Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC179	TELE, 5G, GOVERNANCE AND RISK MANAGEMENT, GOVERNANCE AND RISK MANAGEMENT, MULTI ACCESS EDGE COMPUTING, Virtualization Infrastructure, Virtual Infrastructure Manager (VIM)	Færdig	Extensive assessment of virtualization-related vulnerabilities for MEC components	Extensive assessment of virtualization-related vulnerabilities for MEC components EVIDENCE Documentation of MEC components lists potential vulnerabilities relating to using MEC components in virtualized environments, along with appropriate measures to ensure their secure deployment/operation	a) Make a list of the main risks for security of networks and services, taking into account main threats for the critical assets		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
TC183	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PHYSICAL AND ENVIRONMENTAL SECURITY, MULTI ACCESS EDGE COMPUTING, MEC host	Færdig	Physical security measures such as earthquake-proofing, fire control, secure perimeter, automatic alerts, and remote monitoring are used for edge computing facilities	Physical security measures such as earthquake-proofing, fire control, secure perimeter, automatic alerts, and remote monitoring are used for edge computing facilities EVIDENCE Verify implementation of physical security measures listed in the 'Control' section by checking building certifications, performing onsite inspections, etc.	a) Prevent unauthorized physical access to facilities and infrastructure and set up adequate environmental controls, to protect provider assets (including third party assets, where applicable) against unauthorized access, burglary, fire, flooding, etc. Security controls should be selected based on the risk assessment, which should also take in consideration current and forecasted environmental security risks – e.g. related to climate change		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. TEL 11.1.8/TEL 11.3 ITU-T X.1205
TC207	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PHYSICAL AND ENVIRONMENTAL SECURITY, PHYSICAL INFRASTRUCTURE SECURITY, Physical asset, Cloud data center, Light data center	Færdig	Physical security of communication centers, equipment rooms, and physically isolated operation areas is designed, developed and applied	Physical security of communication centers, equipment rooms, and physically isolated operation areas is designed, developed and applied EVIDENCE Statement of Applicability (SoA) or equivalent record which lists the relevant physical security controls and how they were implemented. Documented physical security-specific policy/policies, which include physical access control, monitoring, continuity of operations and protection against environmental disasters. Such policy/policies list critical assets and their respective controls. Relevant documented procedures, for example covering physical access. On-site inspection to verify implementation of the relevant controls	c) Industry standard implementation of physical and environmental controls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. TEL 11.1.7, TEL 11.1.8, TEL 11.1.9, TEL 11.2.1, TEL 11.3 ITU-T X.1205
TC214	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PHYSICAL AND ENVIRONMENTAL SECURITY, PHYSICAL INFRASTRUCTURE SECURITY, Hardware	Færdig	Protection against side-channel vulnerabilities should be deployed for critical systems	Protection against side-channel vulnerabilities should be deployed for critical systems EVIDENCE Inspection of critical systems confirms that TEMPEST standard guidelines such as equipment distance from walls, amount of shielding in buildings and equipment, and distance separating wires carrying classified information from those carrying unclassified are followed	c) Industry standard implementation of physical and environmental controls		Protect	Fortrolighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC215	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PHYSICAL AND ENVIRONMENTAL SECURITY, PHYSICAL INFRASTRUCTURE SECURITY, Hardware	Færdig	Hardware backdoors, when detected, are removed	Hardware backdoors, when detected, are removed EVIDENCE Visual inspection of the equipment does not reveal any suspicious peripherals or hardware backdoors. Documented processes are in place for obtaining and flashing a BIOS if a hardware backdoor is suspected	c) Industry standard implementation of physical and environmental controls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC209	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, SECURITY OF SUPPLIES, PHYSICAL INFRASTRUCTURE SECURITY, Physical asset	Færdig	Power supply continuity strategy that avoids a single point of supply failure	Power supply continuity strategy that avoids a single point of supply failure EVIDENCE Check for the presence of multiple power supply sources which are capable of withstanding primary power supply failures for the duration of likely outages. Where necessary, batteries are augmented with private electric generators. Additionally, documented business continuity and incident management plans and/or processes with provisions on power supply continuity, including responding to outages	a) Ensure security of critical supplies		Protect	Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. 11.2.2
TC216	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, SECURITY OF SUPPLIES, PHYSICAL INFRASTRUCTURE SECURITY, Hardware	Færdig	Protection against semiconductor doping	Protection against semiconductor doping EVIDENCE Product documentation contains information on certification of semiconductors and their suppliers for compliance with standards such as ISO 26262	c) Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.)		Protect	Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC218	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, SECURITY OF SUPPLIES, PHYSICAL INFRASTRUCTURE SECURITY, Hardware	Færdig	Prevent TPM-Fail vulnerabilities	Prevent TPM-Fail vulnerabilities EVIDENCE Verify product documentation to ensure that the TPM hardware used in the product is certified, for example, by the Trusted Computing Group (TCG)	c) Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.)		Protect	Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC004	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, gNB, AMF	Færdig	AMFs verify that the UE's 5G security capabilities received from the target gNB match with locally stored values	AMFs verify that the UE's 5G security capabilities received from the target gNB match with locally stored values. If there is a mismatch, the AMFs send their locally stored 5G security capabilities of the UE to the target gNB for preventing bidding down on Xn-handover EVIDENCE When UE sends different security capabilities from the ones stored in the AMF, packet captures containing the Path-Switch Acknowledge message sent by AMF to target gNB include locally stored security capabilities and not the ones sent by UE. The mismatch between locally stored security capabilities and those sent by UE is shown in the AMF log	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3/5.5/6.7.3.1 3GPP TS 33.511, cl. 4.2.2.1.14 3GPP TS 33.512, cl. 4.2.2.4.1
TC009	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AMF/SEAF, AUSF	Færdig	SEAF handles failures of primary authentication	SEAF handles failures of primary authentication. Namely, if the verification of HRES* fails at SEAF or verification of RES* fails at AUSF, then the SEAF either initiates an identification procedure with the UE if the 5G-GUTI was used by the UE to retrieve the SUCI, or it sends an authentication failure message to the UE EVIDENCE Upon receiving an incorrect RES* from UE, logs of the SEAF/AMF show that the authentication is rejected with an Authentication Reject message to the UE, or logs of the SEAF/AMF show that that the SEAF/AMF has initiated an identification procedure with the UE to retrieve the SUCI	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.6/6.1.3.2 3GPP TS 33.512, cl. 4.2.2.1.2
TC010	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AUSF	Færdig	AUSFs should implement Nausf_UEAuthentication service in accordance with the 3GPP technical specification	AUSFs should implement Nausf_UEAuthentication service in accordance with 3GPP technical specification 33.501, clause 14.1 EVIDENCE Verify that i) sending SUPI or SUCI with serving network name to the Nausf_UEAuthentication service results in the service returning a 5G AKA authentication vector or an EAP-AKA' packet. ii) sending 5G AKA authentication confirmation message or EAP-AKA' message to the Nausf_UEAuthentication service results in the service returning the authentication result and a master key if authentication was successful	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.1
TC013	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AMF/SEAF, UDM	Færdig	Correct implementation of synchronisation failure handling	Upon receiving an authentication failure message with synchronization failure (AUTS) from the UE, the SEAF sends a synchronization failure indication to the AUSF and does not send new authentication requests to the UE until it has received a response EVIDENCE Sending unsolicited "synchronization failure indication" messages from UE have no effect on the SEAF. If authentication failure with synchronization failure message is received by the SEAF, then access logs of the SEAF show that it does not send new authentication requests before having received the response to its Nausf_UEAuthentication_Authenticate Request message with a "synchronization failure indication" from the AUSF (or before it is timed out)	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.1.3.3 3GPP TS 33.512, cl. 4.2.2.1.1 3GPP TS 33.514, cl. 4.2.2.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC014	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, UPF, SMF	Færdig	UPF (or SMF depending on operator) assigns unique tunnel endpoint IDs (TEIDs) for each PDU session while ensuring that TEID is unique within one IP address	UPF (or SMF depending on operator) assigns unique tunnel endpoint IDs (TEIDs) for each PDU session while ensuring that TEID is unique within one IP address EVIDENCE Packet captures at UPF (or SMF) show unique F-TEIDs	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 23.060, cl. 14.6 3GPP TS 29.281, cl. 5.1 3GPP TS 23.501, cl. 5.8.2.3.1 3GPP TS 33.501, cl. 5.8 3GPP TS 33.513, cl. 4.2.2.6
TC019	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, UDM	Færdig	UDMs should implement Nudm_UEAuthentication_Get service in accordance with the 3GPP technical specification	UDMs should implement Nudm_UEAuthentication_Get service in accordance with 3GPP technical specification 33.501, clause 14.2 EVIDENCE Verify that the Nudm_UEAuthentication_Get service responds with the authentication method and corresponding data on sending the SUPI/SUCI along with the serving network name	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.2
TC020	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, UDM	Færdig	UDMs should implement Nudm_UEAuthentication_ResultConfirmation service in accordance with the 3GPP technical specification	UDMs should implement Nudm_UEAuthentication_ResultConfirmation service in accordance with 3GPP technical specification 33.501, clause 14.2 EVIDENCE Verify that UDM access logs contain information such as SUPI, timestamp of the authentication, the authentication type, and serving network name sent to the Nudm_UEAuthentication_ReultConfirmation service of the UDM	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.2
TC021	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SMF	Færdig	SMF assigns unique charging IDs for each PDU session	SMF assigns unique charging IDs for each PDU session EVIDENCE System logs of the SMF show that it generates a unique charging ID for each new PDU session and uses it for all subsequent messages for that PDU session	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 32.255, cl. 5.1 3GPP TS 33.515, cl. 4.2.2.1.4
TC022	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SMF	Færdig	SMF gives priority to security policy from UDM over locally configured policy	SMF gives priority to security policy from UDM over locally configured policy EVIDENCE Capture of the Namf_Communication_N1N2MessageTsent from the SMF to the AMF includes the user plane security policy configured in the UDM and not the one configured locally in the SMF	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 23.501, cl. 5.10.3 3GPP TS 33.515, cl. 4.2.2.1.1
TC023	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SMF	Færdig	SMF sends locally stored user plane security policy to the gNB/ng-eNB when there is a mismatch in the policy received from the radio network gNB/ng-eNB	SMF sends locally stored user plane security policy to the gNB/ng-eNB when there is a mismatch in the policy received from the radio network gNB/ng-eNB EVIDENCE Capture of the Nsmf_PDUSession_SMContextUpdate Response message sent from the SMF contains the locally stored UE security policy in the n2SmInf IE	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.6.1 3GPP TS 33.515, cl. 4.2.2.1.3
TC027	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	Mutual authentication and cipher suite negotiation between SEPPs in roaming network	Mutual authentication and cipher suite negotiation between SEPPs in roaming network EVIDENCE Packet captures on the N32-f interface of the SEPP show that security parameter exchange request and response messages are used for negotiating the ciphersuites	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.3.2/13.2.2.2/13.5
TC028	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	SEPPs are able to identify mismatch between the PLMN-ID contained in the incoming N32-f message and the PLMN-ID in the related N32-f context, and send appropriate error code on mismatch	SEPPs are able to identify mismatch between the PLMN-ID contained in the incoming N32-f message and the PLMN-ID in the related N32-f context, and send appropriate error code on mismatch EVIDENCE Packet captures at the SEPP show that an error signaling message containing the N32-f Message Id and error code is sent to the peer SEPP if the PLMN-ID in the incoming N32 message from the peer SEPP does not match the peer PLMN ID in the N32-f peer information in the N32-f context	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.2.4.7 3GPP TS 33.517, cl. 4.2.2.4
TC029	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	Ensure correct implementation of handling of serving PLMN ID mismatch	pSEPP checks that the serving PLMN-ID of subject claim in the access token matches the remote PLMN-ID corresponding to the N32-f context Id in the N32 message EVIDENCE Packet captures and logs of the SEPP show that an error signaling message containing the N32-f Message Id and error code is sent to the peer SEPP if the PLMN-ID appended in the subject claim of the access token received is different from PLMN-ID of the peer SEPP in the N32-f content Id	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.4.1.2 3GPP TS 33.517, cl. 4.2.2.4
TC031	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	Ensure correct implementation of handling for protection policies mismatch	SEPPs identify a mismatch between the protection policies manually configured for a specific roaming partner and an IPX provider and the protection policies received on an N32-c connection, and send an error message on mismatch EVIDENCE Logs and packet captures of a SEPP show that sending a Security Parameter Exchange Request message to a peer SEPP containing a data-type encryption policy and modification policy different from what is configured locally on the peer SEPP results in an error message on the N32-c connection	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.2.3.6 3GPP TS 33.517, cl. 4.2.2.6
TC035	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	Prevent misplacement of encrypted IEs in JSON object by IPX	SEPPs ensure that intermediate IPX don't misplace (move or copy) encrypted IE to a different location in a JSON object that would be reflected from the producer NF for an IE without encryption EVIDENCE Logs and packet captures of a SEPP confirm that an N32-f message is discarded if an encrypted IE is moved to a cleartext IE	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.2.4.1 3GPP TS 33.517, cl. 4.2.2.8
TC036	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NRF	Færdig	NRFs authorize discovery requests from network functions based on the profile of the expected function/service and the type of the service consumer	NRFs authorize discovery requests from network functions based on the profile of the expected function/service and the type of the service consumer. If the expected function/service is deployed in a different network slice, NRF authorizes the discovery request according to the configuration of that slice. Example of such policy configuration could be that certain function/service instances are not discoverable from other network slices EVIDENCE NRF access logs and packet captures on the NRF confirm that an NRF returns a response with "403 Forbidden" status code if the requested NF instance does not allow discovery from other slices	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 23.502, cl. 4.17.4 3GPP TS 33.501, cl. 5.9.2.1 3GPP TS 33.518, cl. 4.2.2.2.1
TC037	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NRF	Færdig	NRFs should implement Nnrf_AccessToken_Get service in accordance with the 3GPP technical specification	NRFs should implement Nnrf_AccessToken_Get service in accordance with 3GPP technical specification 33.501, clause 14.3 EVIDENCE Verify that a test NF service consumer can receive an access token with appropriate claims from the Nnrf_AccessToken_Get service by sending it a request with its NF Instance Id, requested "scope", and optional information	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.3

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC038	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NEF	Færdig	Mutual authentication between the NEFs and application functions is based on certificates or pre-shared keys	Mutual authentication between the NEFs and application functions is based on certificates or pre-shared keys. When an application function resides outside the 3GPP operator domain, mutual authentication is only based on client and server certificates with TLS EVIDENCE Verification of successful TLS tunnel setup between NEF and application functions	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.2.3/12.2/12.3 3GPP TS 33.519, cl. 4.2.2.1.1
