ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO2-001	TC179	TELE, 5G, GOVERNANCE AND RISK MANAGEMENT, GOVERNANCE AND RISK MANAGEMENT, Virtual Infrastructure, Virtual Infrastructure Manager (VIM)	SA and NSA	(Private), Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
SO4-004	TC365	TELE, 5G, GOVERNANCE AND RISK MANAGEMENT, SECURITY OF THIRD PARTY DEPENDENCIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	SBOM for software components (including NFV software components) is maintained	SBOM for software components (including NFV software components) is maintained. This makes it possible to quickly scan and search the SBOM for any Zero-Day vulnerability once disclosed, allowing the MNO and the cloud provider to respond quickly to such vulnerability to mitigate potential attacks. SBOM should follow the NTIA guidelines and be in a machine-readable format, such as SPDX, or CycloneDX. EVIDENCE Verify that the software package includes a SBOM.	a) Include security requirements in contracts with third-parties, including confidentiality and secure transfer of information	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	NTIA - The Minimum Elements For a Software Bill of Materials (SBOM), cl. I, 'Automation Support', 'Recommended Data Fields' GSMA - Open Networking & the Security of Open Source Software Deployment, cl. 'The Software Development Process', 'Virtualisation Layer Code'
SO4-039	TC387	TELE, 5G, GOVERNANCE AND RISK MANAGEMENT, SECURITY OF THIRD PARTY DEPENDENCIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Third party hosting environments that support VNFs should meet 3GPP virtualisation security requirements	Third party hosting environments that support VNFs should meet 3GPP virtualisation security requirements. EVIDENCE Verification of an appropriate evaluation report or security certification of a VNF confirming that the VNF meets 3GPP SCAS specifications.	e) Demand specific security standards in third-party supplier's processes during procurement	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.848, cl. 5.21.3
SO9-002	TC207	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PHYSICAL AND ENVIRONMENTAL SECURITY, Physical asset, Cloud data center, Light data center	SA and NSA	Private, Hybrid, (Public)	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. Physical security measures cover (multi-vendor) spare part management. Physical security policy should allow remote shutdown (or data clearing) for ciritcal stolen equipment and/or re-authentication/re-configuration after a physical attack or power failure 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, (multi-vendor) spare part management. Such policy/policies list critical assets and their respective controls. Relevant documented procedures that allow physical access only to security-vetted, trained, and qualified staff. Documented procedures contain measures allowing vendors access only to equipment sourced from them. Log containing records of physical access, especially by third parties and contractors. On-site inspection to verify implementation of the relevant controls. Visual verification of equipment shutdown after issuing test remote shutdown command. Verify memory contents via debug interface after issuing a test remote wipe command on equipment. Logs on critical equipment confirm re-authentication after simulating power failure or physical attack events	c) Industry standard implementation of physical and environmental controls	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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 NIST.SP.800-53-Rev.5, PF1-PF3, PF8, and PF10
SO11-001	TC014	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, SMF	SA	Private, (Hybrid), (Public)	Færdig	UPF (or SMF depending on MNO) 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 MNO) 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO11-002	TC021	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 32.255, cl. 5.1 3GPP TS 33.515, cl. 4.2.2.1.4
SO11-003	TC060	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO11-004	TC065	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117 4.2.3.5 3GPP TS 33.216 3GPP TS 33.511-519
SO11-005	TC073	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.2.2 3GPP TS 33.216 3GPP TS 33.511-519
SO11-006	TC076	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
SO11-007	TC077	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
SO11-008	TC078	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
SO11-009	TC079	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.3 3GPP TS 33.216 3GPP TS 33.511-519
SO11-010	TC142	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.813, cl. 6.2
SO11-011	TC150	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFV MANO	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 014, cl. 6
SO11-012	TC165	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SDN Controller	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-10, R-11, R-12, R-13, R-14
SO11-013	TC317	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF, AUSF, NEF, UDM	SA	Private, (Hybrid), (Public)	Færdig	AKMA reuses the same UE subscription and the same credentials used for 5G access	AKMA reuses the same UE subscription and the same credentials used for 5G access EVIDENCE Verify that a test UE with 5G credentials can connect to an MNO network and an application function (AF) supporting AKMA. Logs at the AF, AAnF, and AUSF confirm successful reuse of UE 5G credentials for authenticating access to the 5G network and to the AF	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 4.4.0
SO11-014	TC318	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF, AUSF, NEF, UDM	SA	Private, (Hybrid), (Public)	Færdig	AKMA reuses the 5G primary authentication procedure for implicit authentication to AKMA services	AKMA reuses the 5G primary authentication procedure for implicit authentication to AKMA services EVIDENCE Verify that a test UE device with SIM credentials from an MNO can successfully authenticate with EAP-AKA' or 5G AKA. Verify that the same procedure is used when authenticating to an AF supporting AKMA. Logs at the AF, AAnF, and AUSF confirm reuse of primary authentication during AKMA authentication	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 4.4.0
SO11-015	TC320	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF	SA	Private, (Hybrid), (Public)	Færdig	A-KID should be globlly unique	A-KID should be globlly unique EVIDENCE Logs at the AAnF show unique/non-repeating A-KIDs	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 4.4.2
SO11-016	TC321	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF	SA	Private, (Hybrid), (Public)	Færdig	AAnFs should implement Naanf_AKMA_AnchorKey_Register service in accordance with the 3GPP technical specification	AAnFs should implement Naanf_AKMA_AnchorKey_Register service in accordance with 3GPP technical specification 33.535, clause 7.1.2 EVIDENCE Verify via logs at the AAnF that it stores the AKMA related key material associated with a SUPI on sending a request containing the SUPI, A-KID, and KAKMA	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 7.1.2
SO11-017	TC322	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF	SA	Private, (Hybrid), (Public)	Færdig	AAnFs should implement Naanf_AKMA_ApplicationKey_Get service in accordance with the 3GPP technical specification	AAnFs should implement Naanf_AKMA_ApplicationKey_Get service in accordance with 3GPP technical specification 33.535, clause 7.1.3 EVIDENCE Verify via packet captures at the AAnF that it responds with the KAF, KAF expiration time, and SUPI on sending a request containing the A-KID and AF_ID	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 7.1.3

