553318b9", "issuerNameHash": "0fd741fe2020f72842fa212a4dc59f00d8d9e04a48d6eb01ea68e63978ac0c4a", "responderURL": "https://www.example.com/", "serialNumber": "3043" }] }
07:14:34.652	CSMS ↔ CS	Authorize (response)	{ "certificateStatus": "Accepted", "idTokenInfo": { "status": "Unknown" } }

TC21_SECC_Authorization_004

TC21_SECC_Authorization_004.

Test objective: signed PnC AuthorizationReq whose contract leaf certificate has a validity window entirely in the past (Sub-CA2/Sub-CA1 valid). Checks the AuthorizationRes reports WARNING_CertificateExpired, EVSEProcessing Finished.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 91 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_005

TC21_SECC_Authorization_005.

Test objective: signed PnC AuthorizationReq whose eMSP Sub-CA2 certificate is expired (leaf/Sub-CA1 valid) → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_006

TC21_SECC_Authorization_006.

Test objective: signed PnC AuthorizationReq whose eMSP Sub-CA1 certificate is expired (leaf/Sub-CA2 valid) → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_007

TC21_SECC_Authorization_007.

Test objective: signed PnC AuthorizationReq with both the contract leaf and eMSP Sub-CA2 expired (Sub-CA1 valid) → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_008

TC21_SECC_Authorization_008.

Test objective: signed PnC AuthorizationReq with both the contract leaf and eMSP Sub-CA1 expired (Sub-CA2 valid) → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 5.99 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_009

TC21_SECC_Authorization_009.

Test objective: signed PnC AuthorizationReq with both eMSP Sub-CA2 and Sub-CA1
expired (leaf valid) → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_010

TC21_SECC_Authorization_010.

Test objective: signed PnC AuthorizationReq with the contract leaf, eMSP

Sub-CA2 and Sub-CA1 all expired → WARNING_CertificateExpired, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 94 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateExpired	got 'WARNING_CertificateExpired' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_011

TC21_SECC_Authorization_011.

Test objective: signed PnC AuthorizationReq whose contract leaf certificate has a validity window entirely in the future (Sub-CA2/Sub-CA1 valid) → WARNING_CertificateNotYetValid, EVSEProcessing Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_012

TC21_SECC_Authorization_012.

Test objective: signed PnC AuthorizationReq whose eMSP Sub-CA2 is not yet valid (leaf/Sub-CA1 valid) → WARNING_CertificateNotYetValid, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info

TC21_SECC_Authorization_013

TC21_SECC_Authorization_013.

Test objective: signed PnC AuthorizationReq whose eMSP Sub-CA1 is not yet valid (leaf/Sub-CA2 valid) → WARNING_CertificateNotYetValid, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_014

TC21_SECC_Authorization_014.

Test objective: signed PnC AuthorizationReq with both the contract leaf and eMSP Sub-CA2 not yet valid (Sub-CA1 valid) →
WARNING_CertificateNotYetValid, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_015

TC21_SECC_Authorization_015.

Test objective: signed PnC AuthorizationReq with both the contract leaf and eMSP Sub-CA1 not yet valid (Sub-CA2 valid) →
WARNING_CertificateNotYetValid, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_016

TC21_SECC_Authorization_016.

Test objective: signed PnC AuthorizationReq with both eMSP Sub-CA2 and Sub-CA1
not yet valid (leaf valid) → WARNING_CertificateNotYetValid, Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 95 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_017

TC21_SECC_Authorization_017.

Test objective: signed PnC AuthorizationReq with the contract leaf, eMSP
 Sub-CA2 and Sub-CA1 all not yet valid → WARNING_CertificateNotYetValid,
 Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 94 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_CertificateNotYetValid	got 'WARNING_CertificateNotYetValid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_018

TC21_SECC_Authorization_018.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends a signed PnC AuthorizationReq whose GenChallenge was NOT the one delivered in the preceding AuthorizationSetupRes (a fresh random value the signature is computed over). Checks the AuthorizationRes reports WARNING_ChallengeInvalid with EVSEProcessing Finished.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 97 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = WARNING_ChallengeInvalid	got 'WARNING_ChallengeInvalid' after 1 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_021

TC21_SECC_Authorization_021.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends a PnC AuthorizationReq whose Header signature is computed with a private key other than the contract leaf's (the OEM provisioning key), so the SUT's signature verification over PnC_AReqAuthorizationMode fails. Checks the AuthorizationRes reports ResponseCode FAILED_SignatureError.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	97 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = FAILED_SignatureError	got 'FAILED_SignatureError'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
AuthorizationRes response time	96.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_Authorization_023

TC21_SECC_Authorization_023.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends a signed PnC AuthorizationReq whose contract leaf is still valid but expires in 14 days or fewer. Checks the AuthorizationRes carries ResponseCode OK_CertificateExpiresSoon with EVSEProcessing Finished.

DUT (dut) **PASS** 6.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
every AuthorizationRes received within V2G_EVCC_Msg_Timeout (2 s)	slowest 96 ms	✓
SUT sends an AuthorizationRes message	got 'AuthorizationRes'	✓
ResponseCode = OK_CertificateExpiresSoon	got 'OK_CertificateExpiresSoon' after 2 poll(s)	✓
EVSEProcessing = Finished	got 'Finished'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_Authorization_024

TC21_SECC_Authorization_024.

Test objective: GoodCase up to AuthorizationSetup; the Test System sends a SessionStopReq from the default parameter set (an EV-initiated shutdown for a non-critical reason). Checks a SessionStopRes is received within the message response window carrying ResponseCode OK.

DUT (dut) **PASS** 6.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SessionStopRes received within V2G_EVCC_Msg_Timeout (2 s)	100 ms	✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	99.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallationOrAuthorization_001

TC21_SECC_CertificateInstallationOrAuthorization_001.

Test objective: GoodCase up to AuthorizationSetup (the SUT now expects either an AuthorizationReq or a CertificateInstallationReq); the Test System instead sends a valid ServiceDiscoveryReq from the default parameter set. Checks the SUT answers a ServiceDiscoveryRes within the message response window carrying ResponseCode FAILED_SequenceError and no Header signature.