TC039	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NEF	Færdig	Internal 5G core information such as SUPI, DNN, S-NSSAI is not disclosed by NEF to application functions residing outside the operator domain	Internal 5G core information such as SUPI, DNN, S-NSSAI is not disclosed by NEF to application functions residing outside the operator domain EVIDENCE Packet captures of interaction between NEF and application functions outside operator domain do not contain any 5G core information	f) Reinforce controls for remote access to critical assets of network and information systems by third parties		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.2.3
TC040	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NEF	Færdig	NEFs authorize requests from application functions using standard Oauth	NEFs authorize requests from application functions using standard OAuth as profiled in 3GPP TS 33.501 EVIDENCE Verification that invocation of NEF northbound APIs with valid OAuth tokens is successful	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.2.3/12.4/13.4 3GPP TS 33.519, cl. 4.2.2.1.1
TC050	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	When not under maintenance, local or remote system functions such as OAM CLI/GUI should not reveal confidential system internal data in the clear to users and administrators	When not under maintenance, local or remote system functions such as OAM CLI/GUI should not reveal confidential system internal data in the clear to users and administrators. Confidential system internal data includes authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as other system internal data such as stack traces in error messages EVIDENCE Verify that system functions as described in the product documentation (e.g. local or remote OAM CLI or GUI, logging messages, alarms, error messages, configuration file exports, stack traces) do not reveal any confidential system internal data in the clear (for example, passphrases)	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.2 3GPP TS 33.216 3GPP TS 33.511-519
TC051	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Sensitive data in persistent/temporary storage has restricted access and files are protected against manipulation	Sensitive data in persistent/temporary storage has restricted access and files are protected against manipulation EVIDENCE Verification that records of sensitive data such as passwords are not stored directly and, instead, they are scrambled with a one-way hash function	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.3 3GPP TS 33.216 3GPP TS 33.511-519
TC059	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	Færdig	System functions are not to be used without successful authentication and authorization	System functions are not to be used without successful authentication and authorization EVIDENCE Verify that attempts to access a system function are only successful when logged in as a user with adequate privileges	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.1.1 3GPP TS 33.216 3GPP TS 33.511-519
TC060	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	Færdig	Users are identified unambiguously by the network product using a user name and an authentication attribute (user could be a person, machine, application or a system)	Users are identified unambiguously by the network product using a user name and an authentication attribute (user could be a person, machine, application or a system). Network products support individual accounts per user and don't enable the use of group accounts, group credentials or sharing of accounts between several users EVIDENCE Documented user access policy shows that group accounts, credentials, and sharing of the same accounts are forbidden. Tests show that the network product does not support credentials unrelated to an account	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.1.2/4.2.3.4.2.1 3GPP TS 33.216 3GPP TS 33.511-519
TC063	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, PHYSICAL INFRASTRUCTURE SECURITY, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	Færdig	Mutual authentication of entities for management interfaces	Mutual authentication of entities for management interfaces EVIDENCE Network product documentation contains a list of management protocols and a corresponding list of authentication mechanisms used by each management protocol. Packet captures of each management protocol confirm successful mutual authentication before allowing access	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.4.1 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC064	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, PSF, ISF, VSF, LCM proxy, MEC orchestrator, EPC+ functions	Færdig	Authorizations for accounts, files, and applications is reduced to the minimum required for the tasks they have to perform	Authorizations for accounts, files, and applications is reduced to the minimum required for the tasks they have to perform. Execution of applications and components shall also take place with rights that are as limited as possible EVIDENCE Documentation of the network product describes an authorization policy which includes details on the lowest access rights assigned to user accounts and applications. Verify that files and applications are not accessible without adequate privileges necessitated by the authorization policy	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.6 3GPP TS 33.216 3GPP TS 33.511-519
TC065	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network functions/products allow signed in users to logout at any time	Network functions/products allow signed in users to logout at any time. All processes under the logged in user ID are terminated on log out. Network function/product is able to continue operation without interactive sessions. OAM user interactive session are terminated automatically after a specified configurable period of inactivity EVIDENCE Verification of successful login and logout with a new account or an existing account. Verification that OAM user sessions are terminated automatically after a predefined configurable amount of time	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117 4.2.3.5 3GPP TS 33.216 3GPP TS 33.511-519
TC072	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Privilege escalation in interactive sessions (CLI or GUI) of a network product is not allowed without re-authentication	Privilege escalation in interactive sessions (CLI or GUI) of a network product is not allowed without re-authentication EVIDENCE Verify that commands such as 'su' which enable a user or function to gain administrator/root privileges from another user account require re-authentication	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.2.1 3GPP TS 33.216 3GPP TS 33.511-519
TC073	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	System accounts in UNIX (and derivatives like LINUX) have unique UIDs	System accounts in UNIX (and derivatives like LINUX) have unique UIDs EVIDENCE Verify that UIDs in the operating system of the network product are all unique and, in particular, only the root account has UID = 0	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.2.2 3GPP TS 33.216 3GPP TS 33.511-519
TC076	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Session ID is unpredictable	Session ID is unpredictable. It uniquely identifies the user and distinguishes the session from all other active sessions. Session ID does not contain sensitive information in clear text EVIDENCE After logging in repeatedly with different user IDs and a number of times with the same user ID, the logs of the network product show that Session IDs are random and are different between sessions of the same and different users	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
TC077	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product only accepts server generated session IDs and does not accept session identifiers from GET/POST variables	Network product only accepts server generated session IDs and does not accept session identifiers from GET/POST variables EVIDENCE Verify that retrieving a session ID and using it to access an existing session through a POST or GET results in a failure. Generating a session ID on the client and attempting to login to a network product results in a failure	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
TC078	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product automatically terminate sessions after a configurable maximum lifetime	Network product automatically terminate sessions after a configurable maximum lifetime. When the maximum lifetime expires, the session is closed, the session ID is deleted, and the user is forced to (re)authenticate to establish a new session. Default value for this maximum lifetime should be set to 8 hours EVIDENCE Verify that it is not possible to keep a session alive for longer than the configured maximum lifetime documented in the network product documentation (default should be 8 hours)	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC079	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product does not use persistent cookies to manage sessions and only uses session cookies	Network product does not use persistent cookies to manage sessions and only uses session cookies. In session cookies: neither the "expire" nor the "max-age" attribute is set; attribute 'HttpOnly' is set to true; 'domain' attribute is set to ensure that the cookie can only be sent to the specified domain; and 'path' attribute is set to ensure that the cookie can only be sent to the specified directory or sub-directory EVIDENCE Verify that, after logging in repeatedly with different user IDs and a number of times with the same user ID, the cookies received in different user sessions have the following properties: neither the "expire" nor the "max-age" attribute is set; attribute 'HttpOnly' is set to true; 'domain' attribute is set; and 'path' attribute is set	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
TC086	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product restricts the reachability of services so that they can only be reached on interfaces where their usage is required	Network product restricts the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces where services are active, the reachability is limited to legitimate peers. This limitation shall be realized on the network product itself (without measures (e.g. firewall) at network side) EVIDENCE Services can be configured on a per-interface basis. Running a network port scanner (e.g. nmap) reveals that services are only active on the interface where they are needed	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.2 3GPP TS 33.216 3GPP TS 33.511-519
TC090	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Direct login as root or equivalent highest privileged user is limited to the system console only	Direct login as root or equivalent highest privileged user is limited to the system console only. Root user will not be allowed to login to the system remotely EVIDENCE Verify that attempts to remotely login to the network product using the credentials of the root or equivalent highest privileged user results in failure. Login to the network product using the credentials of the root or equivalent highest privileged user from the physical console is successful	f) Reinforce controls for remote access to critical assets of network and information systems by third parties		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.6 3GPP TS 33.216 3GPP TS 33.511-519
TC091	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so	Only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so. In Unix® systems, the 'sticky' bit can be set on all directories where all users have write permissions EVIDENCE Verify that modifying files and directories for which the user has the necessary privileges is successful while attempts to modify the files and directories for which the user doesn't have the necessary privileges results in failure	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.7 3GPP TS 33.216 3GPP TS 33.511-519
TC097	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	If normal users are allowed to mount external file systems (locally or via the network), OS-level restrictions should be set properly to prevent privilege escalation or extended access permissions	If normal users are allowed to mount external file systems (locally or via the network), OS-level restrictions should be set properly to prevent privilege escalation or extended access permissions EVIDENCE For Linux® systems: verify that nodev and nosuid options are set in /etc/fstab for all filesystems which have the "user" option. For all operating systems: verify that attempts to gain privileged access by using the contents of a mounted file system are unsuccessful	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.6 3GPP TS 33.216 3GPP TS 33.511-519
TC115	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SMF	Færdig	Extensible Authentication Protocol (EAP) framework is used for secondary authentication	Extensible Authentication Protocol (EAP) framework is used for secondary authentication EVIDENCE Authentication attempt to an external data network with an EAP authentication method (and the corresponding credentials) is successful	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl.11.1
TC118	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, SEAF, AUSF, UDM	Færdig	Mutual authentication between the UE and network using EAP-AKA' and 5G AKA should be supported	Mutual authentication between the UE and network using EAP-AKA' and 5G AKA should be supported EVIDENCE Verify that a test UE device with SIM credentials from an operator can successfully authenticate with EAP-AKA' and 5G AKA. Packet captures of core network nodes SEAF, AUSF, UDM confirm successful authentication of the test UE device	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.1/Annex F
TC119	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, N3IWF, AMF, TNAN	Færdig	Authentication via trusted and untrusted non-3GPP access is performed with vendor-specific EAP method "EAP-5G" in accordance with the 3GPP technical specification	Authentication via trusted and untrusted non-3GPP access is performed with vendor-specific EAP method "EAP-5G" in accordance with 3GPP technical specification 33.501, clauses 7.2 and 7A EVIDENCE Verify that a test UE device with SIM credentials from an operator can successfully authenticate and use operator services when connecting via trusted and untrusted non-3GPP access networks. For untrusted non-3GPP access, packet captures at the N3IWF confirm successful authentication with EAP-5G. For trusted non-3GPP access, packet captures at the TNAN confirm successful authentication with EAP-5G	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 7.2/7A
TC124	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CoRE NETWORK, RADIO NETWORK, AMF, gNB	Færdig	Network should support authenticated and unauthenticated IMS Emergency Sessions in accordance with the 3GPP technical specification	Network should support authenticated and unauthenticated IMS Emergency Sessions in accordance with 3GPP technical specification 33.501, clause 10.2 EVIDENCE Verify that a test UE device can obtain emergency bearer services with authentication and without authentication. Packet captures on the AMF confirm successful emergency bearer service establishment for the test UE with or without authentication	e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 10.2

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC125	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NSSAAF	Færdig	NSSAAF should implement Nnssaaf_NSSAA_Authenticate service in accordance with the 3GPP technical specification	NSSAAF should implement Nnssaaf_NSSAA_Authenticate service in accordance with 3GPP technical specification 33.501, clause 14.4.1.2 EVIDENCE Verify via packet captures that sending an EAP identity response or an EAP response together with the GPSI and S-NSSAI to the Nnssaaf_NSSAA_Authenticate service results in the service i) forwarding the EAP message to the AAA-S handling the network slice specific authentication for the requested S-NSSAI and ii) returning the EAP message received from the AAA-S in response to the message forwarded earlier	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.4
TC126	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NSSAAF	Færdig	NSSAAF should implement Nnssaaf_NSSAA_Re-AuthenticationNotification service in accordance with the 3GPP technical specification	NSSAAF should implement Nnssaaf_NSSAA_Re-AuthenticationNotification service in accordance with 3GPP technical specification 33.501, clause 14.4.1.3 EVIDENCE Verify via packet captures on the AMF that a UE is re-authenticated when the NSSAAF triggers a network slice specific re-authentication procedure via the Nnssaaf_NSSAA_Re-AuthenticationNotification service	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.4
TC127	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, NSSAAF	Færdig	NSSAAF should implement Nnssaaf_NSSAA_RevocationNotification service in accordance with the 3GPP technical specification	NSSAAF should implement Nnssaaf_NSSAA_RevocationNotification service in accordance with 3GPP technical specification 33.501, clause 14.4.1.4 EVIDENCE Verify via packet captures on the AMF that a UE cannot access an S-NSSAI once the NSSAAF triggers a network slice specific revocation procedure via the Nnssaaf_NSSAA_RevocationNotification service	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.4
TC130	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, RADIO NETWORK, gNB	Færdig	Network should ensure security for UEs simultaneously connected to more than one NG-RAN node	Network should ensure security for UEs simultaneously connected to more than one NG-RAN node in accordance with 3GPP technical specification 33.501, clause 6.10 EVIDENCE Verify that MN can establish and modify security context between a test UE and SN. Packet captures at both the MN and SN confirm confidentiality, integrity, and replay protection	e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.10