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO11-018	TC323	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF	SA	Private, (Hybrid), (Public)	Færdig	AAnFs should implement Naanf_AKMA_Context_Remove service in accordance with the 3GPP technical specification	AAnFs should implement Naanf_AKMA_Context_Remove service in accordance with 3GPP technical specification 33.535, clause 7.1.4 EVIDENCE Verify via logs at the AAnF that it removes AKMA related key material associated with a SUPI on sending a request containing that SUPI	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 7.1.4
SO11-019	TC324	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AAnF	SA	Private, (Hybrid), (Public)	Færdig	AAnFs should implement Naanf_AKMA_ApplicationKey_ AnonUser_Getservice service in accordance with the 3GPP technical specification	AAnFs should implement Naanf_AKMA_ApplicationKey_ AnonUser_Getservice service in accordance with 3GPP technical specification 33.535, clause 7.1.5 EVIDENCE Verify via packet captures at the AAnF that it responds with the KAF, KAF expiration time, and optionally the GPSI on sending a request for anonymous AF access containing the A-KID and AF_ID	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 7.1.5
SO11-020	TC325	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NEF	SA	Private, (Hybrid), (Public)	Færdig	NEFs should implement Nnef_AKMA_ApplicationKey_Get service in accordance with the 3GPP technical specification	NEFs should implement Nnef_AKMA_ApplicationKey_Get service in accordance with 3GPP technical specification 33.535, clause 7.1.5 EVIDENCE Verify via packet captures at the NEF that it responds with the KAF, KAF expiration time, and optionally the GPSI on sending a request containing the A-KID and AF_ID	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 7.3.2
SO11-021	TC331	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, VAL server	SA	Private, (Hybrid), (Public)	Færdig	VAL users authenticated and are provided access tokens	VAL users authenticated and are provided access tokens with OAuth 2.0, OpenID Connect 1.0, or ACE-Oauth for light-weight protocol realizations EVIDENCE Verify that a test user can authenticate and obtain an authorization token from the SIM-S over the IM-UU interface. Logs at the SIM-S confirm successful authentication of the test user	a) Users and systems have unique ID's and are authenticated before accessing services or systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.2.3
SO11-022	TC004	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO11-023	TC009	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AMF/SEAF, AUSF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.6/6.1.3.2 3GPP TS 33.512, cl. 4.2.2.1.2
SO11-024	TC010	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AUSF	SA	Private, (Hybrid), (Public)	Færdig	AUSFs should implement Nausf_UEAuthentication service in accordance with 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.1
SO11-025	TC013	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AMF/SEAF, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO11-026	TC019	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.2
SO11-027	TC020	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UDM	SA	Private, (Hybrid), (Public)	Færdig	UDMs should implement Nudm_UEAuthentication_ResultConfirmatio n 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.2
SO11-028	TC022	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 23.501, cl. 5.10.3 3GPP TS 33.515, cl. 4.2.2.1.1
SO11-029	TC023	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SMF	SA	Private, (Hybrid), (Public)	Færdig	During a handover, the 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	During a handover, the 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.6.1 3GPP TS 33.515, cl. 4.2.2.1.3
SO11-030	TC028	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.2.4.7 3GPP TS 33.517, cl. 4.2.2.4
SO11-031	TC029	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	Færdig	Ensure correct implementation of handling of serving PLMN ID mismatch corresponding to the N32-f context Id in the N32 message	SEPP 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.4.1.2 3GPP TS 33.517, cl. 4.2.2.4
SO11-032	TC031	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.2.3.6 3GPP TS 33.517, cl. 4.2.2.6
SO11-033	TC035	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.2.4.1 3GPP TS 33.517, cl. 4.2.2.8
SO11-034	TC036	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NRF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO11-035	TC037	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NRF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.3
SO11-036	TC040	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NEF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.2.3/12.4/13.4 3GPP TS 33.519, cl. 4.2.2.1.1
SO11-037	TC059	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	System functions (such as the Management Plane) are not accessed without successful authentication and authorization	System functions (such as the Management Plane) are not accessed without successful authentication and authorization. Access control policy should restrict and/or control remote access by third parties, especially by suppliers or managed service providers considered to be high-risk or accessing the network from outside of EU. If necessary, only temporary onsite/remote access to third parties should be provided and no permanent credentials are disclosed EVIDENCE Verify that attempts to access a system function are only successful when logged in as a user with adequate privileges. Verify access logs to confirm that attempts for remote access by third parties are either denied, or restricted (e.g. one-time short-lived access grant), according to the documented policy (see control description). Access logs confirm that onsite/remote access by third parties, if allowed, is based on temporary or one-time passwords used only for designated tasks	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.1.1 3GPP TS 33.216 3GPP TS 33.511-519 NIST.SP.800-53-Rev.5, AC-2, AC-3, AC-4, AC-6, and AC-17
SO11-038	TC064	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, PSF, ISF, VSF, LCM proxy, MEC orchestrator, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	A centralized Privileged Access Management (PAM) solution is in place	A centralized Privileged Access Management (PAM) solution is in place. 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. Access control policy is reviewed and revised based on 5G risk assessment EVIDENCE Access to critical or sensitive network components is captured in logs of the PAM solution. 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. MNO has documented access control policy explaining how various rights in the network, such as access rights between network functions, network administrators' rights and alike are minimized. Review of policy, logs, comments and comparison with prior versions indicate that access control policy is reviewed and revised periodically in the context of evolving 5G risks.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.6 3GPP TS 33.216 3GPP TS 33.511-519 NIST.SP.800-53-Rev.5, AC-2, AC-3, AC-4 and AC-6
SO11-039	TC072	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.2.1 3GPP TS 33.216 3GPP TS 33.511-519

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO11-040	TC086	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions, NFVI, VNF, MANO	SA and NSA	Private, Hybrid, (Public)	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), or by implementing devices such as a virtual firewall, hardware firewall, or a third-party firewall agent. 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. Check that the document lists firewall rules. Verify that the network product does not reply to messages with types which are not permitted: Send samples of malicious messages to the network product and verify that the messages are dropped on receipt by the network product (e.g. by means of appropriate firewall rules), and that the network product's applicable system configuration remains unchanged upon receipt of the messages.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.2 3GPP TS 33.216 3GPP TS 33.511-519