DUT (dut) **PASS** 6.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓
VASList omitted (ATS: VASList := omit)	got None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	99.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_CertificateInstallationOrAuthorization_002

TC21_SECC_CertificateInstallationOrAuthorization_002.

Test objective: GoodCase up to AuthorizationSetup; the Test System then sends neither an AuthorizationReq nor a CertificateInstallationReq and stays silent past the SECC sequence timeout. Checks the SUT reacts to the sequence timeout by terminating the TLS connection within the following TLS termination timeout. LONG TEST.

DUT (dut) **PASS** 70.48 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s)	closed 64.0s after AuthorizationSetupRes	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	64009.4 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC21_SECC_ServiceDiscovery_001

TC21_SECC_ServiceDiscovery_001.

Test objective: after AuthorizationRes(Finished), send a ServiceDiscoveryReq built from the default parameter set and check the SUT replies ServiceDiscoveryRes with ResponseCode OK, an EnergyTransferServiceList and a stated ServiceRenegotiationSupported flag; any value-added-service list the SUT chooses to advertise must be well-formed.

DUT (dut) **PASS** 6.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓
ServiceDiscoveryRes states ServiceRenegotiationSupported	got False	✓
ServiceDiscoveryRes offers at least one energy-transfer service	got {'Service': [{'FreeService': False, 'ServiceID': 1}]}	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
ServiceDiscoveryRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ServiceDiscovery_002

TC21_SECC_ServiceDiscovery_002.

Test objective: after AuthorizationRes(Finished), send a ServiceDiscoveryReq carrying a SessionID the SECC never assigned and check the SUT replies ServiceDiscoveryRes with ResponseCode FAILED_UnknownSession and no VASList.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
ServiceDiscoveryRes carries no VASList on the failure path	got None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceDiscovery_003

TC21_SECC_ServiceDiscovery_003.

Test objective: after AuthorizationRes(Finished), send a valid AuthorizationSetupReq instead of the expected ServiceDiscoveryReq (sequence error) and check the SUT replies AuthorizationSetupRes with ResponseCode FAILED_SequenceError.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends an AuthorizationSetupRes message	got 'AuthorizationSetupRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceDiscovery_004

TC21_SECC_ServiceDiscovery_004.

Test objective: after AuthorizationRes(Finished) the Test System sends no further request and waits out V2G_SECC_Sequence_Timeout instead of sending ServiceDiscoveryReq; checks the SUT terminates the session by closing the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout. LONG TEST (waits the ~60 s sequence timeout).

DUT (dut) **FAIL** 16.41 s

FAILURE REASON

harness/test_ev.py:378

AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.5s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TLS connection after V2G_SECC_Sequence_Timeout (within 66s)	closed 9.5s after AuthorizationRes(Finished)	✓
SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s)	closed after 9.5s	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9523.4 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E `AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.5s`

TC21_SECC_ServiceDiscovery_005

TC21_SECC_ServiceDiscovery_005.

Test objective: after AuthorizationRes(Finished), send a SessionStopReq built from the default parameter set (an EV-initiated shutdown for a non-critical reason) and check the SUT replies SessionStopRes with ResponseCode OK.

DUT (dut) **PASS** 6.59 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	100.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ServiceDetail_001

TC21_SECC_ServiceDetail_001.

Test objective: after ServiceDiscoveryRes, send a ServiceDetailReq for the energy-transfer service the SUT offered (matching the configured AC/DC transfer mode) and check the SUT replies ServiceDetailRes with ResponseCode OK, the echoed ServiceID and a ServiceParameterList.

DUT (dut) **PASS** 6.58 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDetailRes message	got 'ServiceDetailRes'	✓
ResponseCode = OK	got 'OK'	✓
ServiceDetailRes echoes the requested ServiceID 1	got 1	✓

Conformance check	Observed	Result
ServiceDetailRes carries a ServiceParameterList	got {'ParameterSet': [{'Parameter': {'Name': 'Connector', 'intValue': 1}, {'Name': 'ControlMode', 'intValue': 2}, {'Name': 'EVSENominalVoltage', 'intValue': 230}, {'Name': 'MobilityNeedsMode', 'intValue': 1}, {'Name': 'Pricing', 'intValue': 0}], 'ParameterSetID': 0}, {'Parameter': {'Name': 'Connector', 'intValue': 2}, {'Name': 'ControlMode', 'intValue': 2}, {'Name': 'EVSENominalVoltage', 'intValue': 230}, {'Name': 'MobilityNeedsMode', 'intValue': 1}, {'Name': 'Pricing', 'intValue': 0}], 'ParameterSetID': 1}, {'Parameter': {'Name': 'Connector', 'intValue': 1}, {'Name': 'ControlMode', 'intValue': 1}, {'Name': 'EVSENominalVoltage', 'intValue': 230}, {'Name': 'MobilityNeedsMode', 'intValue': 1}, {'Name': 'Pricing', 'intValue': 0}], 'ParameterSetID': 2}, {'Parameter': {'Name': 'Connector', 'intValue': 2}, {'Name': 'ControlMode', 'intValue': 1}, {'Name': 'EVSENominalVoltage', 'intValue': 230}, {'Name': 'MobilityNeedsMode', 'intValue': 1}, {'Name': 'Pricing', 'intValue': 0}], 'ParameterSetID': 3}]}	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDetailRes response time	100.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ServiceDetail_002

TC21_SECC_ServiceDetail_002.

Test objective: after ServiceDiscoveryRes, send a ServiceDetailReq for the offered energy-transfer service carrying a SessionID the SECC never assigned and check the SUT replies ServiceDetailRes with ResponseCode FAILED_UnknownSession.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDetailRes message	got 'ServiceDetailRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info

TC21_SECC_ServiceDetail_003

TC21_SECC_ServiceDetail_003.