TC135	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Service Based Interfaces, Os-Ma-Nfvo	Færdig	Slice management interface is accessed only by authorized communication service customers	Slice management interface is accessed only by authorized communication service customers EVIDENCE Verification that attempts to access network management slicing interfaces are only successful after authenticating with authorized accounts	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.1.1
TC141	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Network Slice Instance	Færdig	Access to the network management interface is authorized using OAuth 2.0	Access to the network management interface is authorized using OAuth 2.0 EVIDENCE Verification that the network management interface is accessible only with valid OAuth tokens	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.4.1
TC142	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Network Slice Instance	Færdig	Network slice should perform access authentication and authorization in addition to primary authentication used for 3GPP access	Network slice should perform access authentication and authorization in addition to primary authentication used for 3GPP access. This additional access authentication and authorization should use credentials other than those used for the primary authentication EVIDENCE Verify that access to a slice and its services is not possible without successful slice specific authentication	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.813, cl. 6.2
TC149	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, Control Plane	Færdig	Network functions (NFs) only communicate with other Network functions (NFs) for which they are specifically authorized	Network functions (NFs) only communicate with other Network functions (NFs) for which they are specifically authorized. The rules are applied irrespective of whether a NF is a Virtual Network Function (VNF) or a Physical Network Function (PNF). By default, NFs should block communication unless specifically authorized to communicate EVIDENCE Verify that attempts to access a network function (NF) from another NF without explicit authorization are unsuccessful. Verify that, after explicit authorization, attempts to access a NF with the correct access token are successful	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.848, cl. 5.17
TC150	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, NFV MANO	Færdig	MANO components (NFVO, VIM, and VNFM) should verify identity and location of the sender before acting on received data	MANO components (NFVO, VIM, and VNFM) should verify identity and location of the sender before acting on received data EVIDENCE Verify that access to MANO components (NFVO, VIM, and VNFM) is only possible with correct identity/credentials and from approved locations (such as both source and destination being in the same geographic area)	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 014, cl. 6
TC157	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, Virtualized resources	Færdig	Protection against hypervisor introspection	Protection against hypervisor introspection. Access to state information of guest OS from the hypervisor is restricted and privilege is granted based on "lowest privilege" principle EVIDENCE Verify that attempts to read or modify log files, or perform direct memory access from a hypervisor are unsuccessful	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 003, cl. 4.4.2.1.2
TC165	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, SDN Controller	Færdig	SDN control layer should authenticate and authorize administrators and applications	SDN control layer should authenticate and authorize administrators and applications. SDN controller should authenticate the switches EVIDENCE Verify that: (1) attempts to attach new switches without appropriate credentials are rejected by the SDN controller; (2) access to SDN controller is denied without credentials for an administrator account; and (3) unauthorized applications are not executed by the controller	a) Users and systems have unique ID's and are authenticated before accessing services or systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Rec. ITU-T X.1038, cl. 7.2.2 R-10, R-11, R-12, R-13, R-14
TC172	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, Multi-access edge computing	Færdig	MEC systems comply with regulatory requirements for Lawful Interception (LI) data identified in national laws is retained	MEC systems comply with regulatory requirements for Lawful Interception (LI) data identified in national laws is retained. LI data is retained for a duration mandated by national laws. Secure protocols are used for delivery of retained data to regulatory agencies. LI data is provided in plaintext. LI data can be captured and retained for inbound roamers. Unauthorized parties (including employees) cannot detect if an individual is a target of LI EVIDENCE Simulating a user who is a target of LI confirms that LI data identified in national laws is retained. The data of the simulated target user is deleted after the duration mandated by national laws. Packet captures confirm that TLS (or other protocols) are used for transferring the data of the simulated target user to regulatory bodies. Employees or target users cannot detect any changes during the period of LI targeting	f) Reinforce controls for remote access to critical assets of network and information systems by third parties		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS MEC 002, cl. 8.2

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC175	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, MEC platform, MEC application, Edge Application Server (EAS)	Færdig	MEC platform provides a mobile edge application only the information for which it is authorized	MEC platform provides a mobile edge application only the information for which it is authorized EVIDENCE Access logs of the MEC platform confirm that attempts of the MEC application to access data or resources via CAPIF for which it does not have authorization are unsuccessful	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS MEC 002, cl. 8.1
TC177	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, Virtualization Infrastructure, Virtual Infrastructure Manager (VIM)	Færdig	Virtualization platforms supporting role-based access control in MEC are in use	Virtualization platforms supporting role-based access control in MEC are in use EVIDENCE Existence of role-based access control is confirmed by inspecting access control policies and/or access to resources from accounts with different roles	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
TC182	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, Virtualization infrastructure, MEC host, MEC platform	Færdig	Network and data separation	Network and data separation: Presence of both physical and logical isolation of resources that don't have the same criticality EVIDENCE Verify that physical and logical separation/segregation of networks, resources and data is in place, depending on their criticality. For example, that user data is stored separately on an encrypted disk while system log is integrity protected locally	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. 8.2
TC199	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, eNB, MME	Færdig	S1-MME interface uses IKEv2 certificate based authentication	S1-MME interface uses IKEv2 certificate based authentication as specified in TS 33.310 EVIDENCE Verification of successful IKEv2 authentication between eNB and MME	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.310 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
TC200	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, eNB	Færdig	X2-C interface uses IKEv2 certificate based authentication	X2-C interface uses IKEv2 certificate based authentication as specified in TS 33.310 EVIDENCE Verification of successful IKEv2 authentication between eNBs	d) Choose appropriate authentication mechanisms, depending on the type of access		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.310 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
TC222	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, PHYSICAL INFRASTRUCTURE SECURITY, Virtualization infrastructure, Virtualized resources	Færdig	Protection against VM escape	Protection against VM escape EVIDENCE Documentation of the virtualization platform confirms that VM segregation is supported. Inspection of the virtualization platform with diagnostic tools confirm functional segregation of VMs	b) Implement logical access control mechanism for network and information systems to allow only authorized use		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC001	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, All network functions	Færdig	Service based interfaces (SBIs) of all network functions support transport layer security (TLS) as profiled in 3GPP technical specifications	Service based interfaces (SBIs) of all network functions support transport layer security (TLS) as profiled in 3GPP technical specifications: 33.210, clause 6.2 and 33.310, clause 6.2a. TLS is used for mutual authentication with certificates as well as for integrity and confidentiality protection of messages EVIDENCE Verification of each network function for support of TLS as profiled in 3GPP technical specifications: 33.210, clause 6.2 and 33.310, clause 6.2a. Verification can involve looking at product documentation and establishing test TLS connections to ensure that only protocol versions and cryptographic algorithms mandated by the profile are supported by the network function	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.2.2.2.2 3GPP TS 33.210, cl. 6.2 3GPP TS 33.310, cl. 6.2a 3GPP TS 33.501, cl. 5.9/13.1/13.3
TC003	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, All network functions	Færdig	NF service providers ensure integrity of the access token by verifying signature using the NRF's public key or verifying a MAC when using shared keys	NF service providers ensure integrity of the access token by verifying signature using the NRF's public key or verifying a MAC when using shared keys. NF providers further validate the fields in the access token such as scope, expiration time, etc. EVIDENCE NF service provider rejects malformed access tokens with incorrect MACs or incorrect fields/values and sends an OAuth error response	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.2.2.2.3/4.2.2.2.4 3GPP TS 33.501, cl. 13.4.1
TC011	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AUSF	Færdig	AUSFs should implement Nausf_SoRProtection service in accordance with the 3GPP technical specification	AUSFs should implement Nausf_SoRProtection service in accordance with 3GPP technical specification 33.501, clause 14.1 EVIDENCE Verify that sending the SUPI, service name, requester ID etc. to the Nausf_SoRProtection service results in the service returning a SoR-MAC-IAUSF and CounterSoR or an error	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 14.1
TC012	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AUSF	Færdig	AUSFs should implement Nausf_UPUProtection service in accordance with the 3GPP technical specification	AUSFs should implement Nausf_UPUProtection service in accordance with 3GPP technical specification 33.501, clause 14.1 EVIDENCE Verify that sending the SUPI, service name, UE Parameters Update Data. etc. to the Nausf_UPUProtection service results in the service returning a UPU-MAC-IAUSF and CounterUPU or an error	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.15/14.1
TC024	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	SEPP meets end-to-end security requirements	SEPP meets end-to-end security requirements listed in 3GPP TS 33.501 for interconnection between networks EVIDENCE Verification of SEPPs for compliance with 3GPP end-to-end security requirements. Verification can involve looking at product documentation detailing compliance with security requirements. Verification can also involve checking the packet captures on the SEPP to confirm that message elements at the application are confidentiality and/or integrity protected and no information about the internal network topology is contained in the packets	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.3 3GPP TS 33.517, cl. 4.2.2.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC030	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	SEPPs correctly replace information elements requiring encryption with the value "NULL" and create JSON patches with the encrypted values	SEPPs correctly replace information elements requiring encryption with the value "NULL" and create JSON patches with the encrypted values EVIDENCE Packet capture at the SEPP shows that information elements in the original message that require encryption according to the Data-type encryption policy are replaced with the value "NULL"	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.2.4.3.1 3GPP TS 33.517, cl. 4.2.2.5
TC034	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, SEPP	Færdig	SEPPs ensure that IEs requiring encryption are not inserted at a different location in the JSON object	SEPPs ensure that IEs requiring encryption are not inserted at a different location in the JSON object EVIDENCE Logs and packet captures of a SEPP confirm that an N32-f message is discarded if an encrypted IE in the message received has been moved to a cleartext IE	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 13.2.3.4 3GPP TS 33.517, cl. 4.2.2.8
TC042	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, RADIO NETWORK, gNB	Færdig	Ensure control plane data confidentiality and integrity protection over N2/Xn interface	gNB implements IPsec ESP and IKEv2 certificate based authentication as well as DTLS for integrity, confidentiality, and replay protection of E1, F1-U, F1-C, N2, N3, and Xn interfaces EVIDENCE Verification that a secure IPsec ESP connection can be established after IKEv2 certificate-based authentication. Verification that a secure DTLS record layer connection can be established after a DTLS handshake with certificates	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3/9.2/9.3/9.4/9.8 3GPP TS 33.511, cl. 4.2.2.1.16/4.2.2.1.17
TC052	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Transmission of data which needs protection uses industry standard network protocols with industry accepted algorithms	Transmission of data which needs protection uses industry standard network protocols with industry accepted algorithms. A protocol version without known vulnerabilities or a secure alternative protocol should be used EVIDENCE Packet captures show traffic is properly protected and insecure options are not accepted by the network products	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.4 3GPP TS 33.216 3GPP TS 33.511-519
TC055	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network products can boot only from the memory devices intended for this purpose	Network products can boot only from the memory devices intended for this purpose EVIDENCE Verification with 'bootlist' or similar command line tools to confirm that the network product is configured to boot from memory devices declared in the network product documentation and it cannot boot from another memory device. Verification that access to the firmware is not possible without correct authentication	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.2 3GPP TS 33.216 3GPP TS 33.511-519
TC056	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Validate all input data before processing	Validate all input data before processing EVIDENCE Documented fuzz testing results confirm robustness against malformed input data	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.4 3GPP TS 33.216 3GPP TS 33.511-519
TC057	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network products validate software package integrity during installation/upgrade via cryptographic means	Network products validate software package integrity during installation/upgrade via cryptographic means, e.g. a digital signature. A list of public keys or certificates of authorized software sources are provisioned to verify software origin. Tampered software is not executed or installed EVIDENCE Log files of the update manager/utility (e.g. application/history logs) in the network product show that installation/upgrade operation of network product fails when using an invalid software package. Log files of the update manager/utility (e.g. application/history logs) in the network product show that installation/upgrade operation is successful when using a valid software package	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.5 3GPP TS 33.216 3GPP TS 33.511-519
TC058	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Security mechanism to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list cryptographic credentials used for verifying software sources	Security mechanism to guarantee that only authorized individuals can initiate and deploy a software update, and modify the list cryptographic credentials used for verifying software sources EVIDENCE Verify that attempts to modify the list of cryptographic credentials used for verifying software sources are unsuccessful when logged in as a user without adequate privileges. Verify that attempts to install software packages are unsuccessful when logged in as a user without adequate privileges	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.5 3GPP TS 33.216 3GPP TS 33.511-519