SO11-041	TC091	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.7 3GPP TS 33.216 3GPP TS 33.511-519
SO11-042	TC118	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEAF, AUSF, UDM	SA	Private, (Hybrid), (Public)	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 MNO 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.1/Annex F
SO11-043	TC125	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NSSAAF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.4
SO11-044	TC126	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NSSAAF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.4
SO11-045	TC127	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NSSAAF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.4
SO11-046	TC135	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Service Based Interfaces, Os-Ma-Nfvo	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.1.1
SO11-047	TC141	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Network Slice Instance	SA	Private, Hybrid, (Public)	Færdig	Access to the network management interface is authorized using OAuth 2	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.4.1
SO11-048	TC149	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Control Plane	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 5.17
SO11-049	TC157	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtualized resources	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 003, cl. 4.4.2.1.2
SO11-050	TC175	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, MEC platform, MEC application, Edge Application Server (EAS)	SA and NSA	(Private), Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS MEC 002, cl. 8.1
SO11-051	TC177	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtual Infrastructure, Virtual Infrastructure Manager (VIM)	SA and NSA	(Private), Hybrid, (Public)	Færdig	Virtualization platforms or container infrastructure supporting role-based access control in MEC are in use	Virtualization platforms or container infrastructure 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
SO11-052	TC182	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtualization infrastructure, MEC host, MEC platform	SA and NSA	(Private), Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ISO/IEC 27011, cl. 8.2
SO11-053	TC222	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtualization assets	SA	Private, Hybrid, (Public)	Færdig	Protection against VM escape	VM escape protection: To prevent an attacker from utilising a VNF vulnerability to attack the virtualisation layer and gain control over it, the virtualisation layer shall reject abnormal access from the VNF ('abnormal' is understood as, for example, the VNF accessing memory not allocated to it) and log the attack. Access filtering rules should be defined in the VNF descriptor to allow enough capability for correct execution of the VNF as a permitted list of calls depending on the VNF. Access filtering rules shall be included in the VNF Package as a descriptor in the MCIOP, or in a separate security file. EVIDENCE Documentation of the virtualisation platform confirms that VM segregation is supported. Inspection of the virtualisation platform with diagnostic tools confirms functional segregation of VMs. Test: Attempt abnormal access to the virtualisation layer and check that the virtualisation layer rejects the abnormal access from the VNF and logs the attack. Verify that the access filtering policies are included either in the MCIOP or in a separate security file (descriptor) in the VNF package.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.6.7.4
SO11-054	TC332	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEAL server	SA	Private, (Hybrid), (Public)	Færdig	SEAL servers provide service access only to authorized users	SEAL servers provide service access only to authorized users EVIDENCE Verify via logs at the SEAL server that requests from a SEAL client without an access token or with an invalid access token are rejected. Verify via logs at the SEAL server that service access is granted when a valid access token is presented	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.2.2
SO11-055	TC333	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, VAL server	SA	Private, (Hybrid), (Public)	Færdig	VAL servers provide service access only to authorized users	VAL servers provide service access only to authorized users EVIDENCE Verify via logs at the VAL server that requests from a VAL client without an access token or with an invalid access token are rejected. Verify via logs at the VAL server that service access is granted when a valid access token is presented	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.2.6
SO11-056	TC341	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Administration of the virtualisation fabric : Access to the management plane needs to be temporary and time-bound	Administration of the virtualisation fabric : Access to the management plane needs to be temporary and time-bound. The MNO needs to constrain the number of administrator accounts able to modify the Virtualisation Fabric, and the number of administrators, to a minimal manageable number to meet their needs. Administrators need to be prevented from being able to grant themselves privileged access to the network, and should not have access to the host's hardware or the virtualised workloads running within the environment. All administrative access needs to be logged, and the activity of the session recorded. Manual administration of the Virtualisation Fabric (e.g. access to a command line on host infrastructure) should raise a security incident. The devices and locations from which the fabric can be modified should be limited. Functions that support the administration and security of the Virtualisation Fabric should not be run on the fabric itself, and should be considered as Security Critical functions running on separate dedicated hardware. EVIDENCE Verify that restrictions are set properly for administrators allowed to manage the virtualisation fabric. Mount an external file system prepared by a tester with files exploiting privilege escalation methods. Subsequently, attempt gaining privileged access by using a suitable privilege escalation method with the contents of the mounted file system. Confirm that privilege escalation has not occurred.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 6.4
SO11-057	TC343	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Access control on NFV of admins attempting to gain access to the NFV resources (VNF or the NFVI)	Access control on NFV of admins attempting to gain access to the NFV resources (VNF or the NFVI). Two potential solutions: • Ticket-based authentication system and Attribute Based Access Control (ABAC) such as Kerberos, specified in IETF RFC 4120 • Token-based authorization framework such as OAuth 2.0, specified in IETF RFC 6749 EVIDENCE Verify that the access token is based on OAuth 2.0. In case of a verification failure, check that NFV resources reject the request based on OAuth 2.0 error response defined in RFC 6749. Verify that the access ticket based on Kerberos. In case of a verification failure, check that NFV resources reject the request based on Kerberos error response defined in RFC 4120. Examples of tests for the verification failure of the access token/ticket integrity: 1. Compute an access token/ticket correctly, except that the signature or the MAC is incorrect, e.g., the signature or the MAC is randomly selected, and then includes the access token/ticket in the Request. The integrity verification by NFV resources of the access token/ticket fails. 2. Compute an access token/ticket correctly, except that the expiration time has expired against the current data/time, and then includes the access token/ticket in the Request sent to NFV resources. NFV verifies that the integrity of the access token/ticket, is valid. However, the expiration time in the access token/ticket has expired against the current data/time.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 6.8 ETSI GS NFV-SEC 003, cl. 4.4.6.2