Test objective: after ServiceDiscoveryRes, send a second, valid ServiceDiscoveryReq instead of the expected ServiceDetailReq (sequence error) and check the SUT replies ServiceDiscoveryRes with ResponseCode FAILED_SequenceError and no VASList.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
ServiceDiscoveryRes carries no VASList on the failure path	got None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceDetail_004

TC21_SECC_ServiceDetail_004.

Test objective: after ServiceDiscoveryRes, send a ServiceDetailReq naming a valid ServiceID the SUT did NOT offer in ServiceDiscoveryRes and check the SUT replies ServiceDetailRes with ResponseCode FAILED_ServiceIDInvalid.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDetailRes message	got 'ServiceDetailRes'	✓
ResponseCode = FAILED_ServiceIDInvalid	got 'FAILED_ServiceIDInvalid'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceDetail_005

TC21_SECC_ServiceDetail_005.

Test objective: after ServiceDiscoveryRes the Test System sends no further request and waits out V2G_SECC_Sequence_Timeout instead of sending ServiceDetailReq; checks the SUT terminates the session by closing the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout. LONG TEST (waits the ~60 s sequence timeout).

DUT (dut) **FAIL** 16.21 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.4s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TLS connection after V2G_SECC_Sequence_Timeout (within 66s)	closed 9.4s after ServiceDiscoveryRes	✓
SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s)	closed after 9.4s	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	410.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9384.4 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.4s

TC21_SECC_ServiceDetail_006

TC21_SECC_ServiceDetail_006.

Test objective: after ServiceDiscoveryRes, send a SessionStopReq built from the default parameter set (an EV-initiated shutdown for a non-critical reason) and check the SUT replies SessionStopRes with ResponseCode OK.

DUT (dut) **PASS** 6.78 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ServiceSelection_001

TC21_SECC_ServiceSelection_001.

Test objective: GoodCase; after ServiceDetailRes the Test System sends a ServiceSelectionReq selecting the energy-transfer service and parameter set the SUT offered, with all other elements at their default parameter-set values, and checks that the SUT replies with a ServiceSelectionRes carrying ResponseCode OK within the message-response timeout.

DUT (dut) **PASS** 7.20 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceSelectionRes message	got 'ServiceSelectionRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceSelection_002

TC21_SECC_ServiceSelection_002.

Test objective: GoodCase; after ServiceDetailRes the Test System sends a ServiceSelectionReq that otherwise matches the default parameter set but carries a SessionID the SUT never assigned, and checks that the SUT replies with a ServiceSelectionRes carrying ResponseCode FAILED_UnknownSession within the message-response timeout.

DUT (dut) **PASS** 7.61 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceSelectionRes message	got 'ServiceSelectionRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceSelection_003

TC21_SECC_ServiceSelection_003.

Test objective: GoodCase; after ServiceDetailRes the Test System sends a valid ServiceDiscoveryReq (default parameter set) rather than the expected ServiceSelectionReq, and checks that the SUT replies with a ServiceDiscoveryRes carrying ResponseCode FAILED_SequenceError and no VASList within the message-response timeout.

DUT (dut) **PASS** 7.39 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
ServiceDiscoveryRes carries no VASList on the failure path	got None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ServiceSelection_004

TC21_SECC_ServiceSelection_004.

Test objective: GoodCase; after ServiceDetailRes the Test System sends a ServiceSelectionReq naming a ServiceID that was never offered in ServiceDiscoveryRes together with a ParameterSetID that was never offered in ServiceDetailRes, and checks that the SUT replies with a ServiceSelectionRes carrying ResponseCode FAILED_ServiceSelectionInvalid within the message-response timeout.

DUT (dut) **FAIL** 7.00 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_ServiceSelectionInvalid – got
'FAILED_NoEnergyTransferServiceSelected'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=Everest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=Everest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceSelectionRes message	got 'ServiceSelectionRes'	✓
ResponseCode = FAILED_ServiceSelectionInvalid	got 'FAILED_NoEnergyTransferServiceSelected'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Failure detail (excerpt):

```
E   AssertionError: ResponseCode = FAILED_ServiceSelectionInvalid - got  
'FAILED_NoEnergyTransferServiceSelected'
```

TC21_SECC_ServiceSelection_006

TC21_SECC_ServiceSelection_006.

Test objective: GoodCase up to ServiceDetailRes, then the Test System sends nothing further (no ServiceSelectionReq) and waits. The pass criterion is that the SUT closes the TLS connection no earlier than the SECC sequence timeout and no later than that timeout plus the TLS connection termination bound.

DUT (dut) **FAIL** 16.21 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.3s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT closes the TLS connection within 66s of silence after ServiceDetailRes	closed after 9.3s	✓
SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s)	closed after 9.3s	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	411.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9283.0 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E AssertionError: SUT does not close before V2G_SECC_Sequence_Timeout expires (>= 59s) – closed after 9.3s

TC21_SECC_ServiceSelection_007

TC21_SECC_ServiceSelection_007.

Test objective: GoodCase up to ServiceDetailRes, then the Test System sends a SessionStopReq for a non-critical, EV-initiated shutdown (default parameter set), and checks that the SUT replies with a SessionStopRes carrying ResponseCode OK within the message-response timeout.

DUT (dut) **PASS** 6.79 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

TC21_SECC_ChargeParameterDiscovery_001

TC21_SECC_ChargeParameterDiscovery_001.

Test objective: happy-path ChargeParameterDiscovery. GoodCase through the CommonMessages negotiation sequence up to ServiceSelection, then the Test System sends the ChargeParameterDiscoveryReq for the negotiated energy-transfer type (DC or AC), built from the default parameter set.

Checks that the matching schema-specific ChargeParameterDiscoveryRes arrives within the message response window carrying ResponseCode OK. The presence of the energy-transfer-mode sub-element is recorded informationally (the ATS format leaves it a wildcard).

DUT (dut) **PASS** 7.51 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a AC_ChargeParameterDiscoveryRes message	got 'AC_ChargeParameterDiscoveryRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	408.9 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ChargeParameterDiscoveryRes response time	99.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
energy-transfer-mode element	AC_CPDResEnergyTransferMode	-	info

TC21_SECC_ChargeParameterDiscovery_002

TC21_SECC_ChargeParameterDiscovery_002.