TC070	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Processing of ICMPv4 and ICMPv6 packets which are not required for operation is disabled on the network product	Processing of ICMPv4 and ICMPv6 packets which are not required for operation is disabled on the network product. Certain ICMP types should not be used by the network product by default but support can be enabled for debugging etc. These ICMP types must be identified in the network product documentation. Certain ICMP types are generally permitted and do not need separate documentation. Permitted, forbidden, and optional ICMP types are identified in TS 33.117, cl. 4.2.4.1.1.2 EVIDENCE Network product documentation identifies a closed group of ICMP message types which are optional or permitted and lead to responses/configuration changes on receipt. Verify that the network product drops the message, does not reply and does not change any configuration when it receives ICMP messages not listed in the closed group in network product documentation, or identified as forbidden in the network product configuration	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.1.2 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC071	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	IPv4 packets with unnecessary options or IPv6 packets with unnecessary extension headers are filtered and not processed	IPv4 packets with unnecessary options or IPv6 packets with unnecessary extension headers are filtered and not processed EVIDENCE Packet captures confirm that a network product which is configured for dropping certain IPv4 options and certain IPv6 extension headers does not generate any ACK responses when packets with those options/extension headers are sent	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.1.3 3GPP TS 33.216 3GPP TS 33.511-519
TC074	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Protect communication between web client and web server	Communication between web client and web server is protected using TLS as profiled in Annex E of TS 33.310 with the following additional requirement: cipher suites with NULL encryption shall not be supported EVIDENCE Packet captures between the web client and the web server show the use of TLS and confirm that the protocol version/cryptographic algorithms mandated by the security profile are used	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.1 3GPP TS 33.216 3GPP TS 33.310, cl. Annex E 3GPP TS 33.511-519
TC080	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network Product validates, filters, escapes, and encodes user controllable input before it is used or output	Network Product validates, filters, escapes, and encodes user controllable input before it is used or output EVIDENCE Fuzz testing does not reveal attacks such as SQL injection caused by lack of input validation	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.4 3GPP TS 33.216 3GPP TS 33.511-519
TC081	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product has mechanisms for filtering incoming IP packets at the network and transport layer	Network product has mechanisms for filtering incoming IP packets at the network and transport layer as defined in RFC 3871 and 3GPP TS 33.117, cl. 4.2.6.2.1. The network product provides an option to drop/discard/accept/account packets that match a filter rule. Filtering on the basis of any portion of the protocol header should be possible. Logging of packets that match a rule can be enabled/disabled EVIDENCE Verify that after enabling packet filtering and configuring a rule to allow ICMP packets, a 'ping' sent to the product is logged and answered back	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.1 3GPP TS 33.216 3GPP TS 33.511-519 IETF RFC 3871
TC082	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	A network device shall be not affected in its availability or robustness by incoming packets that are manipulated or differing from the norm	A network device shall be not affected in its availability or robustness by incoming packets that are manipulated or differing from the norm. Robustness should be as effective for a large number of invalid packets as it is for small number of packets EVIDENCE Fuzz testing confirms that the network product is functional and robust when faced with a large number of malformed packets	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.2 3GPP TS 33.216 3GPP TS 33.511-519
TC083	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Checking against a whitelist/blacklist of permitted message type/sender identity combinations to ensure that the sender of a GTP-C based protocol message is authorized to send a message and the possibility to discard/accept/account for messages when the check is satisfied	Checking against a whitelist/blacklist of permitted message type/sender identity combinations to ensure that the sender of a GTP-C based protocol message is authorized to send a message and the possibility to discard/accept/account for messages when the check is satisfied. If a network product does not support such checks, then it needs to be deployed together with a separate entity which provides such checking capability EVIDENCE Verify that, after configuring GTP-C filtering rule to accept GTP-C messages from a certain source IP address, messages from that address are accepted and accounted, while messages from other source IP address not matching the rule are discarded	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.3 3GPP TS 33.216 3GPP TS 33.511-519
TC084	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Checking against a whitelist/blacklist of permitted message type/sender identity combinations to ensure that the sender of a GTP-U based protocol message is authorized to send a message and the possibility to discard/accept/account for messages when the check is satisfied	Checking against a whitelist/blacklist of permitted message type/sender identity combinations to ensure that the sender of a GTP-U based protocol message is authorized to send a message and the possibility to discard/accept/account for messages when the check is satisfied. If a network product does not support such checks, then it needs to be deployed together with a separate entity which provides such checking capability EVIDENCE Verify that, after configuring GTP-U filtering rule to accept GTP-U messages from a certain source IP address, messages from that address are accepted and accounted, while messages from other source IP address not matching the rule are discarded	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.4 3GPP TS 33.216 3GPP TS 33.511-519
TC085	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product only runs protocols and services which are needed for its operation, and which do not have any known security vulnerabilities	Network product only runs protocols and services which are needed for its operation, and which do not have any known security vulnerabilities. By default: FTP, TFTP, telnet, SNMP v1 and v2, rlogin, RCP, RSH, SSHv1, finger, HTTP, BOOTP, discovery protocols (LLDP, CDP), Identd, PAD, MOP, and TCP/UDP small servers (Echo, Chargen, Discard and Daytime) are disabled except if services are needed during deployment (in which case, those services are disabled after deployment) EVIDENCE List of protocols/services in the network product documentation that are necessary for correct operation of the network product. Verifying that the list of protocols/services in the network product documentation match with the list of protocols/services returned by tools for enumerating protocols/services (such as nmap)	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.1 3GPP TS 33.216 3GPP TS 33.511-519
TC092	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Systems should not process IP packets if their source address is not reachable via the incoming interface	Systems should not process IP packets if their source address is not reachable via the incoming interface. Use of "Reverse Path Filter" (RPF) provides one option to ensure such reachability checks EVIDENCE The logs of the network product show that sending a ping message from an IP address which is not reachable through the interface results in the ping packet being dropped without any response	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.1 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC096	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Systems should support mechanisms for buffer overflow protection	Systems should support mechanisms for buffer overflow protection EVIDENCE Documentation which describes buffer overflow mechanisms and also how to check that they have been enabled and/or implemented. Tests listed in the documentation produce expected results confirming buffer overflow protection	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.5 3GPP TS 33.216 3GPP TS 33.511-519
TC113	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, Network Function (NF), 5G Core (5GC), Service-Based Interfaces (SBI), UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF	Færdig	Parsers used by Network Functions (NF) should not execute JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI)	Parsers used by Network Functions (NF) should not execute JavaScript or any other code contained in JSON objects received on Service Based Interfaces (SBI). These parsers should not include any resources external to the received JSON object itself, such as files from the NF's filesystem EVIDENCE Verification that on sending an HTTP message containing JavaScript code, the network product does not execute any of the contained actions. A traffic analyzer connected to the network product confirms that no external resources get loaded during JSON parsing	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.3.6.2 3GPP TS 33.512-519
TC116	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, Network Function (NF), 5G Core (5GC), Service-Based Interfaces (SBI), UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF	Færdig	For data structures where values are accessible using names, the name should be unique	For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, the name should be unique. The occurrence of the same name (or key) twice within such a structure is an error and such a message should be rejected. The valid format and range of values for each information element (IE), when applicable, should be defined unambiguously. API implementation should fulfill the requirements specified in 3GPP TS 29.501, cl. 6.2: for each message the number of leaf IEs should not exceed 16000, the maximum size of the JSON body of any HTTP request should not exceed 2 million bytes, and the maximum nesting depth of leaves should not exceed 32 EVIDENCE Verify that sending a request to the network product with duplicate keys in message IE payload results in an error response. Sending a request with out of bounds IEs results in an error response from the network product	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 29.501, cl. 6.2 3GPP TS 33.117, cl. 4.3.6.3/4.3.6.4 3GPP TS 33.512-519
TC122	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, DNS server	Færdig	DNS servers in the 3GPP network should support and use DNS over (D)TLS	DNS servers in the 3GPP network should support and use DNS over (D)TLS as specified in RFC 7858 and RFC 8310 EVIDENCE Packet captures at DNS servers in the core network confirm the use of TLS for protection of DNS requests and responses	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, Annex P IETF RFC 7858/RFC 8310
TC128	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, SMF, UPF	Færdig	Non-SBA interfaces internal to the 5G core as well as interfaces between the 5G Core and entities not part of the 5G System are protected with NDS/IP	Non-SBA interfaces internal to the 5G core (such as N4 and N9), as well as DIAMETER or GTP-based interfaces between the 5G Core and entities not part of the 5G System (such as Rx and N26) are protected with NDS/IP as specified in TS 33.210 EVIDENCE Verification of packet captures on the interface under test confirms the use of IPsec for integrity, confidentiality, and replay protection	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.210 3GPP TS 33.501, cl. 9.5/9.9
TC129	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, RADIO NETWORK, VPLMN AMF, HPLMN AUSF, HPLMN UDM	Færdig	Network should provide a mechanism for steering UEs to a preferred roamed-to network indicated by the HPLMN during and after registration	Network should provide a mechanism for steering UEs to a preferred roamed-to network indicated by the HPLMN during and after registration in accordance with 3GPP technical specification 33.501, clause 6.14 EVIDENCE Verify that a test UE can be steered to a preferred roamed-to network both during and after registration in a VPLMN. Verification can involve checking the system logs of the test UE for an updated preferred/forbidden PLMN list and checking the packet captures of the HPLMN UDM for Nudm_SDM_Info	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.14
TC131	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, AMF	Færdig	AMF state machines handling registration over 3GPP and non-3GPP access follow the 3GPP technical specification	AMF state machines handling registration over 3GPP and non-3GPP access follow 3GPP technical specification 33.501, clause 6.8 EVIDENCE System logs of the AMF confirm that transitions between RM-DEREGISTERED and RM-REGISTERED/CM-CONNECTED states during UE registration follow the guidelines listed in 3GPP technical specification 33.501, clause 6.8	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.8
TC133	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, CORE NETWORK, UDM	Færdig	Operators should ensure that UEs conceal the Subscription Permanent Identifier (SUPI)	Operators should ensure that UEs conceal the Subscription Permanent Identifier (SUPI) by using the ECIES profile A or B defined in 3GPP technical specification, clause 6.12 and Annex C EVIDENCE Verify that the UDM correctly deconceals the Subscription Concealed Identifier (SUCI) using the implementer's test data in Annex C of 3GPP technical specification 33.501	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.12/Annex C
TC138	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Network Slice Subnet Instance	Færdig	Network slice subnet template (NSST) is integrity protected and management systems should verify the source and integrity of the subnet template	Network slice subnet template (NSST) is integrity protected and management systems should verify the source and integrity of the subnet template EVIDENCE Verify that the integrity of network slice subnet templates is ensured with cryptographic tools such as a digital signature or a hash. In addition, verify that a slice instance cannot be created with a tampered slice subnet template	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.3.1
TC145	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Network Slice Instance	Færdig	Log files must be protected from breaches of their confidentiality and integrity	Log files must be protected from breaches of their confidentiality and integrity EVIDENCE Using file inspection tools demonstrates log file integrity protection with checksums/digital signatures. Using file inspection tools demonstrates log file encryption with tools such as gpg/ccrypt. Verification that log files cannot be inspected without supplying necessary credentials	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NIST 800-92
TC146	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK SLICING, Network Slice Instance	Færdig	Isolation of distinct slices in the slice manager and restrictions on performing changes to parameters shared among slices belonging to different tenants	Isolation of distinct slices in the slice manager and restrictions on performing changes to parameters shared among slices belonging to different tenants EVIDENCE Verify that attempts to modify/change shared parameters from a slice are unsuccessful. Verify that attempts to decrypt/modify traffic intended for a different slice are unsuccessful	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC148	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, NFV MANO	Færdig	Each interface of a MANO entity should use TLS for API communication to ensure integrity protection, replay protection, and confidentiality	Each interface of a MANO entity should use TLS for API communication to ensure integrity protection, replay protection, and confidentiality EVIDENCE Verification of TLS support for API communication by looking at packet captures and setting up test TLS connections	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 022, cl. 4
TC151	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, VIM	Færdig	Integrity protection of data store used for VM images	Integrity protection of data store used for VM images EVIDENCE Manual inspection of VM images confirms that their integrity is protected with cryptographic tools such as a digital signature or a hash. Verify that VMs cannot be created with tampered images	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 014, cl. 5.2-c.1.1.4
TC152	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, Control Plane	Færdig	Control plane data between NFV hosts is sent over an authenticated and encrypted channel with standard protocols	Control plane data between NFV hosts is sent over an authenticated and encrypted channel with standard protocols EVIDENCE Packet captures confirm the use of standard security protocols such as TLS for authentication and encryption of control plane data exchanged between hosts	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.848, cl. 5.15
TC153	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, VNF	Færdig	Regular and effective patch management	Regular and effective patch management EVIDENCE Check for presence of patch management tools notifying of patch releases, allowing review and testing of patches, and controlled deployment	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 001, cl. 7.2.2
TC159	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, PHYSICAL INFRASTRUCTURE SECURITY, NFVI	Færdig	Host systems should implement Hardware-Based Root of Trust (HBRT) which serves as the initial root of trust for sensitive virtualized components	Host systems should implement Hardware-Based Root of Trust (HBRT) which serves as the initial root of trust for sensitive virtualized components EVIDENCE Verify that documentation of the host system describes support for HBRT. Verify via a guest OS that HBRT can be used for attestation	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 012, cl. 5.1
TC160	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, SOFTWARE DEFINED NETWORKS, VNF, SDN Controller	Færdig	Regular and effective vulnerability management program	Regular and effective vulnerability management program EVIDENCE Verify that documented processes and tools are in place to track public and vendor/supplier databases of disclosed vulnerabilities. Verify that vulnerability scanning tools are activated. Verify that documented processes are in place for addressing vulnerabilities with temporary measures such as filtering traffic until a software patch is available and applied	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 001, cl. 7.2.2 ITU-T X.1038, cl. 7.2.2 R-25