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO11-058	TC344	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	VNF lifecycle management security: 1) VNF authenticates VNFM when VNFM initiates communication with VNF	VNF lifecycle management security: 1) VNF authenticates VNFM when VNFM initiates communication with VNF. 2) VNF establishes securely protected connection with the VNFM. 3) VNF checks whether VNFM has been authorized when VNFM accesses VNF's API. 4) VNF logs VNFM's management operations for auditing. EVIDENCE Trigger the establishment of communication between the VNF and the VNFM. Capture the communication between the VNF and the VNFM using a tool (e.g. wireshark). Check whether the VNF authenticates the VNFM according to the mechanism described in the vendor's document. For example, the VNF can use HTTPS to communicate with the VNFM, and the VNF uses VNFM's certificate for authentication. Check whether the VNF establishes a secure connection with the VNFM after successful authentication. For example, a TLS connection is established after the VNF successfully authenticates the VNFM. Check whether the VNF authorizes the VNFM according to the mechanism described in vendor's document. For example, VNF can use OAuth2.0 to authorize the VNFM. The VNF uses VNFM's token for authorization. Check whether the VNF logs the operations from VNFM by reviewing VNF logs.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GR NFV 003, cl. 4.4 3GPP TR 33.818, cl. 5.2.5.5.7.1
SO11-059	TC346	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) is separated from the network used for the communication between VNFs (inter-VNF traffic) to prevent security threats from spreading between different networks	The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) is separated from the network used for the communication between VNFs (inter-VNF traffic) to prevent security threats from spreading between different networks. Software defined traffic rules applied directly to each virtual function are used to limit both incoming and outgoing traffic in an efficient and scalable way. Each VNF has at least two separate (logical) interfaces dedicated to different network domains. EVIDENCE A document containing the definition of trust domains and the separation requirements to be implemented and enforced. A document containing the software defined rules. Verification that those rules are implemented: - Check whether the inter-VNF traffic and intra-VNF traffic are separated according to the documentation stating the software defined rules, network domains and separation requirements. - A VNF has at least two separate (logical) interfaces dedicated to different network domains. Check whether the VNF refuses traffic intended for one network domain on all interfaces meant for the other network domain, and vice versa. Perform this check for all pairs of different network domains. - Check whether a VNFCI refuses inter-VNF traffic on all intra-VNF interfaces. For example, by way of sending a ping to all intra-VNF interfaces through an inter-VNF interface. - Check whether a VNFCI refuses intra-VNF traffic on all inter-VNF interfaces. For example, by way of sending a ping to all inter-VNF interfaces through an intra-VNF interface.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.5.8.5.2
SO11-060	TC354	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	When a VNF moves from one host to another or when a VNF is terminated, the system should ensure that resources, privacy sensitive data, and/or keys are fully and securely cleared	When a VNF moves from one host to another or when a VNF is terminated, the system should ensure that resources, privacy sensitive data, and/or keys are fully and securely cleared. In addition, the hypervisor or the CIS should be configured to securely wipe out the virtual volume disks in the event a VNF is crashed or intentionally destroyed to prevent its resources from unauthorised access. EVIDENCE A documented privacy impact assessment (PIA) for personally identifiable information (PII) identifying privacy risks to data assets and appropriate mitigating actions. Documented security policies restricting where certain types of data can reside and how sensitive data is cleared. Verify using testing and analysis tools that hypervisor or CIS is properly configured for securely wiping out the virtual volume disks in the event a VNF is crashed or intentionally destroyed. Such tools for detecting misconfigurations include: - In Kubernetes: kubeaudit, kubesec.io, kube-bench - In Docker: inspec.io, dev-sec.io, Docker Bench for Security - In Openstack: Tempest, Shaker, OS-Faults - In VMWARE: ONTAP, Log Insight	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ERICSSON Security Considerations of Cloud RAN August 2021, cl. 'Data protection and privacy' OWASP - Kubernetes Security Cheat Sheet, cl. 'If breached, scale suspicious pods to zero', 'Use Pod Security Policies to prevent risky containers/Pods from being used' VMWARE - Top 10 VMware Admin Tools OpenStack testing tools
SO11-062	TC391	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtualization infrastructure, MEC host, MEC platform, MEC application, MEC orchestrator	SA	(Private), Hybrid, (Public)	Færdig	The MEC platform should authenticate all MEC application instances, and only provide them with the information for which the application is authorized	The MEC platform should authenticate all MEC application instances, and only provide them with the information for which the application is authorized. OAuth 2.0 based on X.509 client certificates are used for authorization of access to RESTful MEC service APIs defined by ETSI ISG MEC. In case of service-producing applications defined by third parties, other mechanisms such as standalone use of JWT can be used to secure related APIs. EVIDENCE Verification that the MEC platform and applications use OAuth for authentication and authorization following ETSI ISG MEC and IETF RFC 6749. Verification can involve looking at product documentation and establishing test OAuth connections. Verification that invocation of MEC service APIs with valid OAuth tokens is successful. Verification that MEC platform rejects malformed access tokens with incorrect fields/values and sends an OAuth error response.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI White Paper No. 46, cl. 2.2, 3.2
SO11-063	TC392	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	OSS systems should be consistent with the ETSI NFV architectural framework ETSI GS NFV 002 and support the Os-Ma interface between the traditional OSS/BSS and the NFV management and orchestration (MANO) framework	OSS systems should be consistent with the ETSI NFV architectural framework ETSI GS NFV 002 and support the Os-Ma interface between the traditional OSS/BSS and the NFV management and orchestration (MANO) framework. Os-Ma interface uses OAuth for authentication and authorization. EVIDENCE Verification that the Os-Ma interface uses OAuth for authentication and authorization. Verification can involve looking at product documentation and establishing test OAuth connections. Verification that the Os-Ma interface is accessible only with valid OAuth tokens.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ONF - Impact of SDN and NFV on OSS/BSS, cl. 8 ETSI GS NFV 002