Test objective: out-of-sequence check. GoodCase up to ServiceSelection; the Test System then sends a valid ServiceDiscoveryReq in place of the expected ChargeParameterDiscoveryReq. Checks the SUT answers with a ServiceDiscoveryRes within the message response window, carrying ResponseCode FAILED_SequenceError and no Header signature.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
ServiceDiscoveryRes response time	99.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ChargeParameterDiscovery_003

TC21_SECC_ChargeParameterDiscovery_003.

Test objective: sequence-timeout observation. GoodCase up to ServiceSelection; the Test System then stays silent, sending no ChargeParameterDiscoveryReq. Checks the SUT terminates the TLS connection after the sequence timeout elapses and within the following TLS connection termination timeout. LONG TEST.

DUT (dut) **FAIL** 16.41 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s) – SUT closed prematurely 9.2s after ServiceSelection (before V2G_SECC_Sequence_Timeout 60s)

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s)	SUT closed prematurely 9.2s after ServiceSelection (before V2G_SECC_Sequence_Timeout 60s)	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9184.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s) – SUT closed prematurely 9.2s after ServiceSelection (before V2G_SECC_Sequence_Timeout 60s)

TC21_SECC_ChargeParameterDiscovery_004

TC21_SECC_ChargeParameterDiscovery_004.

Test objective: EV-initiated shutdown for a non-critical reason. GoodCase up to ServiceSelection; the Test System then sends a SessionStopReq (ChargingSession Terminate) built from the default parameter set. Checks a SessionStopRes is received within the message response window carrying ResponseCode OK.

DUT (dut) **PASS** 7.59 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info

Measurement	Measured	Target / range	Result
SessionStopRes response time	99.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ScheduleExchange_002

TC21_SECC_ScheduleExchange_002.

Test objective: ScheduleExchange completion. GoodCase up to ChargeParameterDiscoveryRes; the Test System sends a ScheduleExchangeReq and, while the SUT answers EVSEProcessing Ongoing, repeats the ScheduleExchangeReq/Res exchange (bounded by the EVCC Ongoing timeout) until the SUT reports EVSEProcessing Finished. Checks the final ScheduleExchangeRes carries a ResponseCode starting with OK and EVSEProcessing Finished.

DUT (dut) **PASS** 8.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ScheduleExchangeRes message	got 'ScheduleExchangeRes'	✓
ResponseCode starts with OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ScheduleExchange polls to EVSEProcessing=Finished	1	-	info

TC21_SECC_ScheduleExchange_003

TC21_SECC_ScheduleExchange_003.

Test objective: unknown-SessionID negative. GoodCase up to ChargeParameterDiscoveryRes; the Test System then sends a single ScheduleExchangeReq (default parameter set, negotiated control mode) but stamps its header with a freshly generated SessionID the SUT never assigned. Checks the SUT answers a ScheduleExchangeRes within the message response window carrying ResponseCode FAILED_UnknownSession, with the response Header omitting the Signature and the response omitting GoToPause.

DUT (dut) **PASS** 8.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ScheduleExchangeRes message	got 'ScheduleExchangeRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
response Header carries no Signature	None	✓
response omits GoToPause	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
ScheduleExchangeRes response time	100.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ScheduleExchange_004

TC21_SECC_ScheduleExchange_004.

Test objective: out-of-sequence check. GoodCase up to ChargeParameterDiscoveryRes; the Test System then sends a valid ServiceDiscoveryReq in place of the expected ScheduleExchangeReq. Checks the SUT answers a ServiceDiscoveryRes within the message response window, carrying ResponseCode FAILED_SequenceError and no Header signature.

DUT (dut) **PASS** 7.60 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	100.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ScheduleExchange_005

TC21_SECC_ScheduleExchange_005.

Test objective: sequence-timeout observation. GoodCase up to ChargeParameterDiscoveryRes; the Test System then stays silent, sending no ScheduleExchangeReq. Checks the SUT terminates the TLS connection after the sequence timeout elapses and within the following TLS connection termination timeout. LONG TEST.

DUT (dut) **FAIL** 16.01 s

FAILURE REASON

harness/test_ev.py:378

AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s) – SUT closed prematurely 9.1s after ChargeParameterDiscoveryRes (before V2G_SECC_Sequence_Timeout 60s)

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s)	SUT closed prematurely 9.1s after ChargeParameterDiscoveryRes (before V2G_SECC_Sequence_Timeout 60s)	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9082.2 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout (59..66s) – SUT closed prematurely 9.1s after ChargeParameterDiscoveryRes (before V2G_SECC_Sequence_Timeout 60s)

TC21_SECC_ScheduleExchange_006

TC21_SECC_ScheduleExchange_006.

Test objective: Scheduled-control-mode schedule tuple. GoodCase up to ChargeParameterDiscoveryRes, selecting a Scheduled parameter set in ServiceSelection (the precondition fails if the SUT offers none); the Test System sends a ScheduleExchangeReq in Scheduled control mode and drives the Ongoing→Finished processing loop. Checks the final ScheduleExchangeRes carries ResponseCode starting with OK, EVSEProcessing Finished, and a Scheduled_SEResControlMode whose first ScheduleTuple has a ScheduleTupleID in the range 1..255 and a present ChargingSchedule.