TC161	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NETWORK FUNCTION VIRTUALIZATION - MANO, VNF Manager	Færdig	Confidentiality and integrity protection of VNF packages during instantiation/on-boarding	Confidentiality and integrity protection of VNF packages during instantiation/on-boarding EVIDENCE Verify that integrity of VNF packages is ensured with cryptographic tools such as a digital signature or a hash. Verify that VNF manager does not accept VNF packages if the integrity checks fail. Verify by making API calls to the VNF manager that a VNF package can be encrypted before storage and decrypted before instantiation with the provided keys	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 021, cl. 5.1/5.2/6.3/6.4/6.5
TC162	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, SDN Controller	Færdig	SDN controller should not allow conflicting flow rules	SDN controller should not allow conflicting flow rules EVIDENCE Verify that attempts to add a conflicting flow rule are rejected by the SDN controller	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Rec. ITU-T X.1038, cl. 7.2.2 R-15
TC163	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, Northbound Interface, Southbound Interface, Eastbound, Westbound Interface	Færdig	APIs for the SDN controller and applications should be secured	APIs for the SDN controller and applications should be secured EVIDENCE Verify that access to APIs is only possible after authenticating with authorized accounts over encrypted channels. Verification involves checking the product documentation and executing test API calls	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 8.1
TC164	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, SDN Controller	Færdig	Integrity and confidentiality protection of configuration interfaces and configuration data stored in SDN controller	Integrity and confidentiality protection of configuration interfaces and configuration data stored in SDN controller EVIDENCE Verify that integrity of configuration data is ensured with cryptographic tools such as a digital signature or a hash. Verify that SDN controller does not accept configuration data from SDN applications over the application-control interface if the integrity checks fail. Verify via packet captures at the SDN controller that the communication between the SDN applications and the SDN controller is encrypted	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Rec. ITU-T X.1038, cl. 7.2.2 R-18, R-22
TC166	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, SDN Controller	Færdig	Operating systems hardening	Operating systems hardening EVIDENCE Diagnostic tools confirm that unused ports and services are disabled, firewall is activated, software packages are updated, and system monitoring tools have been activated	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Rec. ITU-T X.1038, cl. 7.2.2 R-24
TC169	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SOFTWARE DEFINED NETWORKS, SDN Applications, SDN Resources	Færdig	Protection against application misbehavior and bugs with the use of techniques such as sandboxing, application-kernel isolation, and application permissions	Protection against application misbehavior and bugs with the use of techniques such as sandboxing, application-kernel isolation, and application permissions EVIDENCE Check configuration files and diagnostic tools to verify that sandboxing techniques such as application-kernel isolation identified in product documentation are enabled and used	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 8.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC173	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, 3GPP SA6 interfaces, ETSI MEC interfaces	Færdig	Mutual authentication followed by confidentiality and integrity of messages on the Common API Framework (CAPIF) are ensured	Mutual authentication followed by confidentiality and integrity of messages on the Common API Framework (CAPIF) are ensured EVIDENCE Verify that API communication is protected with TLS by looking at packet captures and setting up test TLS connections	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI white paper #36 - Harmonizing standards for edge computing 3GPP TS 23.501, cl. 6.2.5.1 3GPP TS 33.122, cl. 6.5.2 3GPP TS 33.501, cl. 12.5
TC176	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, Virtualization Infrastructure, Virtual Infrastructure Manager (VIM)	Færdig	Virtualization platform is hardened using vendor-provided guidelines	Virtualization platform is hardened using vendor-provided guidelines EVIDENCE Verification of conformance to vendor provided guidelines by checking log files, configuration files, and automated tools	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
TC178	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, Virtualization Infrastructure, Virtual Infrastructure Manager (VIM)	Færdig	VMs in MEC are encrypted	VMs in MEC are encrypted EVIDENCE Inspection of servers and storage containing VMs confirm that the VMs are encrypted	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
TC185	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MULTI ACCESS EDGE COMPUTING, MEC host	Færdig	MEC systems provide a secure environment for services of users, network operators, third-party application providers, application developers, and platform vendors	MEC systems provide a secure environment for services of users, network operators, third-party application providers, application developers, and platform vendors EVIDENCE Documentation of the MEC system contains a list of service isolation techniques implemented. Verify that attempts to access other services from within a service instance are unsuccessful	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS MEC 002, cl. 8.1
TC186	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, eNB, MME	Færdig	User plane data is integrity-protected	User plane data is integrity-protected EVIDENCE Packet captures of the traffic between the RN and the DeNB confirm the use of the PDCP protocol for integrity protection	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.401, cl. 5.1.4 3GPP TS 36.323 3GPP TS 33.501, cl. 5.4
TC187	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, LTE Visiting PLMN	Færdig	Monitoring of edge network nodes such as Signal Transfer Points (STPs) and Diameter Edge/Routing Agents (DEAs/DRAs) with firewalls or other tools	Monitoring of edge network nodes such as Signal Transfer Points (STPs) and Diameter Edge/Routing Agents (DEAs/DRAs) with firewalls or other tools to protect roaming attacks from SS7 and DIAMETER signaling vulnerabilities EVIDENCE Check the log files of the firewall or other monitoring tools to confirm that a simulated roaming attack launched using SS7/DIAMETER vulnerabilities is detected by the firewall rules or other tools used to monitor edge network nodes	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ENISA - Signaling Security in Telecom SS7/Diameter/5G, cl. 3.3
TC188	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, LTE Visiting PLMN	Færdig	Monitoring of core network elements such as such as Visitor Location Register (VLR) and Mobility Management Entity (MME) with firewalls or other tools	Monitoring of core network elements such as such as Visitor Location Register (VLR) and Mobility Management Entity (MME) with firewalls or other tools to detect and prevent roaming attacks from SS7 and DIAMETER signaling vulnerabilities EVIDENCE Check the log files of the firewall or other monitoring tools to confirm that a simulated roaming attack launched using SS7/DIAMETER vulnerabilities is detected by the firewall rules or other tools used to monitor core network nodes	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ENISA - Signaling Security in Telecom SS7/Diameter/5G, cl. 3.3
TC189	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, LTE Visiting PLMN	Færdig	End-to-end signaling security is used for DIAMETER signaling	End-to-end signaling security is used for DIAMETER signaling EVIDENCE Packet captures confirm that Diameter End-to-End Signaling (DESS) is used to provide end-to-end security	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	GSMA FS.19
TC190	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, LTE Visiting PLMN	Færdig	Protections against ReVOLTE attacks are implemented	Protections against ReVOLTE attacks are implemented EVIDENCE Depending on the mitigation implemented: i) packet captures at the eNodeB confirm that different radio bearer identities are used for subsequent calls even within the same radio connection, and/or ii) system logs of the eNB show that it has initiated an intra-cell handover to derive fresh keys for subsequent calls on the same radio connection, and/or iii) packet captures at the IMS access gateway confirm the use of SRTP for encryption and integrity protection of VoLTE calls	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	TS 33.328, cl. 4 TS 33.401, cl. 7.2.8.4.1/E.2.2 TS 33.501, cl. 5.4
TC196	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, MME	Færdig	Bidding down should be prevented by including the replayed security capabilities of the UE in the Security Mode Command sent from the MME	Bidding down should be prevented by including the replayed security capabilities of the UE in the Security Mode Command sent from the MME EVIDENCE Verify that eliminating certain UE capabilities on the interface between the UE and MME results in a protocol continuation failure and the UE responds with a NAS Security Mode Reject message	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116, cl. 4.2.2.3.1 3GPP TS 33.401, cl. 7.2
TC197	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, MME	Færdig	The MME protects the Security Mode Command message with the integrity algorithm which has the highest priority according to the ordered lists	The MME protects the Security Mode Command message with the integrity algorithm which has the highest priority according to the ordered lists EVIDENCE MME system logs confirm that the MME has selected the integrity algorithm which has the highest priority according to the locally configured ordered lists and is also contained in the UE security capabilities	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116, cl. 4.2.2.3.2 3GPP TS 33.401, cl. 7.2.4.3.1
TC198	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, MME	Færdig	MME releases any established non-emergency bearers when the authentication of UE fails	MME releases any established non-emergency bearers when the authentication of UE fails EVIDENCE Check the system logs of the MME to confirm that when the UE sends a request for EPS emergency bearer services and UE authentication fails, the established non-emergency bearers are released by the MME	e) Set up state of the art controls to protect integrity of systems		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116, cl. 4.2.2.6.1 3GPP TS 33.401, cl. 15.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC206	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, IMPLEMENTATION OPTIONS, eNB	Færdig	eNBs should have a secure environment for storage of sensitive data and execution of sensitive functions	eNBs should have a secure environment for storage of sensitive data and execution of sensitive functions EVIDENCE Documentation of the eNB contains a list of mechanisms such as Trusted Execution Environment (TEE) used to protect storage of sensitive data and execution of sensitive functions. Diagnostic tools on the eNB confirm that the mechanisms are implemented, enabled, and used	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.401, cl. 5.3.5 3GPP TS 33.501, cl. 5.4
TC221	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, PHYSICAL INFRASTRUCTURE SECURITY, Virtualization infrastructure, Virtualized resources	Færdig	Protection against VM sprawl	Protection against VM sprawl EVIDENCE Documentation of the hypervisor has a list of hardening techniques. Diagnostic tools confirm that hypervisor hardening techniques described in documentation are enabled	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC224	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, PHYSICAL INFRASTRUCTURE SECURITY, Base stations	Færdig	Anti radio jamming techniques such as uncoordinated spread spectrum should be implemented	Anti radio jamming techniques such as uncoordinated spread spectrum should be implemented EVIDENCE Verify that product documentation contains a list jamming resistance mechanisms and support for hardware-based real-time encryption and decryption. Verify product configuration files to ensure that hardware-based real-time encryption and decryption, as well as jamming resistance mechanisms listed in the documentation are enabled	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC002	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, All network functions	Færdig	Certificates for mutual authentication of network functions follow the profiles given in 3GPP technical specifications	Certificates for mutual authentication of network functions follow the profiles given in 3GPP technical specifications: 33.310 and 33.501 EVIDENCE Verification of all client and server certificates indicates their compliance with the 3GPP profiles given in TS 33.310 and 33.501. Verification can involve manual inspection of certificates or automated tools, if available	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.310, cl. 6.1 3GPP TS 33.501, cl. 5.9
TC005	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, AMF	Færdig	AMFs protect signaling messages with ciphering and integrity protection of NAS signaling messages using appropriate algorithms	AMFs protect signaling messages with ciphering and integrity protection of NAS signaling messages using appropriate algorithms such as 128-NEA1 128-NIA1 standardized in 3GPP TS 33.501 EVIDENCE Packet captures of NAS SMC procedure taking place between UE and AMF demonstrate integrity protection, replay protection, and encryption	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.5.1/5.5.2/5.11/6.4 3GPP TS 33.512, cl. 4.2.2.3.1
TC006	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, AMF	Færdig	Support for NIA0 integrity protection is disabled in AMF unless support for unauthenticated emergency session is a regulatory requirement	Support for NIA0 integrity protection is disabled in AMF unless support for unauthenticated emergency session is a regulatory requirement EVIDENCE NAS Security Mode Command message to the UE containing the selected NAS algorithms does not include NIA0 if it is disabled	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.5.2 3GPP TS 33.512, cl. 4.2.2.3.2
TC007	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, AMF	Færdig	During the handover, if the AMF changes, the target AMF selects the NAS algorithm with the highest priority in the ordered list of the UE security capabilities	During the handover, if the AMF changes, the target AMF selects the NAS algorithm with the highest priority in the ordered list of the UE security capabilities EVIDENCE Packet capture of the NGAP HANDOVER REQUEST message sent by the target AMF to the gNB includes the algorithm with the highest priority of the target AMF and not the highest priority in the ordered list received from the source AMF	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.4/6.7.1 3GPP TS 33.512, cl. 4.2.2.4.2
TC008	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, AMF	Færdig	AMFs reject registration request messages containing invalid or unacceptable UE security capabilities	AMFs reject registration request messages containing invalid or unacceptable UE security capabilities. For example: UE security capabilities message containing no integrity algorithms EVIDENCE Sending invalid/unacceptable UE security capabilities such as those with no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported are rejected by the AMF and their rejection is captured in its access logs	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 24.501, cl. 5.5.1.2.8 3GPP TS 33.501, cl. 5.5 3GPP TS 33.512, cl. 4.2.2.6
TC017	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, UDM	Færdig	SIDF uses protection scheme indicator in the concealed identifier (SUCI) for determining which ECIES profile should be used for resolving the SUCI to the SUPI	SIDF uses protection scheme indicator in the concealed identifier (SUCI) for determining which ECIES profile should be used for resolving the SUCI to the SUPI EVIDENCE SUPI available from SUCI resolution at the SIDF matches the SUPI of the UE	b) Implement encryption policy		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.8.2 3GPP TS 33.514, cl. 4.2.1.1
TC026	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, SEPP	Færdig	Protect application layer messages on the N32 interface of SEPPs in different PLMN	Protect application layer messages on the N32 interface of SEPPs in different PLMN EVIDENCE SEPP documentation and system logs confirm the use of PRINS (PRotocol for N32 Interconnect Security) for protecting application layer messages on the N32 interface of SEPPs when there are IPX entities between SEPPs	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.3.2/13.2/Annex G
TC032	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, SEPP	Færdig	Comply with JWS profile restriction	SEPPs follow the JWS profile defined in 3GPP TS 33.210 EVIDENCE Logs of the SEPP show that sending an N32-f message with a JWS not following the 3GPP TS 33.210 profile is rejected	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.210, cl. 6.3.3 3GPP TS 33.501, cl. 13.2.4.9 3GPP TS 33.517, cl. 4.2.2.7
TC033	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, CORE NETWORK, SEPP	Færdig	Ensure that SEPPs only use the ES256 algorithm with IPX entities	SEPPs only use the ES256 algorithm with IPX entities EVIDENCE Review of the network product documentation shows that SEPP only supports the JWS ES256 algorithm for use with IPX entities	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.210, cl. 6.3.3 3GPP TS 33.501, cl. 13.2.4.9 3GPP TS 33.517, cl. 4.2.2.7