SO11-064	TC405	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Control Plane	SA	Private, Hybrid, (Public)	Færdig	Lock-down of infrastructure: All interfaces on physical hosts are locked down to restrict access to trusted hosts, and there is no hard-coded configuration (e	Lock-down of infrastructure: All interfaces on physical hosts are locked down to restrict access to trusted hosts, and there is no hard-coded configuration (e.g. virtual span ports or hard-coded MAC addresses) in the NFVI as these make it significantly harder to update and patch. Virtualisation hosts only open the minimum number of ports required and all ports and services are locked down and managed. EVIDENCE All interfaces are identified in the documentation. Instructions of how an administrator user can use all the interfaces are provided in the documentation. Run a port scanner and verify that the required interfaces are open/reachable. Run a port scanner and verify that unneeded ports are not opn/reachable.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 5.17 3GPP TR 33.848, cl. 6.3
SO11-065	TC406	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, Virtualization assets	SA	Private, Hybrid, (Public)	Færdig	Protection against container escape: - Ensure containers are not running as root by default and do not use unnecessary privileges or mounted components	Protection against container escape: - Ensure containers are not running as root by default and do not use unnecessary privileges or mounted components. In Kubernetes environments, consider defining a Pod Security Policy that prevents pods from running privileged containers. - Use read-only containers, read-only file systems, and minimal images where possible to prevent the running of commands. - Monitor deployment of suspicious or unknown container images and pods, particularly containers running as root. - Monitor installation of kernel modules that could be abused to escape containers to a host. - Monitor unexpected usage of syscalls such as mount that may indicate an attempt to escape from a privileged container to a host. - Monitor process activity (such as unexpected processes spawning outside a container and/or on a host) that might indicate an attempt to escape from a privileged container to a host. - Monitor cluster-level (Kubernetes) data and events associated with changing containers' volume configurations. EVIDENCE By way of reviewing (1) test reports, including testing plans and results captured therein, (2) documented container and host processes and (3) logs associated with container and host activities, verify that during onboarding/instantiation/runtime of containers MNOs perform continuous monitoring for misconfiguration of runtime workloads, container privileges, host, usage of syscalls and container volumes. Documentation of secure configuration of the host, privileges to be associated with containers and authorized usage of syscalls confirms secure isolation between containers, as well as between containers and the host. Inspection of the host with diagnostic tools confirms its secure configuration. Test: Attempt abnormal access from a container to the host and verify that the host rejects such access and logs the attack.	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	MITRE ATT&CK® Containers Matrix 'Escape to Host'
SO11-066	TC050	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.2 3GPP TS 33.216 3GPP TS 33.511-519
SO11-067	TC051	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.3 3GPP TS 33.216 3GPP TS 33.511-519
SO11-068	TC097	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.6 3GPP TS 33.216 3GPP TS 33.511-519
SO11-069	TC358	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The hypervisor or CIS is configured to support multiple administration roles, and as a minimum there must be an admin role (highest privilege) and a separate operational role with minimal privileges	The hypervisor or CIS is configured to support multiple administration roles, and as a minimum there must be an admin role (highest privilege) and a separate operational role with minimal privileges. All administration login attempts must be logged and audited. EVIDENCE Administration document and system logs confirm the correct configuration and the use of administration roles and rules.	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 009, cl. 7
SO11-070	TC359	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Root user isn't used within VM or Containers except during initialization, and privileges are dropped on completion of the runtime	Root user isn't used within VM or Containers except during initialization, and privileges are dropped on completion of the runtime. Containers or VMs cannot be granted any additional privileges during their runtime (for example, 'no-new-privileges' flag in the Container). EVIDENCE A document that describes the interfaces to VMs or Containers and how users can login to them. Verify that the use of root user within VMs or Containers for operations other than initialization is not allowed. The tester tries to login to the VM or Container using the credentials of the root or equivalent highest privileged user to perform operations other than initialization. The tester is not able to perform any such operations using the root credentials. Verify that the use of root user within VMs or Containers for initialization is allowed. The tester tries to login to the VM or Container using the credentials of the root or equivalent highest privileged user for initialization. The tester is able to perform initialization using the root credentials.	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	CIS Docker Benchmark, cl. 2.1, 3 CIS VMWARE Benchmark, cl. 4.1 CIS Kubernetes Benchmark, cl. 1.1, 4.1, 5.2.7 OWASP Container Security Verification Standard, cl. V3 (3.1, 3.9)
SO11-071	TC366	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Sensitive information should never be published in a production VM/Container image	Sensitive information (e.g., private keys, critical configuration files, credentials) should never be published in a production VM/Container image. EVIDENCE Verify through scan that no sensitive information is included in a VM/Container image before its deployment to NFV.	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 021, cl.6

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO11-073	TC027	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.3.2/13.2.2.2/13.5
SO11-074	TC038	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NEF	SA	Private, (Hybrid), (Public)	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 MNO domain, mutual authentication is only based on client and server certificates with TLS. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verification of successful TLS tunnel setup between NEF and application functions. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	d) Choose appropriate authentication mechanisms, depending on the type of access	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.2.3/12.2/12.3 3GPP TS 33.519, cl. 4.2.2.1.1
SO11-075	TC063	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	Access to the Management Plane shall be through a dedicated jump server and require Multi Factor Authentication, wherever feasible	Access to the Management Plane shall be through a dedicated jump server and require Multi Factor Authentication, wherever feasible. Exceptions should follow a defined emergency access procedure. Mutual authentication of entities for management interfaces is implemented. EVIDENCE Network product documentation contains the list of management protocols with a corresponding list of authentication mechanisms, and access control rules used for accessing the management plane and its interfaces. Exceptions and emergency access procedure are documented. Packet captures of each management protocol confirm successful mutual authentication before allowing access. Management plane logs confirm correct use of authentication mechanisms and access control rules.	d) Choose appropriate authentication mechanisms, depending on the type of access	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.4.1 3GPP TS 33.216 3GPP TS 33.511-519