DUT (dut) **PASS** 6.99 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓

Conformance check	Observed	Result
Response echoes the current SessionID		✓
SUT sends a ScheduleExchangeRes message	got 'ScheduleExchangeRes'	✓
ResponseCode starts with OK	got 'OK'	✓
EVSEProcessing = Finished	got 'Finished' after 1 poll(s)	✓
Scheduled_SEResControlMode carries at least one ScheduleTuple	got {'ScheduleTuple': [{'ChargingSchedule': {'PowerSchedule': {'PowerScheduleEntries': {'PowerScheduleEntry': [{'Duration': 86400, 'Power': {'Exponent': 0, 'Value': 0}}]}, 'TimeAnchor': 1791703625621}}, 'ScheduleTupleID': 1}]}	✓
ScheduleTupleID is in the range 1..255	got 1	✓
ScheduleTuple carries a ChargingSchedule	got {'PowerSchedule': {'PowerScheduleEntries': {'PowerScheduleEntry': [{'Duration': 86400, 'Power': {'Exponent': 0, 'Value': 0}}]}, 'TimeAnchor': 1791703625621}}	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ScheduleExchange polls to EVSEProcessing=Finished	1	-	info

TC21_SECC_ScheduleExchange_008

TC21_SECC_ScheduleExchange_008.

Test objective: EV-initiated shutdown for a non-critical reason. GoodCase up to ChargeParameterDiscoveryRes; the Test System then sends a SessionStopReq (ChargingSession Terminate) built from the default parameter set. Checks a SessionStopRes is received within the message response window carrying ResponseCode OK.

DUT (dut) **PASS** 7.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info

Measurement	Measured	Target / range	Result
SessionStopRes response time	99.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_001

TC21_SECC_PowerDelivery_001.

Test objective: GoodCase to the PowerDelivery precondition (DC_PreChargeRes on DC, ScheduleExchangeRes(Finished) on AC); the Test System sends a PowerDeliveryReq with ChargeProgress=Start from the default parameter set, and on AC signals CP State C right after sending it ([V2G20-847]). Checks a PowerDeliveryRes carrying ResponseCode OK is received within the message response window.

DUT (dut) **PASS** 7.40 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_002

TC21_SECC_PowerDelivery_002.

Test objective: GoodCase through PowerDelivery(Start) and several ChargeLoop exchanges; the Test System then sends a PowerDeliveryReq with ChargeProgress=Stop from the default parameter set, and on AC signals CP State B right after sending it ([V2G20-848]). Checks a PowerDeliveryRes carrying ResponseCode OK is received within the message response window.

DUT (dut) **PASS** 8.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
PowerDeliveryRes response time	148.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_003

TC21_SECC_PowerDelivery_003.

Test objective: GoodCase to the PowerDelivery precondition; the Test System sends a PowerDeliveryReq with ChargeProgress=Start but a freshly generated, unknown SessionID (and on AC signals CP State C right after sending it). Checks the SUT answers a PowerDeliveryRes carrying ResponseCode FAILED_UnknownSession within the message response window, with no EVSEStatus.

DUT (dut) **PASS** 7.10 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
PowerDeliveryRes carries no EVSEStatus	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_004

TC21_SECC_PowerDelivery_004.

Test objective: as _003 but in the Stop context -- GoodCase through the charge loop, then a PowerDeliveryReq with ChargeProgress=Stop and an unknown SessionID (on AC, CP State B right after sending it). Checks the SUT answers a PowerDeliveryRes carrying ResponseCode FAILED_UnknownSession within the message response window, with no EVSEStatus.

DUT (dut) **PASS** 8.10 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
PowerDeliveryRes carries no EVSEStatus	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.0 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	408.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_005

TC21_SECC_PowerDelivery_005.

Test objective: GoodCase to the PowerDelivery precondition; the Test System sends a valid ServiceDiscoveryReq in place of the expected PowerDeliveryReq(Start). Checks the SUT answers a ServiceDiscoveryRes carrying ResponseCode FAILED_SequenceError (and no Header signature) within the message response window.

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	99.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_006

TC21_SECC_PowerDelivery_006.

Test objective: as _005 but in the Stop context -- GoodCase through the charge loop, then a valid ServiceDiscoveryReq in place of the expected PowerDeliveryReq(Stop). Checks the SUT answers a ServiceDiscoveryRes carrying ResponseCode FAILED_SequenceError (and no Header signature) within the message response window.

DUT (dut) **PASS** 7.80 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓

Conformance check	Observed	Result
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.1 ms	-	info
ServiceDiscoveryRes response time	2.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_PowerDelivery_007

TC21_SECC_PowerDelivery_007.

Test objective: GoodCase to the PowerDelivery precondition; the Test System sends a PowerDeliveryReq with ChargeProgress=Start whose EVPowerProfile requests a power beyond the limit the SUT offered in ScheduleExchangeRes. Checks the SUT answers a PowerDeliveryRes carrying ResponseCode FAILED_EVPowerProfileInvalid. The EVPowerProfile is encoded on the wire. Only a Scheduled ScheduleExchangeRes carries a power limit ([V2G20-478], [V2G20-1559]; in Dynamic mode [V2G20-1070] makes the SECC accept any profile), so the GoodCase selects a Scheduled parameter set in ServiceSelection (the precondition fails if the SUT offers none).

DUT (dut) **FAIL** 7.20 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_EVPowerProfileInvalid – got 'OK'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_EVPowerProfileInvalid	got 'OK'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

E **AssertionError:** ResponseCode = FAILED_EVPowerProfileInvalid – got 'OK'

TC21_SECC_PowerDelivery_008

TC21_SECC_PowerDelivery_008.

Test objective: GoodCase to the PowerDelivery precondition (Scheduled control mode); the Test System sends a PowerDeliveryReq with ChargeProgress=Start and PowerToleranceAcceptance=PowerToleranceNotConfirmed. Checks the SUT answers either PowerDeliveryRes(FAILED_PowerToleranceNotConfirmed, EVSENotification Terminate) or PowerDeliveryRes(WARNING_PowerToleranceNotConfirmed, EVSENotification Renegotiation) within the message response window; the EVSEStatus's NotificationMaxDelay is recorded. The EVPowerProfile carrying the tolerance flag is encoded on the wire and stays within the offered PowerSchedule, so only the tolerance flag deviates from the default. The GoodCase selects a Scheduled parameter set in ServiceSelection (the precondition fails if the SUT offers none).