TC041	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Ensure proper Ciphering of RRC-signalling	gNB implements ciphering algorithms NEA0, 128-NEA1, 128-NEA2, 128-NEA3 for ciphering of RRC signaling EVIDENCE Packet captures show that control plane packets sent to the UE after the gNB sends AS Security Mode Command (SMC) are ciphered	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3.2/5.11 3GPP TS 33.511, cl. 4.2.2.1.6
TC043	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Ensure proper replay protection of RRC-signalling	gNB implements NIA0, 128-NIA1, 128-NIA2, 128-NIA3 algorithms with NIA0 disabled unless necessary by regulatory requirements for integrity and replay protection of RRC signaling EVIDENCE Packet captures show that control plane packets sent/received to/from the UE are integrity protected	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3.3/5.11 3GPP TS 33.511, cl. 4.2.2.1.1/4.2.2.1.9

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC044	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	gNB verify RRC and user plane integrity	gNB verify RRC and user plane integrity EVIDENCE gNB system logs show that gNB rejects a RRC message or a PDCP PDU sent with faulty or missing MAC-I	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3/6.5.1/6.6.4 3GPP TS 33.511, cl. 4.2.2.1.4/4.2.2.1.5
TC045	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Ensure proper ciphering of User data between UE and gNB	gNB activates ciphering of user data based on security policy sent by the SMF EVIDENCE Packet captures show that user plane packets sent to the UE after the gNB sends RRCConnectionReconfiguration are confidentiality protected	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3.3 3GPP TS 33.511, cl. 4.2.2.1.7
TC046	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Ensure integrity protection of user data between the UE and the gNB	gNB ensures integrity of user data based on security policy sent by the SMF EVIDENCE Packet captures show that user plane packets sent between UE and gNB over the NG RAN air interface after gNB sends RRCConnectionReconfiguration are integrity protected	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3.2 3GPP TS 33.511, cl. 4.2.2.1.2/4.2.2.1.8
TC047	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Ensure proper procedures for AS algorithm selection	gNB selects the ciphering and integrity algorithm with the highest priority from the UE's 5G security capabilities and locally configured list of algorithms EVIDENCE Packet captures at the gNB show that the AS Security Mode Command message includes the chosen algorithm with the highest priority according to the ordered lists locally configured and contained in the UE 5G security capabilities	e) Use state of the art encryption algorithms		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.3/6.7.3 3GPP TS 33.511, cl. 4.2.2.1.12/4.2.2.1.15
TC048	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Prevent failure to refresh keys by gNB	gNBs refresh keys KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc when the PDCP COUNT value is about to be re-used with the same Radio Bearer identity and with the same KgNB EVIDENCE gNB system logs and packet captures on the gNB confirm that it performs KgNB refresh when PDCP COUNTs are about to wrap around because of RRC or UP messages with increasing PDCP COUNT from the UE	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.9.4 3GPP TS 33.511, cl. 4.2.2.1.13
TC049	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, gNB	Færdig	Prevent failure to update key at the gNB on Dual Connectivity	In dual connectivity, a secondary node (SN) asks the master node (MN) to derive a fresh KSN when PDCP COUNT values are about to wrap around. While adding subsequent radio bearer(s) to the same SN, the MN assigns a new radio bearer identity that has not previously been used for the current KSN. If the MN cannot allocate an unused identity due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh KSN which it then updates with SN modification procedure EVIDENCE gNB system logs and packet captures on a gNB acting as an MN show that it performs KSN update and sends it to the SN via the SN Modification Request when DRB-IDs are about to be reused	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501 6.10.2.1 3GPP TS 33.511 4.2.2.1.18
TC121	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, RADIO NETWORK, IAB donor	Færdig	IAB donor should support confidentiality, integrity, and replay protection of RRC-signalling between the IAB donor and the IAB-node (IAB-UE)	IAB donor should support confidentiality, integrity, and replay protection of RRC-signalling between the IAB donor and the IAB-node (IAB-UE) EVIDENCE Packet captures at the IAB donor confirm integrity, confidentiality, and replay protection of RRC-signalling	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, Annex M
TC136	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NETWORK SLICING, Service Based Interfaces, Os-Ma-Nfvo	Færdig	Slice management interface messages have replay protection, integrity protection, and confidentiality	Slice management interface messages have replay protection, integrity protection, and confidentiality EVIDENCE Verify that standard security protocols such as TLS which provide integrity, confidentiality, and replay protection are used for communicating with the slice management interfaces. This can be confirmed by checking packet captures or by setting up test connections	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.1.1
TC137	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NETWORK SLICING, Network Slice Instance	Færdig	Supervision and performance reporting of a Network Slice Instance (NSI) should at least be integrity protected and may additionally be confidentiality protected	Supervision and performance reporting of a Network Slice Instance (NSI) should at least be integrity protected and may additionally be confidentiality protected EVIDENCE Verify that standard security protocols such as TLS which provide integrity, confidentiality, and replay protection are used for communicating supervising and performance reporting of NSIs. This can be confirmed by checking packet captures or by setting up test connections	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.2.1
TC139	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NETWORK SLICING, Network Slice Instance	Færdig	Network slice subnet template (NSST) should be confidentiality protected	Network slice subnet template (NSST) should be confidentiality protected EVIDENCE Inspection of the encrypted network slice subnet template does not reveal configuration and topology information. Verification that network slice subnet template can only be used after decryption with appropriate credentials	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.3.1
TC140	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NETWORK SLICING, Network Slice Instance	Færdig	Negotiation of slice characteristics such as bandwidth, latency, and reliability between a communication service customer and an operator should have replay, integrity, and confidentiality protection with TLS	Negotiation of slice characteristics such as bandwidth, latency, and reliability between a communication service customer and an operator should have replay, integrity, and confidentiality protection with TLS. Version 1.2 or 1.3 of TLS are recommended EVIDENCE Verify by successfully setting up test connections with slice management interface and negotiating different slice characteristics via TLS	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.811, cl. 4.4.1
TC170	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, SOFTWARE DEFINED NETWORKS, SDN Infrastructure layer	Færdig	Interconnect traffic between data centers should be authenticated and encrypted	Interconnect traffic between data centers should be authenticated and encrypted EVIDENCE Check documentation of SDN controller/switches, business agreements, and packet captures for use of L1 and/or L2 encryption techniques such as MACsec	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 5.3
TC191	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, MME	Færdig	NAS signaling should be confidentiality protected by the MME	NAS signaling should be confidentiality protected by the MME EVIDENCE Packet captures confirm the encryption of the NAS signaling messages	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Fortrolighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116, cl. 4.2.2.3.4 3GPP TS 33.401, cl. 5.1.3.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC192	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, MME	Færdig	User data sent via MME should be confidentiality protected	User data sent via MME should be confidentiality protected EVIDENCE Packet captures show that the user plane messages over the access stratum at PDCP layer are encrypted	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Fortrolighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.401, cl. 5.1.3.1
TC193	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, MME	Færdig	User data sent via the MME should be integrity protected	User data sent via the MME should be integrity protected EVIDENCE Packet captures confirm the integrity protection of user data with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.401, cl. 5.1.4.1
TC194	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, MME	Færdig	All NAS signaling messages except those explicitly listed in TS 24.301 as exceptions should be integrity-protected	All NAS signaling messages except those explicitly listed in TS 24.301 as exceptions should be integrity-protected EVIDENCE Packet captures confirm the integrity protection of the NAS signaling messages with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.401, cl. 5.1.4.1/8.1
TC195	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, MME	Færdig	NAS NULL integrity with EIA0 is only used for emergency calls	NAS NULL integrity with EIA0 is only used for emergency calls EVIDENCE Packet captures at the MME confirm that that the SECURITY MODE COMMAND message sent by the MME after successful UE authentication contains an algorithm different from EIA0 (except for emergency calls)	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116, cl. 4.2.2.3.3 3GPP TS 33.401, cl. 5.1.4.1
TC201	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, eNB	Færdig	eNB ensures confidentiality and integrity protection of control plane data	eNB ensures confidentiality and integrity protection of control plane data EVIDENCE Packet captures confirm the use of IPsec on X2-C and S1-MME interfaces	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.216 4.2.2.1.1/4.2.2.1.2 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
TC202	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, eNB	Færdig	eNB ensures confidentiality and integrity protection of user plane packets between the Uu reference point and the S1/X2 reference points	eNB ensures confidentiality and integrity protection of user plane packets between the Uu reference point and the S1/X2 reference points EVIDENCE Packet captures confirm that user plane packets sent by the eNB after sending the AS SMC command to the UE are ciphered	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.216, cl. 4.2.2.1.3/4.2.2.1.4 3GPP TS 33.401, cl. 5.3.4 3GPP TS 33.501, cl. 5.4
TC203	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, eNB	Færdig	eNB protects the Security Mode Command message with the integrity and ciphering algorithms which have the highest priority according to the ordered lists	eNB protects the Security Mode Command message with the integrity and ciphering algorithms which have the highest priority according to the ordered lists EVIDENCE System logs of the eNB confirm that it has selected the integrity and ciphering algorithms which have the highest priority according to the locally configured ordered lists and which are also contained in the UE security capabilities	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.216, cl. 4.2.2.1.5/4.2.2.1.9/4.2.2.1.11 3GPP TS 33.401, cl. 7.2.4.2.1 3GPP TS 33.501, cl. 5.4
TC204	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, eNB	Færdig	eNBs verify RRC integrity	eNBs verify RRC integrity EVIDENCE Verify that eNB rejects a RRC message sent with faulty or missing MAC-I	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.216, cl. 4.2.2.1.6 3GPP TS 33.401, cl. 7.4.1 3GPP TS 33.501, cl. 5.4
TC205	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IMPLEMENTATION OPTIONS, eNB	Færdig	AS NULL integrity with EIA0 is only used for emergency calls	AS NULL integrity with EIA0 is only used for emergency calls EVIDENCE Confirmation that the SECURITY MODE COMMAND message sent by the eNB after successful UE authentication contains an algorithm different from EIA0 (except for emergency calls)	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents		Protect	Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.216, cl. 4.2.2.1.7 3GPP TS 33.401, cl. 5.1.4.2 3GPP TS 33.501, cl. 5.4

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC015	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, UDM	Færdig	Protect the Home Network private key from physical attacks in the UDM	Protect the Home Network private key from physical attacks in the UDM EVIDENCE UDM documentation lists mechanisms for protection of private key from physical attacks. Verification with a key management utility that the home network private key in the UDM is protected in the system keystore. If hardware security tools such as TEEs are used, then the system logs of the UDM show that sending a test SUCI to the TEE inside the UDM results in the correct mapping to SUPI	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.8.2
TC016	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, UDM	Færdig	The algorithm for subscriber privacy (SUCI to SUPI mapping) is executed in the secure environment of the UDM	The algorithm for subscriber privacy (SUCI to SUPI mapping) is executed in the secure environment of the UDM EVIDENCE UDM documentation lists mechanisms for protection of the algorithm for mapping concealed identity to permanent identity. If hardware security tools such as TEEs are used, then the system logs of the UDM show that sending a test SUCI to the TEE inside UDM results in the correct mapping to SUPI	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.8.2
TC018	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, UDM	Færdig	UDM logs the authentication status and timestamp of subscriber authentication, in particular when the subscriber is in a visited network	UDM logs the authentication status and timestamp of subscriber authentication, in particular when the subscriber is in a visited network EVIDENCE Logs of the UDM show the status and timestamp of subscriber authentication	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.1.4.1a 3GPP TS 33.514, cl. 4.2.2.2
TC025	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, SEPP	Færdig	SEPPs clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications	SEPPs clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications EVIDENCE Verification that the SEPPs don't accept N32-c TLS connections if raw public keys/certificates are used. Verification that SEPPs don't accept N32-f JSON patches signed with raw public keys/certificates of peer SEPPs	c) Implement policy for management of cryptographic keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.9.3.2 3GPP TS 33.517, cl. 4.2.2.2
TC061	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Predefined or default accounts are deleted or disabled	Predefined or default accounts are deleted or disabled EVIDENCE Access logs of the network product confirm that login attempts with predefined accounts are unsuccessful	d) Implement policy for management of user passwords		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.2.2/4.2.3.4.2.3 3GPP TS 33.216 3GPP TS 33.511-519
TC062	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	Færdig	Password change is only possible if documented password complexity criteria is met	Password change is only possible if documented password complexity criteria is met. Password change is enforced after initial login. Users can change password at any time. Captcha's and timers are used to prevent repeated login attempts. Accounts are blocked after a certain number of failed attempts. Passwords are hidden, for example, by replacing individual characters with * EVIDENCE Documented password policy with requirements on complexity and change frequency, means of protection against brute force/dictionary attacks, and means for hiding password display in clear	d) Implement policy for management of user passwords		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.3 3GPP TS 33.216 3GPP TS 33.511-519
TC114	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, UDM, AUSF	Færdig	Subscription permanent identifier (SUPI) is encrypted to derive the Subscription Concealed Identifier (SUCI) using a non-null protection scheme by default	Subscription permanent identifier (SUPI) is encrypted to derive the Subscription Concealed Identifier (SUCI) using a non-null protection scheme by default EVIDENCE Verification of UE authentication confirms that SUPI is not transmitted in clear text. Inspection of the protection scheme in the SUCI confirms a non-null protection scheme was used	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.12
TC120	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, CORE NETWORK, RADIO NETWORK, AUSF, SEAF, AMF, gNB, N3IWF	Færdig	Key hierarchy defined in the technical specification is followed for deriving and distributing keys	Key hierarchy defined in technical specification 33.501, clause 6.2 is followed for deriving and distributing keys KAUSF, KSEAF, KAMF, KgNB, and KN3IWF EVIDENCE After a test UE device has successfully authenticated and registered, debug tools on the test UE and network nodes AUSF/SEAF/AMF/gNB/N3IWF confirm that the keys in the network nodes are identical to the ones derived by the UE	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 6.2
TC143	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NETWORK SLICING, NSSAI	Færdig	Security of the User ID and credentials used for slice specific authorization and authentication is ensured during transfer and network storage	Security of the User ID and credentials used for slice specific authorization and authentication is ensured during transfer and network storage EVIDENCE Verification that User ID and credentials used for slice specific authorization and authentication are protected with the use of password salting, database encryption, etc. Packet captures show that secure protocols such as TLS are used for slice specific authorization and authentication.	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.813, cl. 6.5