SO11-076	TC115	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl.11.1
SO11-077	TC119	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, N3IWF, AMF, TNAN	SA	Private, Hybrid, (Public)	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 7.1, 7.2, and 7A EVIDENCE Verify that a test UE device with SIM credentials from an MNO can successfully authenticate and use MNO 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 7.1/7.2/7A
SO11-078	TC199	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, eNB, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.310 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
SO11-079	TC200	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, eNB	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.310 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4
SO11-080	TC339	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, HSE	SA	Private, (Hybrid), (Public)	Færdig	HSE performs key agreement with a BEST UE using either i) AKMA ii) 5G AKA or EAP-AKA' , or iii) proprietary key agreement protocol	HSE performs key agreement with a BEST UE using either i) AKMA ii) 5G AKA or EAP-AKA' , or iii) proprietary key agreement protocol EVIDENCE Verify via logs at the HSE that a test BEST UE can perform key agreement and key refresh. Regardless of the key agreement scheme used, HSE logs confirm the following keys are derived after key agreement: KE2Menc, KE2Mint, KIntermediate, KEAS_PSK	d) Choose appropriate authentication mechanisms, depending on the type of access	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.163, cl. 4.6
SO11-081	TC360	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Remote management services such as SSH or RDP are disabled or not even installed within VMs or containers	Remote management services such as SSH or RDP are disabled or not even installed within VMs or containers. Exposed services (such as etcd for container) are either only available to fully trusted systems or require authentication. EVIDENCE Documentation stating which security protocols and exposed services are implemented provided by vendors. Documentation provided by vendors accompanying the VNF if the VNF supports the capability to restrict service reachability only to nodes authorized to access them. It details how this capability can be configured. It states which security protocols and exposed services are implemented. At least the following information is included: - protocol handlers and services needed for the operation of VNF; - their open ports and associated services; - the configuration options; - and a description of their purposes. Verify using a network port scanner (e.g., nmap) that the use SSH, RDP or other remote services within VMs or containers is not allowed by sending requests and checking that those requests are unsuccessful. Verify using a network port scanner that all exposed services by VMs or containers requires authentication and authorization.	d) Choose appropriate authentication mechanisms, depending on the type of access	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	OWASP Container Security Verification Standard, cl. V2 (2.15), V3 (3.12, 3.13)
SO11-082	TC124	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, AMF, gNB	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 10.2
SO11-083	TC130	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.10
SO11-084	TC039	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, NEF	SA	Private, (Hybrid), (Public)	Færdig	Internal 5G core information such as SUPI, DNN, S-NSSAI is not disclosed by NEF to application functions residing outside the MNO domain	Internal 5G core information such as SUPI, DNN, S-NSSAI is not disclosed by NEF to application functions residing outside the MNO domain EVIDENCE Packet captures of interaction between NEF and application functions outside MNO 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.2.3
SO11-085	TC090	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.6 3GPP TS 33.216 3GPP TS 33.511-519
SO11-087	N/A	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, ACCESS CONTROL TO NETWORK AND INFORMATION SYSTEMS, SMF	SA	Private, (Hybrid), (Public)	Færdig	SMF provides a user plane security policy to the ng-eNB/gNB during PDU session establishment	SMF provides a user plane security policy to the ng-eNB/gNB during PDU session establishment as specified in 3GPP TS 23.502 EVIDENCE Capture of the Nsmf_PDUSession_SMContext Response message sent from the SMF contains the UP security policy	b) Implement logical access control mechanism for network and information systems to allow only authorized use	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	TS 33.501, cl. 6.6 TS 23.502, cl. 4.3.2
SO12-001	TC056	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.4 3GPP TS 33.216 3GPP TS 33.511-519
SO12-002	TC070	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.1.2 3GPP TS 33.216 3GPP TS 33.511-519
SO12-003	TC071	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.1.3 3GPP TS 33.216 3GPP TS 33.511-519
SO12-004	TC080	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.4 3GPP TS 33.216 3GPP TS 33.511-519

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO12-005	TC081	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-006	TC082	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.2 3GPP TS 33.216 3GPP TS 33.511-519
SO12-007	TC083	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.3 3GPP TS 33.216 3GPP TS 33.511-519
SO12-008	TC084	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.6.2.4 3GPP TS 33.216 3GPP TS 33.511-519
SO12-009	TC092	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.1 3GPP TS 33.216 3GPP TS 33.511-519
SO12-010	TC096	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.5 3GPP TS 33.216 3GPP TS 33.511-519
SO12-011	TC113	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Network Function (NF), 5G Core (5GC), Service-Based Interfaces (SBI), UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.3.6.2 3GPP TS 33.512-519
SO12-012	TC116	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Network Function (NF), 5G Core (5GC), Service-Based Interfaces (SBI), UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-013	TC138	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Network Slice Subnet Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.3.1
SO12-014	TC145	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	NIST 800-92
SO12-015	TC169	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Applications, SDN Resources	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 8.1
SO12-016	TC187	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VPLMN	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ENISA - Signaling Security in Telecom SS7/Diameter/5G, cl. 3.3
SO12-017	TC188	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VPLMN	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ENISA - Signaling Security in Telecom SS7/Diameter/5G, cl. 3.3