DUT (dut) **FAIL** 7.10 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode/EVSENotification = FAILED_PowerToleranceNotConfirmed/Terminate or WARNING_PowerToleranceNotConfirmed/Renegotiation – got 'OK'/None

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓

Conformance check	Observed	Result
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓
ResponseCode/EVSENotification = FAILED_PowerToleranceNotConfirmed/Terminate or WARNING_PowerToleranceNotConfirmed/ Renegotiation	got 'OK'/None	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.6 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

E **AssertionError:** ResponseCode/EVSENotification = FAILED_PowerToleranceNotConfirmed/Terminate
or WARNING_PowerToleranceNotConfirmed/Renegotiation – got 'OK'/None

TC21_SECC_PowerDelivery_009

TC21_SECC_PowerDelivery_009.

Test objective: GoodCase to the PowerDelivery precondition (DC_PreChargeRes on DC, ScheduleExchangeRes(Finished) on AC); the Test System then withholds the PowerDeliveryReq entirely. Checks the SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and the following TLS_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **FAIL** 15.90 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout – closed prematurely 9.0s after the PowerDelivery precondition, before V2G_SECC_Sequence_Timeout (60s)

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout	closed prematurely 9.0s after the PowerDelivery precondition, before V2G_SECC_Sequence_Timeout (60s)	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	9035.7 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

Failure detail (excerpt):

E `AssertionError: SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout – closed prematurely 9.0s after the PowerDelivery precondition, before V2G_SECC_Sequence_Timeout (60s)`

TC21_SECC_PowerDelivery_010

TC21_SECC_PowerDelivery_010.

Test objective: GoodCase through PowerDelivery(Start) and several ChargeLoop exchanges; the Test System then withholds the next PowerDeliveryReq entirely.

Checks the SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and the following TLS_Connection_Termination_Timeout. LONG TEST.

DUT (dut) **PASS** 72.29 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout	closed 63.8s after the last ChargeLoopRes	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.4 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	63757.2 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC21_SECC_PowerDelivery_011

TC21_SECC_PowerDelivery_011.

Test objective: GoodCase to the PowerDelivery precondition (Scheduled control mode); the Test System sends a PowerDeliveryReq(Start) whose EVPowerProfile Scheduled control mode names a SelectedScheduleTupleID that was not offered in ScheduleExchangeRes. Checks the SUT answers a PowerDeliveryRes carrying the tuple-selection failure ResponseCode. The EVPowerProfile is encoded on the wire. The GoodCase selects a Scheduled parameter set in ServiceSelection (the precondition fails if the SUT offers none).

DUT (dut) **FAIL** 7.70 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_ScheduleSelectionInvalid (ATS: FAILED_TariffSelectionInvalid, not schema-encodable) – got 'OK'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_ScheduleSelectionInvalid (ATS: FAILED_TariffSelectionInvalid, not schema-encodable)	got 'OK'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

```
E   AssertionError: ResponseCode = FAILED_ScheduleSelectionInvalid (ATS:
FAILED_TariffSelectionInvalid, not schema-encodable) - got 'OK'
```

TC21_SECC_PowerDelivery_012

TC21_SECC_PowerDelivery_012.

Test objective: as _011 -- GoodCase to the PowerDelivery precondition (Scheduled control mode), then a PowerDeliveryReq(Start) selecting a schedule tuple id that ScheduleExchangeRes never contained. Checks a PowerDeliveryRes carrying the tuple-selection failure ResponseCode (no EVSEStatus). The EVPowerProfile is encoded on the wire. The GoodCase selects a Scheduled parameter set in ServiceSelection (the precondition fails if the SUT offers none).

DUT (dut) **FAIL** 7.10 s

FAILURE REASON

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_ScheduleSelectionInvalid (ATS: FAILED_TariffSelectionInvalid, not schema-encodable) – got 'OK'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a PowerDeliveryRes message	got 'PowerDeliveryRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_ScheduleSelectionInvalid (ATS: FAILED_TariffSelectionInvalid, not schema-encodable)	got 'OK'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.3 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
PowerDeliveryRes response time	148.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

```
E  AssertionError: ResponseCode = FAILED_ScheduleSelectionInvalid (ATS:
FAILED_TariffSelectionInvalid, not schema-encodable) - got 'OK'
```

TC21_SECC_PowerDelivery_013

TC21_SECC_PowerDelivery_013.

Test objective: GoodCase to the PowerDelivery precondition; instead of the PowerDeliveryReq the Test System sends a SessionStopReq from the default parameter set (an EV-initiated shutdown for a non-critical reason). Checks the SUT answers a SessionStopRes carrying ResponseCode OK within the message response window.

DUT (dut) **FAIL** 7.10 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode = OK – got 'FAILED_SequenceError'

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = OK	got 'FAILED_SequenceError'	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	409.5 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	99.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

E **AssertionError:** ResponseCode = OK – got 'FAILED_SequenceError'

TC21_SECC_ChargeLoop_001

TC21_SECC_ChargeLoop_001.

Test objective: GoodCase up to PowerDeliveryRes(Start), i.e. inside the charge loop; the Test System then sends a valid ServiceDiscoveryReq in place of the expected (DC|AC)_ChargeLoopReq. Checks the SUT answers a ServiceDiscoveryRes carrying ResponseCode FAILED_SequenceError (and no Header signature) within the message response window.

DUT (dut) **PASS** 7.72 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.2 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	409.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
ServiceDiscoveryRes response time	99.9 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_ChargeLoop_002

TC21_SECC_ChargeLoop_002.

Test objective: GoodCase up to PowerDeliveryRes(Start), i.e. inside the charge loop; the Test System then withholds the (DC|AC)_ChargeLoopReq entirely. Checks the SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and the following TLS_Connection_Termination_Timeout.

LONG TEST.

DUT (dut) **PASS** 71.28 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and TLS_Connection_Termination_Timeout	closed 64.0s after PowerDeliveryRes(Start)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_ATTEN_CHAR.IND after sounding	408.6 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	64008.5 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC21_SECC_SessionStop_001

TC21_SECC_SessionStop_001.

Test objective: GoodCase up to the point a SessionStop is legal (DC: DC_WeldingDetectionRes Finished). The Test System sends a SessionStopReq built from the default parameter set (ChargingSession=Terminate). Checks a SessionStopRes is received within the message response window carrying ResponseCode OK.