TC158	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NETWORK FUNCTION VIRTUALIZATION - MANO, SOFTWARE DEFINED NETWORKS, NSM, SDN Controller	Færdig	SDN controller and NFV Security Manager (NSM) should have a key and certificate management system which includes key generation, storage, deletion and cryptographic processing	SDN controller and NFV Security Manager (NSM) should have a key and certificate management system which includes key generation, storage, deletion and cryptographic processing. EVIDENCE Verify that system documentation outlines an API for key management. Making API calls to create, store, delete keys/certificates confirms support for key management	c) Implement policy for management of cryptographic keys		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 012, cl. 5.1.2 Rec. ITU-T X.1038, cl. 7.2.2 R-19
TC093	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Kernel based network functions not needed for the operation of the network element should be deactivated	Kernel based network functions not needed for the operation of the network element should be deactivated. Kernel functions such as IP packet forwarding, proxy ARP, gratuitous ARP, IPv4 multicast handling, and directed broadcast are deactivated unless needed in certain deployments EVIDENCE Verification method: After connecting two hosts to the two interfaces of the network product, it is confirmed that i) an IP packet from Host 1 on subnet A destined for Host 2 on subnet B with the network product configured as a default gateway is logged but not forwarded by the network product, ii) an ARP request from Host 1 on subnet A to discover the MAC of Host 2 on subnet B does not result in an ARP reply from the network product to Host 1 with its own MAC address, iii) an IP packet from Host 1 whose IP destination address is a valid broadcast address belonging to the subnet B is dropped by the network product rather than being broadcast, iv) system commands confirm that none of the network product's interface is running multicast, v) a gratuitous ARP request from Host 1 is received by the network product but discarded without updating the ARP cache (unless gratuitous ARP is necessary for a deployment scenario). The fact that kernel based network functions are disabled is also confirmed in the configuration files	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.2 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC094	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network products should not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-storage drives are connected	Network products should not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-storage drives are connected. If the operating system of the network product supports an automatic launch, it should be deactivated unless it is needed for availability requirements EVIDENCE Verify that after logging in to a network product and inserting removable media devices (CD-, DVD-, USB-Sticks and/or USB-Storage drives) no applications open the contents of the removable media device	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.3 3GPP TS 33.216 3GPP TS 33.511-519
TC098	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Directory listings (indexing)/Directory browsing is deactivated in all web server components	Directory listings (indexing)/Directory browsing is deactivated in all web server components EVIDENCE Using automated tools demonstrates that directory listing/browsing has been deactivated in all web server components	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.10 3GPP TS 33.216 3GPP TS 33.511-519
TC099	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	HTTP header does not include information about the version of the web server and the modules/add-ons used	HTTP header does not include information about the version of the web server and the modules/add-ons used EVIDENCE Automatic assessment tool shows that HTTP headers do not include information on the version of the web server or the modules/add-ons used	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.11 3GPP TS 33.216 3GPP TS 33.511-519
TC100	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	User-defined error pages should not include version information about the web server and the modules/add-ons used	User-defined error pages should not include version information about the web server and the modules/add-ons used. Error messages should not information such as internal server names, error codes, etc. Default error pages of the web server should be replaced by error pages defined by the vendor EVIDENCE Automatic assessment tools show that generated error pages and error messages do not include information about the web server	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.12 3GPP TS 33.216 3GPP TS 33.511-519
TC101	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	File type- or script-mappings that are not required should be deleted	File type- or script-mappings that are not required should be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs EVIDENCE Automatic assessment tools confirm that file type- or script-mappings which are not required have been deleted	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.13 3GPP TS 33.216 3GPP TS 33.511-519
TC102	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory	Restrictive access rights are assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. A web server should not have access to files which are not meant to be delivered EVIDENCE Verification that the servable content of a web server is owned by the user that runs the web server and the files are not writable for others. Verification that the user running the web server is an unprivileged account and, in case of operating systems that have chrooted environments, the web server runs inside a jail/chrooted environment	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.14 3GPP TS 33.216 3GPP TS 33.511-519
TC103	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	If CGI or other scripting technology is used, only the scripting directory should have execute rights	If CGI or other scripting technology is used, only the scripting directory should have execute rights. Other directories used or meant for web content should not have execute rights EVIDENCE Verification that only the scripting directory has execute permissions in the web server. Verification of only operating system permissions may not be sufficient and may require also examining the configuration files of the web server	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.15 3GPP TS 33.216 3GPP TS 33.511-519
TC104	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Web server process should not run with system privileges	Web server process should not run with system privileges. Even if the web server process is started by a user with system privileges, execution should be transferred to a different user without system privileges after the start EVIDENCE Automatic assessment tools confirm that no web server processes run with system privileges, even if these processes have been started by a user with system privileges	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.2 3GPP TS 33.216 3GPP TS 33.511-519
TC105	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	HTTP methods not required should be deactivated	HTTP methods not required should be deactivated. Standard requests to web servers should only use GET, HEAD, and POST. If other methods are required, they should not introduce security leaks such as TRACK or TRACE EVIDENCE Verification of system settings and configurations of all web components confirms that unneeded HTTP methods are deactivated	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.3 3GPP TS 33.216 3GPP TS 33.511-519

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC106	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	All optional add-ons and components of the web server which are not needed should be deactivated	All optional add-ons and components of the web server which are not needed should be deactivated. In particular, components such as CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required EVIDENCE Verification with automated tools and/or manual inspection of configuration files confirms that, firstly, the web server is only running and listening on known ports and, secondly, that CGI or other scripting components, Server Side Includes (SSI), and WebDAV are deactivated unless they are required	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.4 3GPP TS 33.216 3GPP TS 33.511-519
TC107	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	If CGI (Common Gateway Interface) or other scripting technologies (including PERL, PHP, and others) are used, the scripting directory should not include compilers or interpreters	If CGI (Common Gateway Interface) or other scripting technologies (including PERL, PHP, and others) are used, the scripting directory should not include compilers or interpreters EVIDENCE Inspection of the directory/directories used for CGI or other scripting tools confirms that the scripting directory/directories include no compilers or interpreters (e.g., PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells)	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.5 3GPP TS 33.216 3GPP TS 33.511-519
TC108	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads	If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads EVIDENCE Verification of the web server configuration files confirms that the upload directory is configured to be different from the CGI/scripting directory	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.6 3GPP TS 33.216 3GPP TS 33.511-519
TC109	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	Færdig	If Server Side Includes (SSI) is active, the execution of system commands should be deactivated	If Server Side Includes (SSI) is active, the execution of system commands should be deactivated EVIDENCE Verification of the web server configuration shows that parameters such as NOEXEC (APACHE) or ssiExecDisable (IIS) are set to ensure that system command execution is deactivated	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.3.4.7 3GPP TS 33.511-519
TC110	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	Færdig	Access rights for web server configuration files are only granted to the owner of the web server process or to a user with system privileges	Access rights for web server configuration files are only granted to the owner of the web server process or to a user with system privileges EVIDENCE Verification of the access rights settings for web server system configuration files confirms that access is only granted to the owner of the web server process or to a user with system privileges	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.3.4.8 3GPP TS 33.511-519
TC111	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	Færdig	Default content (examples, help files, documentation, aliases) provided with the standard installation of the web server should be removed	Default content (examples, help files, documentation, aliases) provided with the standard installation of the web server should be removed EVIDENCE Verification that all default content (examples, help files, documentation, aliases) provided with the standard installation of the web server have been removed	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.3.4.9 3GPP TS 33.511-519
TC112	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, CORE NETWORK, RADIO NETWORK, O&M, control plane, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	Færdig	Network products should support physical or logical separation of traffic belonging to different network domains	Network products should support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains and must be separated EVIDENCE If a network product handles traffic from different network domains, then packet-forwarding tests confirm that the network product refuses traffic intended for one network domain on all interfaces meant for other network domains, and vice versa	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.117, cl. 4.3.5.1 3GPP TS 33.511-519 IETF RFC 3871, cl. 2.3.5
TC156	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, NETWORK FUNCTION VIRTUALIZATION - MANO, VNF	Færdig	VNFs should synchronize with trusted time sources	VNFs should synchronize with trusted time sources EVIDENCE Check that time synchronization sources such as NTP servers used by VNFs are reliable and trusted. This can be verified by checking documentation and configuration	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TR 33.848, cl. 5.20
TC211	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, PHYSICAL INFRASTRUCTURE SECURITY, Physical asset	Færdig	Proper maintenance of equipment in data centers	Proper maintenance of equipment in data centers EVIDENCE Documented policy / processes for carrying out periodic maintenance at supplier recommended intervals show that only authorized personnel are allowed to perform repairs/maintenance	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. 12.1.4
TC213	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, PHYSICAL INFRASTRUCTURE SECURITY, Hardware	Færdig	Network products should use secure firmware images	Network products should use secure firmware images EVIDENCE Verification of the firmware images confirms that they are secured with cryptographic tools such as digital signatures. Verification of the network product confirms that automated tools for downloading, scheduling, and installing firmware images are installed	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	NA
TC242	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource support and operations processes	Færdig	MNO correctly manages the design of any improvements or changes to the operational support processes for new resource capabilities and infrastructure	MNO correctly manages the design of any improvements or changes to the operational support processes for new resource capabilities and infrastructure EVIDENCE Documented evidence that a network product and its compliance reports and accreditation status are evaluated in light of internal policies when improving or changing operational support processes	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.2.5

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC246	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource capability delivery process, Resource Management & Operations Processes	Færdig	Ensure that relevant requirements are met and prerequisites are in place before new resource infrastructure is deployed and handed over to operations	Ensure that relevant requirements are met and prerequisites are in place before new resource infrastructure is deployed and handed over to operations EVIDENCE MNO has documented processes in place to take into use new resource infrastructure. These documented processes include checks to ensure that the resource requirements are met and other prerequisites are satisfied	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.2.7
TC247	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource Development & Retirement Process	Færdig	Resource specifications for 5G components should be developed	Resource specifications for 5G components should be developed EVIDENCE MNO has documented processes to define and document technical, performance, and operational specifications for components	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.3.4
TC255	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource management and operation processes	Færdig	Adequate processes for resource provisioning should be in place	Adequate processes for resource provisioning should be in place EVIDENCE MNO has documented processes for i) creation and deployment of support tools for resource deployment, ii) scheduling, management, and monitoring of the new infrastructure roll-out, and iii) monitoring of newly deployed infrastructure to provide early detection of potential shortfalls	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.4.1
TC256	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource management and operation processes	Færdig	Adequate processes to support resource performance management	Adequate processes to support resource performance management EVIDENCE MNO has documented processes to monitor and assess resource infrastructure performance	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.4.2
TC257	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Resource management and operation processes	Færdig	Adequate processes to support resource trouble management	Adequate processes to support resource trouble management EVIDENCE MNO has documented processes for resource trouble management, such as statistically driven preventive maintenance	a) Set up operational procedures and assign responsibilities for operation of critical systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.4.3
TC293	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, MNO PROCESSES, Security Management	Færdig	Security management processes should be used for operational deployment considerations	Security management processes should be used for operational deployment considerations EVIDENCE Verify that documented operational procedures across the company, including division of responsibilities and monitoring capabilities, are guided by security management principles of prevention, monitoring, detection, analysis and incident management	a) Set up operational procedures and assign responsibilities for operation of critical systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.7.2.2.4
TC244	TELE, 5G, OPERATIONS MANAGEMENT, CHANGE MANAGEMENT, MNO PROCESSES, Resource capability delivery process	Færdig	Integration process of existing legacy infrastructure with the new resource infrastructure should be robust	Integration process of existing legacy infrastructure with the new resource infrastructure should be robust EVIDENCE Documented migration policies/processes and/or project logs which indicate upon review that the migration project is based on standards and best practices	a) Follow predefined methods or procedures when making changes to critical systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.2.4