SO12-018	TC340	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Separate physical infrastructure for critical network functions: Hosts are physically separated such that compromise of one physical host does not allow an attacker to impact a very large amount of virtualised network nodes, and a physical host's risk profile is used to determine which workloads can be deployed on it	Separate physical infrastructure for critical network functions: Hosts are physically separated such that compromise of one physical host does not allow an attacker to impact a very large amount of virtualised network nodes, and a physical host's risk profile is used to determine which workloads can be deployed on it. A physical host is not able to impact hosts in other host pools. For example, among other controls, spoofing VLAN/VXLANs of virtual networks is not allowed. Where the virtualisation platform is used to enforce separation between trust domains (i.e. where discrete physical hardware is not used), type-1 hypervisors are used. Virtual workloads do not have direct access to the physical hardware. Containers are not used to enforce separation between trust domains. Correspondingly, containerised hosts only support a single trust domain. EVIDENCE A document containing the definition of trust domains and the separation requirements to be implemented and enforced. Documented risk analysis determining which controls set out in the 'control description' field are appropriate.	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 6.2
SO12-019	TC363	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Only containers or VMs with the same data classification level run on the same node	Only containers or VMs with the same data classification level run on the same node. Only containers or VMs with the same level of exposure (e.g. Internet facing) run on the same node. EVIDENCE Data classification process is documented. Documented risk assessment includes the sensitivity level of VNFs. Documented definition of trust domains, and their separation requirements to be implemented and enforced.	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	CIS Benchmarks (Docker, VMWARE, Kubernetes) OWASP Container Security Verification Standard, cl. V4 (4.9)
SO12-023	TC001	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, All network functions	SA	Private, (Hybrid), (Public)	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) (unless other countermeasures are used, such as physical security for local services on a single site) 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. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verification of each network function for support of TLS (unless other countermeasures are used, such as physical security for local services on a single site) 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. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-024	TC024	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.3 3GPP TS 33.517, cl. 4.2.2.1
SO12-025	TC042	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, gNB	SA and NSA	Private, (Hybrid), (Public)	Færdig	Ensure control plane data confidentiality and integrity protection over N2/Xn interface	gNB implements IPsec ESP and IKEv2 certificate based authentication. When physical security is not provided, DTLS or a similar protection mechanism, such as IPSec, is implemented for integrity, confidentiality, and replay protection of E1, F1-U, F1-C, N2, N3, and Xn interfaces. Cryptographic keys/certificates for IKEv2 authentication are protected EVIDENCE Verification that a secure IPsec ESP connection can be established after IKEv2 certificate-based authentication. Verification that a secure record layer connection can be established. Verification with a key management utility that the keys/certificates for IKEv2 authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-026	TC052	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.4 3GPP TS 33.216 3GPP TS 33.511-519

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO12-027	TC074	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	Protect communication between web client and web server	Communication between web client and web server is protected using TLS (unless other countermeasures, such as physical security for local services on a single site, are used) as profiled in Annex E of TS 33.310 with the following additional requirement: cipher suites with NULL encryption shall not be supported. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Packet captures between the web client and the web server show the use of TLS (unless other countermeasures, such as physical security for local services on a single site, are used) and confirm that the protocol version/cryptographic algorithms mandated by the security profile are used. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-028	TC122	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, DNS server	SA	Private, (Hybrid), (Public)	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. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Packet captures at DNS servers in the core network confirm the use of TLS for protection of DNS requests and responses. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, Annex P IETF RFC 7858/RFC 8310
SO12-029	TC128	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SMF, UPF, gNB	SA	Private, Hybrid, (Public)	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 IPsec ESP and IKEv2 certificate-based authentication as specified in TS 33.510, cl. 9.1.2, unless security is provided by other means, such as physical security. Cryptographic keys/certificates for IKEv2 authentication in NDS/IP are protected EVIDENCE Verification of packet captures on the interface under test confirms the use of IPsec for integrity, confidentiality, and replay protection. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.210 3GPP TS 33.501, cl. 9.5/9.9
SO12-030	TC129	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VPLMN AMF, HPLMN AUSF, HPLMN UDM	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.14
SO12-031	TC131	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.8
SO12-032	TC132	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, AMF, gNB	SA	Private, Hybrid, (Public)	Færdig	Network ensures that security is maintained during UE mobility	Network ensures that security is maintained during UE mobility in accordance with 3GPP technical specification 33.501, clause 6.9 and 6.11 EVIDENCE Packet captures on the AMF as well as on the source and target gNBs confirm successful UE mobility and handover	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.9/6.11
SO12-033	TC133	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UDM	SA	Private, (Hybrid), (Public)	Færdig	Operators should ensure that UEs conceal the Subscription Permanent Identifier (SUPI)	MNOs should ensure that UEs conceal the Subscription Permanent Identifier (SUPI) by using the ECIES profile A or B defined in 3GPP technical specification 33.501, clause 6.12 and Annex C. A null-scheme may be used in the following cases: (1) if the UE is making an unauthenticated emergency session and does not have a 5G-GUTI to the chosen PLMN, (2) if the home network has configured "null-scheme" to be used, or (3) if the home network has not provisioned the public key needed to generate a SUCI 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.12/Annex C
SO12-034	TC146	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020
SO12-035	TC148	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFV MANO	SA	Private, Hybrid, (Public)	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. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verification of TLS support for API communication by looking at packet captures and setting up test TLS connections. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 022, cl. 4
SO12-036	TC152	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Control Plane	SA	Private, Hybrid, (Public)	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. Cryptographic keys/certificates for authentication are protected EVIDENCE Packet captures confirm the use of standard security protocols such as TLS for authentication and encryption of control plane data exchanged between hosts. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 5.15