DUT (dut) **PASS** 9.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓

Conformance check	Observed	Result
ResponseCode = OK	got 'OK'	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	1.3 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionStop_002

TC21_SECC_SessionStop_002.

Test objective: unknown-SessionID negative. GoodCase up to the point a SessionStop is legal (DC: DC_WeldingDetectionRes Finished); the Test System then sends a SessionStopReq (default parameter set, ChargingSession=Terminate) but stamps its header with a freshly generated SessionID the SUT never assigned. Checks the SUT answers a SessionStopRes within the message response window carrying ResponseCode FAILED_UnknownSession, with the response Header omitting the Signature.

DUT (dut) **PASS** 9.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_UnknownSession	got 'FAILED_UnknownSession'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.8 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	1.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionStop_003

TC21_SECC_SessionStop_003.

Test objective: GoodCase up to the point a SessionStop is legal; the Test System then sends a valid ServiceDiscoveryReq in place of the expected SessionStopReq. Checks the SUT answers a ServiceDiscoveryRes within the message response window, carrying ResponseCode FAILED_SequenceError and no Header signature.

DUT (dut) **PASS** 9.00 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a ServiceDiscoveryRes message	got 'ServiceDiscoveryRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_SequenceError	got 'FAILED_SequenceError'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.7 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info
ServiceDiscoveryRes response time	1.8 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionStop_004

TC21_SECC_SessionStop_004.

Test objective: GoodCase up to the point a SessionStop is legal; the Test System then withholds the SessionStopReq entirely and stays silent. Checks the SUT terminates the TLS connection between V2G_SECC_Sequence_Timeout and the following TLS connection termination timeout (i.e. it does not tear the connection down early, and does so within the sequence timeout plus the TLS termination budget). LONG TEST.

DUT (dut) **PASS** 72.89 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVERest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVERest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓

Conformance check	Observed	Result
SUT terminates the TLS connection within V2G_SECC_Sequence_Timeout + TLS_Connection_Termination_Timeout (66s) with no SessionStopReq	closed 63.7s after the final response	✓
SUT does not terminate before V2G_SECC_Sequence_Timeout expires (≥ 55 s)	closed after 63.7s	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.3 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	411.1 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
TCP connection close after failure/timeout	63728.1 ms	≤ 5000 ms (CMN_TCP_Connection_Termination_Timeout)	✗

TC21_SECC_SessionStop_005

TC21_SECC_SessionStop_005.

Test objective: GoodCase driving the full message flow for the selected charging mode through to SessionStop, with every request built from the default parameter set. Checks that the SessionID in the header of each received response equals the value the SUT assigned in the SessionSetupRes, for the entire session.

DUT (dut) **PASS** 9.21 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓

Conformance check	Observed	Result
every response echoes the SessionID assigned in SessionSetupRes	assigned 'a2625e91955f555d'; all responses matched	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.8 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.3 ms	-	info

TC21_SECC_SessionStop_006

TC21_SECC_SessionStop_006.

Test objective: GoodCase up to the point a SessionStop is legal, on an SUT that does not support service renegotiation. The Test System sends a SessionStopReq with ChargingSession=ServiceRenegotiation. Checks the SUT answers a SessionStopRes within the message response window carrying ResponseCode FAILED_NoServiceRenegotiationSupported and no Header signature.

DUT (dut) **PASS** 8.90 s

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓

Conformance check	Observed	Result
ResponseCode = FAILED_NoServiceRenegotiationSupported	got 'FAILED_NoServiceRenegotiationSupported'	✓
response Header carries no Signature	None	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	1.1 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.7 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	1.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

TC21_SECC_SessionStop_007

TC21_SECC_SessionStop_007.

Test objective: GoodCase up to the point a SessionStop is legal, under a dynamic control mode, with the SUT never having signalled EVSENotification=Pause. The Test System sends a SessionStopReq with ChargingSession=Pause. Checks the SUT answers a SessionStopRes within the message response window carrying ResponseCode FAILED_PauseNotAllowed and no Header signature.

DUT (dut) **FAIL** 9.00 s**FAILURE REASON**

harness/test_ev.py:378

AssertionError: ResponseCode = FAILED_PauseNotAllowed – got 'OK' (control mode 'Dynamic')

Conformance check	Observed	Result
TLS protocol version = TLSv1.3 [V2G20-2365]	negotiated TLSv1.3	✓
TLS ciphersuite in ISO 15118-20 Table 6 [V2G20-2458]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS ciphersuite = TLS_AES_256_GCM_SHA384 (most preferred offered suite) [V2G20-1857]	negotiated TLS_AES_256_GCM_SHA384	✓
TLS key share named group = secp521r1 (Table 7) [V2G20-1634]	client key_share pinned; handshake completed	✓
SECC certificate key on secp521r1 (ISO 15118-20 Annex B.4, [V2G20-2674] curve)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: key curve secp521r1	✓
SECC certificate signed with ECDSA-SHA512 (ISO 15118-20 Annex B.4)	DC=CPO,C=DE,O=EVerest,CN=SECCCert: signature digest sha512	✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
SUT sends a SessionStopRes message	got 'SessionStopRes'	✓
ResponseCode = FAILED_PauseNotAllowed	got 'OK' (control mode 'Dynamic')	✗

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.0 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
SessionStopRes response time	1.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Failure detail (excerpt):

E **AssertionError:** ResponseCode = FAILED_PauseNotAllowed – got 'OK' (control mode 'Dynamic')

Test case details — PIONIX interop testing (vendor-defined)

TC_SECC_AC_VTB_PionixInterop_005

TC_SECC_AC_VTB_PionixInterop_005.