TC249	TELE, 5G, OPERATIONS MANAGEMENT, CHANGE MANAGEMENT, MNO PROCESSES, Resource Development & Retirement Process	Færdig	Resource deployment should be managed	Resource deployment should be managed EVIDENCE MNO has documented processes for coordinated deployment of new resources	c) Document change management procedures, and record for each change the steps of the followed procedure		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.3.6
TC087	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Unused software components/libraries which are not needed for operation or functionality of the network product are not installed or are deleted after installation	Unused software components/libraries which are not needed for operation or functionality of the network product are not installed or are deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data) EVIDENCE Identification of software components/libraries installed on a network product with command line tools matches the list of software components/libraries in product documentation that are necessary for the correct operation of the network product	b) Implement policy/procedures for asset management and configuration control		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.3 3GPP TS 33.216 3GPP TS 33.511-519
TC088	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Unused software should be deleted or deinstalled	Unused software should be deleted or deinstalled. If that is not possible, such functions should be permanently deactivated in the configuration and they should not be reactivated after reboot. Hardware functions which are not required for operation or function of the system (e.g. unused interfaces) should be deactivated permanently EVIDENCE Identification of hardware and software functions which are installed in the system or might have been disabled using any suitable command line tools or other suitable means of determination matches with the hardware and software functions listed in the product documentation that are necessary for the correct operation of the network product	b) Implement policy/procedures for asset management and configuration control		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.4 3GPP TS 33.216 3GPP TS 33.511-519
TC089	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Network product does not contain software and hardware components that are no longer supported by their vendor, producer, or developer	Network product does not contain software and hardware components that are no longer supported by their vendor, producer, or developer EVIDENCE Verify that there is no entry in the list of hardware and software installed which is not supported by the vendor, producer, or developer of the network product	b) Implement policy/procedures for asset management and configuration control		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.5 3GPP TS 33.216 3GPP TS 33.511-519
TC154	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, NETWORK FUNCTION VIRTUALIZATION - MANO, VNF	Færdig	Configuration management including careful planning, detailed documentation, configuration review, testing before production, and periodic security configuration checks	Configuration management including careful planning, detailed documentation, configuration review, testing before production, and periodic security configuration checks EVIDENCE Detailed documentation of various configuration options. Presence of tools to allow testing of configuration before production as well as checks and notifications of configuration during operation	b) Implement policy/procedures for asset management and configuration control		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 001, cl. 7.1

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC155	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, NETWORK FUNCTION VIRTUALIZATION - MANO, NFV MANO	Færdig	Instantiation of MANO components and managed entities only at explicit geographic locations	Instantiation of MANO components and managed entities only at explicit geographic locations. Support for attribute-based access control and multi-factor authentication where location is one of the attributes/factors EVIDENCE Verification method: attempts to instantiate MANO components in unauthorized locations are unsuccessful	b) Implement policy/procedures for asset management and configuration control		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS NFV-SEC 014, cl. 6
TC053	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	If access to personal data in clear text is required, any access to this data is logged and the log information includes the user identity that has accessed the data	If access to personal data in clear text is required, any access to this data is logged and the log information includes the user identity that has accessed the data EVIDENCE Access logs of the network product show that all access attempts to personal data (in clear text) are recorded in the relevant logs, with the user identity of the person accessing included and no personal data visible in the log	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.5 3GPP TS 33.216 3GPP TS 33.511-519
TC066	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING , IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	Færdig	Security events are logged together with a unique system reference	Security events are logged together with a unique system reference (e.g. host name, IP or MAC address) along with the exact time of the incident. Network product documentation should provide a list of security events and event data (such as username, length of session etc.) the product logs and where they are stored EVIDENCE Review security event log files of the network product to check (1) that they are indeed triggered by security events described in the network product documentation and (2) that they contain the relevant event data	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.6.1 3GPP TS 33.216 3GPP TS 33.511-519 IETF RFC 3871, cl. 2.11.10
TC067	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	Færdig	Network Products support forwarding of security event logging data to an external central system with secure transport protocols	Network Products support forwarding of security event logging data to an external central system with secure transport protocols EVIDENCE Check that the network product documentation contains a list of standard security protocols for transferring event logging data. Confirm that successful test sessions using the standard protocols listed by the manufacturer in the documentation can be setup between the product and the central system where event logging data is sent. Packet captures confirm that the protocol used for transferring logs provides encryption, integrity protection, and replay protection	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.6.2 3GPP TS 33.216 3GPP TS 33.511-519
TC068	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, CORE NETWORK, RADIO NETWORK, NETWORK FUNCTION VIRTUALIZATION - MANO, MULTI ACCESS EDGE COMPUTING, IMPLEMENTATION OPTIONS , UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	Færdig	Security event log has appropriate access control mechanism allowing only privileged users with the necessary rights to have access to the log files	Security event log has appropriate access control mechanism allowing only privileged users with the necessary rights to have access to the log files EVIDENCE Verify that security event log files of the network product are accessible when signed in with a user account with appropriate authorization. Verify that security event log files are not accessible when singed in as a user without the correct permissions	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.6.3 3GPP TS 33.216 3GPP TS 33.511-519
TC075	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	Færdig	Access to the webserver is logged and the webserver access logs contain sufficient information	Access to the webserver is logged and the webserver access logs contain at least the following information: access timestamp, source IP address, account/login name if known, requested URL, and status code of response EVIDENCE Checking the webserver access logs confirms that all webserver events are logged along with the required log information listed in the 'Control' section	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.2 3GPP TS 33.216 3GPP TS 33.511-519
TC144	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NETWORK SLICING, Network Slice Instance	Færdig	Appropriate logging and auditing mechanisms should be implemented throughout the slice life cycle	Appropriate logging and auditing mechanisms should be implemented throughout the slice life cycle. Real-time analysis of security events in the logs should be performed to immediately detect any attempted attacks EVIDENCE System logs of the network slice instance contain event information and timestamps of the following slice life-cycle stages: 1) Preparation phase; 2) Installation, Configuration, and Activation phase; 3) Run-time phase; 4) Decommissioning phase	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020
TC147	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NETWORK SLICING, Network Slice Instance	Færdig	All resources and network functions consumed by a slice are monitored	All resources and network functions consumed by a slice are monitored EVIDENCE Log files of a slice contain detailed information of the resources and network functions consumed	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp.
TC167	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, SOFTWARE DEFINED NETWORKS, SDN Controller	Færdig	Appropriate logging and auditing mechanisms should be implemented in the SDN control layer	Appropriate logging and auditing mechanisms should be implemented in the SDN control layer EVIDENCE Check that log files containing event information and timestamps are present in the SDN controller. Check that tools for auditing log files at regular intervals are installed	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	Rec. ITU-T X.1038, cl. 7.2.2 R-17

Overskrift	Emneord	Status	Anbefaling	Anvisning	Formål	Bemærk-ninger	Sikkerheds-koncept	Beskyttelses-fomål	Forud-sætning	Organisatorisk niveau	Område-model	I overensstemmelse med (EU)	Referencer
TC171	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MULTI ACCESS EDGE COMPUTING, Application data traffic, MEC host	Færdig	MEC system collects charging related data, logs it securely, and makes it available for further processing	MEC system collects charging related data, logs it securely, and makes it available for further processing EVIDENCE Log files in MEC components include information such as traffic usage, application instantiation, access, usage duration, resource usage, etc. Log files are accessible only to authorized users. Packet captures confirm that the transport protocol used for making the log files available to other components is secure	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ETSI GS MEC 002, cl. 8.3
TC184	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MULTI ACCESS EDGE COMPUTING, MEC host	Færdig	Event logs containing user activities, exceptions, faults, and information security events are generated, stored, and reviewed	Event logs containing user activities, exceptions, faults, and information security events are generated, stored, and reviewed. These logs are integrated and corelated with service provider monitoring mechanisms EVIDENCE Verify that event logs are integrated and corelated with service provider monitoring mechanisms and that they contain user activities, exceptions, faults, and information security events, as appropriate	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. A.12.4.1 ITU-T X.1205
TC212	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, PHYSICAL INFRASTRUCTURE SECURITY, Physical asset	Færdig	Adequate monitoring of hardware parameters	Adequate monitoring of hardware parameters EVIDENCE Check that (1) hardware resources are monitored with both physical and virtual sensors; (2) alarms and alerts are in place to notify of impending hardware failures and (3) that documented processes are in place for responding to alarms and alerts to ensure preventive maintenance	c) Set up tools for monitoring critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. 12.1.4
TC270	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MNO PROCESSES, Security Data	Færdig	Security and management data should be accurate, timely, and complete	Security and management data should be accurate, timely, and complete EVIDENCE MNO has documented processes and tools to collect performance, management and security data from networks, systems and security sensors, as well as distribute the information to other processes/services. Presence of performance and security data in logs	a) Implement monitoring and logging of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.7.1
TC271	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MNO PROCESSES, Security Data	Færdig	Security and management data should be properly processed	Security and management data should be properly processed EVIDENCE MNO has documented processes and tools to process security and management data. Review of security and management data shows processing according to intended recipient processes, resource instances, or service instances (e.g.: privacy sensitive identifiers are removed from logged data)	d) Set up tools to collect and store logs of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.7.2
TC273	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MNO PROCESSES, Performance data	Færdig	Resource performance should be monitored	Resource performance should be monitored EVIDENCE MNO has documented processes and tools for monitoring performance information and for detecting performance degradation/threshold violations. Recent monitoring records (e.g. reports).	d) Set up tools to collect and store logs of critical systems		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.5.9.1
TC294	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MNO PROCESSES, Security Management	Færdig	Tools for capturing relevant operational data should be used and regularly updated	Tools for capturing relevant operational data should be used and regularly updated EVIDENCE Verify that MNO has tools and infrastructure for data collection of operational activity. Documented and updated i) monitoring policy, ii) processes, iii) monitoring logs, iv) monitoring reports, v) policy/processes/capabilities (including tools) review comments, and vi) change logs	f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.7.2.2.5
TC298	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, MNO PROCESSES, Security Management	Færdig	Policy-based processes and tools for collection, filtering, aggregation, distribution, and retention of data should be used and regularly updated	Policy-based processes and tools for collection, filtering, aggregation, distribution, and retention of data should be used and regularly updated EVIDENCE MNO has documented policy-based security monitoring procedures/tools for data collection and storage. MNO has records of reviews of these procedures and tools, including review comments, and/or change logs	f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.7.2.2.9
TC285	TELE, 5G, MONITORING, AUDITING AND TESTING, EXERCISE CONTINGENCY PLANS, MNO PROCESSES, BCM Processes	Færdig	Infrastructure recovery planning should be undertaken	Infrastructure recovery planning should be undertaken EVIDENCE MNO has documented up-to-date recovery procedures and backup planning which are proactively and regularly tested for ensuring business continuity. Reports of tests/exercises showing execution of recovery procedures and lessons learnt	b) Implement a program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time		Protect	Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	eTOM 20, cl. 1.7.2.1.3
TC181	TELE, 5G, MONITORING, AUDITING AND TESTING, NETWORK AND INFORMATION SYSTEMS TESTING, MULTI ACCESS EDGE COMPUTING, MEC applications, Edge Application Server (EAS)	Færdig	A regular security testing program is used for identifying and mitigating vulnerabilities in MEC applications in a timely manner	A regular security testing program is used for identifying and mitigating vulnerabilities in MEC applications in a timely manner EVIDENCE A documented policy for regular testing of MEC applications exits. Check for testing reports, logs from testing tools, review comments, and change logs. Verify that tools are available for isolating applications until remedial updates are available once vulnerabilities are detected	b) Implement policy/procedures for testing network and information systems		Protect	Fortrolighed, Integritet, Tilgængelighed		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	ISO/IEC 27011, cl. A.18.2.3
TC117	TELE, 5G, THREAT AWARENESS, INFORMING USERS ABOUT THREATS, CORE NETWORK, RADIO NETWORK, AMF, MME, gNB, eNB	Færdig	Visibility of the operation of AS confidentiality and integrity, as well as, NAS confidentiality and integrity should be provided to the user/application	Visibility of the operation of AS confidentiality and integrity, as well as, NAS confidentiality and integrity should be provided to the user/application. The serving network identifier information should be available to applications in the UE EVIDENCE Verify that the status of AS confidentiality and integrity, as well as NAS confidentiality and integrity shown in a test application on the UE matches with the use of confidentiality and integrity reflected in the packet captures on the gNB/eNB/AMF/MME/. Verify that the serving network identifier shown by a test application on the UE is the serving network identifier for the operator network to which the UE is connected	a) Inform end-users of communication networks and services about particular and significant security threats to network or service that may affect them		Protect	Fortrolighed, Integritet		Implementering og Drift	Tek.	ENISA 5G Security Controls Matrix 20210910	3GPP TS 33.501, cl. 5.10.1