Test objective: Interop; AC twin of the DC session-setup timing TC. The Test System runs a complete AC ISO 15118-2 session (eIM, TLS off) up to and including PowerDelivery(Start) and measures the EVSE response time of EVERY exchange before the ChargingStatus loop: supportedAppProtocol, SessionSetup, ServiceDiscovery, PaymentServiceSelection, Authorization, ChargeParameterDiscovery (AC energy transfer mode; no CableCheck/PreCharge on AC) and PowerDelivery -- polled messages contribute one sample per poll. The measurement starts with the supportedAppProtocol handshake: the preceding SLAC matching is a precondition only and expressly NOT measured. Requests are timestamped at V2GTP frame send, responses at V2GTP frame arrival. Checks per message: the minimum shall be ≥ 90 ms (PIONIX interop requirement) and the maximum $\leq$ the standard's per-message limit V2G_SECC_Msg_Performance_Time (ISO 15118-2 Table 109: 1.5 s, resp. 4.5 s for PowerDeliveryRes). Per-message min/max are recorded; on failure every violating exchange is named exactly (message + sample number) with whether it came too quickly or took too long.

DUT (dut) **PASS** 11.20 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Every AC session-setup response time within bounds (min 90 ms / Table 109 max per message)	all exchanges within bounds	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.9 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.4 ms	≤ 200 ms (TT_match_response)	✓
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.5 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.2 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Measurement	Measured	Target / range	Result
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.2 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
V2G exchanges measured up to PowerDelivery(Start)	8	-	info
AuthorizationRes response time (min of 2)	100.2 ms	≥ 90.0 ms	✓
AuthorizationRes response time (max of 2)	100.4 ms	≤ 1500.0 ms	✓
ChargeParameterDiscoveryRes response time (min of 1)	100.3 ms	≥ 90.0 ms	✓
ChargeParameterDiscoveryRes response time (max of 1)	100.3 ms	≤ 1500.0 ms	✓
PaymentServiceSelectionRes response time (min of 1)	100.3 ms	≥ 90.0 ms	✓
PaymentServiceSelectionRes response time (max of 1)	100.3 ms	≤ 1500.0 ms	✓
PowerDeliveryRes response time (min of 1)	100.3 ms	≥ 90.0 ms	✓
PowerDeliveryRes response time (max of 1)	100.3 ms	≤ 4500.0 ms	✓
ServiceDiscoveryRes response time (min of 1)	100.3 ms	≥ 90.0 ms	✓
ServiceDiscoveryRes response time (max of 1)	100.3 ms	≤ 1500.0 ms	✓
SessionSetupRes response time (min of 1)	100.4 ms	≥ 90.0 ms	✓
SessionSetupRes response time (max of 1)	100.4 ms	≤ 1500.0 ms	✓
supportedAppProtocolRes response time (min of 1)	100.5 ms	≥ 90.0 ms	✓
supportedAppProtocolRes response time (max of 1)	100.5 ms	≤ 1500.0 ms	✓
PowerDeliveryRes(Stop) response time	101.0 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓

TC_SECC_AC_VTB_PionixInterop_006

TC_SECC_AC_VTB_PionixInterop_006.

Test objective: Interop; AC twin of the DC CurrentDemand-loop timing TC.

The Test System runs a complete AC ISO 15118-2 charging session (eIM, plain TCP only: no-transport-security SDP request, the Test System never initiates TLS even on a TLS-capable DUT) into the AC charge loop (PowerDelivery(Start) done, contactors closed), then holds the loop for 10 minutes, sending a ChargingStatusReq (the AC analogue of CurrentDemandReq) every 250 ms. Every exchange is timestamped on the wire: request at V2GTP frame send, response at V2GTP frame arrival. Checks every ChargingStatusRes is OK, then the aggregate response times: the minimum shall be ≥ 90 ms and the maximum ≤ 120 ms (PIONIX interop requirement, not a normative ISO 15118 limit -- Table 109 would allow 1.5 s); the average is informational. The session is then ended cleanly (PowerDelivery(Stop), CP B, SessionStop(Terminate)), each with ResponseCode OK.

DUT (dut) **PASS** 608.65 s

Conformance check	Observed	Result
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
Response echoes the current SessionID		✓
PowerDeliveryRes(Stop) after the 10-min loop = OK	got 'OK'	✓
Response echoes the current SessionID		✓
SessionStopRes after the 10-min loop = OK	got 'OK'	✓
ChargingStatus response time min ≥ 90 ms (PIONIX interop requirement)	min 100.5 ms (1705 exchanges, avg 100.9 ms, max 102.1 ms)	✓
ChargingStatus response time max ≤ 120 ms (PIONIX interop requirement)	max 102.1 ms (1705 exchanges, min 100.5 ms, avg 100.9 ms)	✓

Measurement	Measured	Target / range	Result
CM_SLAC_PARM.CNF response time	0.6 ms	≤ 200 ms (TT_match_response)	✓
CM_ATTEN_CHAR.IND after sounding	410.2 ms	≤ 1200 ms (TT_EV_atten_results)	✓
CM_SLAC_MATCH.CNF response time	0.5 ms	≤ 200 ms (TT_match_response)	✓

Measurement	Measured	Target / range	Result
CM_SET_KEY.CNF response time	0.2 ms	-	info
supportedAppProtocolRes response time	100.4 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
SessionSetupRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
ServiceDiscoveryRes response time	101.1 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PaymentServiceSelectionRes response time	101.0 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓
PowerDeliveryRes(Start) response time	101.1 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
ChargingStatus exchanges (10 min loop)	1705	-	info
ChargingStatus response time (min)	100.5 ms	≥ 90.0 ms	✓
ChargingStatus response time (avg)	100.9 ms	-	info
ChargingStatus response time (max)	102.1 ms	≤ 120.0 ms	✓
PowerDeliveryRes(Stop) response time	101.7 ms	V2G_SECC_Sequence_Performance_Time (informational)	✓
SessionStopRes response time	101.7 ms	≤ 2000 ms (V2G_EVCC_Msg_Timeout)	✓

Appendix

Codec self-tests

No codec self-tests were included in this run.

Toolchain / report metadata

pytest version	unknown
Report created	2026-10-11 07:58:37
pytest exit code	1
Report generator	Pionix conformance tester report generator
Generation timestamp	2026-10-11 07:59:37