SO12-037	TC162	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Controller	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-15
SO12-038	TC163	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Northbound Interface, Southbound Interface, Eastbound, Westbound Interface	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 8.1
SO12-039	TC166	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Controller	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-24
SO12-040	TC173	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, 3GPP SA6 interfaces, ETSI MEC interfaces	SA and NSA	(Private), Hybrid, (Public)	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. Cryptographic keys/certificates for authentication are protected EVIDENCE Verify that API communication is protected with TLS by looking at packet captures and setting up test TLS connections. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO12-041	TC176	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Virtual Infrastructure, Virtual Infrastructure Manager (VIM)	SA and NSA	(Private), Hybrid, (Public)	Færdig	Virtualization platform or container infrastructure is hardened using vendor-provided guidelines	Virtualization platform or container infrastructure 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
SO12-042	TC178	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Virtual Infrastructure, Virtual Infrastructure Manager (VIM)	SA and NSA	(Private), Hybrid, (Public)	Færdig	VMs or containers in MEC are encrypted	VMs or containers in MEC are encrypted EVIDENCE Inspection of servers and storage containing VMs or containers confirm that the VMs or containers are encrypted	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Cloud Security Alliance - Best practices for mitigating risks in virtualized environments
SO12-043	TC185	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MEC host	SA and NSA	(Private), Hybrid, (Public)	Færdig	MEC systems provide a secure environment for services of users, MNOs, third-party application providers, application developers, and platform vendors	MEC systems provide a secure environment for services of users, MNOs, 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS MEC 002, cl. 8.1
SO12-044	TC186	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, eNB, MME	NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.401, cl. 5.1.4 3GPP TS 36.323 3GPP TS 33.501, cl. 5.4
SO12-045	TC189	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, LTE Visiting PLMN	SA and NSA	Private, Hybrid, (Public)	Færdig	End-to-end signaling security is used for DIAMETER signaling when physical security is not provided	End-to-end signaling security is used for DIAMETER signaling when physical security is not provided EVIDENCE Packet captures confirm that Diameter End-to-End Signaling (DESS), or a similar protection mechanism, is used to provide end-to-end security, unless physical security is provided	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	GSMA FS.19
SO12-046	TC190	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, LTE Visiting PLMN	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	TS 33.328, cl. 4 TS 33.401, cl. 7.2.8.4.1/E.2.2 TS 33.501, cl. 5.4
SO12-047	TC196	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116, cl. 4.2.2.3.1 3GPP TS 33.401, cl. 7.2
SO12-048	TC206	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, eNB	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.401, cl. 5.3.5 3GPP TS 33.501, cl. 5.4
SO12-049	TC221	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Virtualization assets	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	NA

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO12-050	TC326	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEAL group management server, SEAL key management server	SA	Private, (Hybrid), (Public)	Færdig	SEAL-X1 interface between the SEAL key management server and the SEAL group management server is protected using HTTPS with TLS usage following the profile specified in the 3GPP technical specification	SEAL-X1 interface between the SEAL key management server and the SEAL group management server is protected using HTTPS with TLS usage following the profile specified in clause 6.2a of 3GPP TS 33.310. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verification that the SEAL key management server and the SEAL group management server support HTTPS with TLS as profiled in clause 6.2a of 3GPP TS 33.310. 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. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.1.1.1
SO12-051	TC327	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEAL location management server, SEAL key management server	SA	Private, (Hybrid), (Public)	Færdig	SEAL-X2 interface between the SEAL location management server and the SEAL group management server is protected using HTTPS with TLS usage following the profile specified in the 3GPP technical specification	SEAL-X2 interface between the SEAL location management server and the SEAL group management server is protected using HTTPS with TLS usage following the profile specified in clause 6.2a of 3GPP TS 33.310. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verification that the SEAL location management server and the SEAL group management server support HTTPS with TLS as profiled in clause 6.2a of 3GPP TS 33.310. 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. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.1.1.2
SO12-052	TC328	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEAL server, SEAL key management server, SEAL identity management server	SA	Private, (Hybrid), (Public)	Færdig	i) SEAL-UU interface between the SEAL server and the SEAL client, ii) KM-UU interface between SEAL key management server and SEAL key management client, and iii) IM-UU interface between SEAL identity management server and SEAL identity management client are protected	i) SEAL-UU interface between the SEAL server and the SEAL client, ii) KM-UU interface between SEAL key management server and SEAL key management client, and iii) IM-UU interface between SEAL identity management server and SEAL identity management client are protected either using i) HTTPS with TLS following the profile specified in clause 6.2a of 3GPP TS 33.310, or ii) CoAP with OSCORE as profiled in RFC 8613 or iii) CoAP with DTLS/TLS as profiled in clause 6.2a of 3GPP TS 33.310. Cryptographic keys/certificates for TLS/DTLS/OSCORE authentication are protected EVIDENCE Verification that the SEAL client, SEAL server, SEAL key management client, SEAL key management server, SEAL identity management client, and the SEAL identity management server either i) support HTTPS with TLS as profiled in clause 6.2a of 3GPP TS 33.310, or ii) CoAP with OSCORE as profiled in RFC 8613 or iii) CoAP with DTLS/TLS as profiled in clause 6.2a of 3GPP TS 33.310. Verification can involve looking at product documentation and establishing test DTLS, TLS, OSCORE connections to ensure that only protocol versions and cryptographic algorithms mandated by the respective profiles are supported. Verification with a key management utility that the keys/certificates for DTLS, TLS, and OSCORE authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.1.1.3, 5.1.1.4, 5.1.1.5
SO12-053	TC329	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VAL server, SEAL server	SA	Private, (Hybrid), (Public)	Færdig	SEAL server authenticates and authorizes requests from VAL server using either i) Certificate based TLS authentication followed OAuth-based authorization following profiles in the 3GPP technical specification	SEAL server authenticates and authorizes requests from VAL server using either i) Certificate based TLS authentication followed OAuth-based authorization following profiles in 3GPP technical specifications: 33.210, clause 6.2 and 33.310, clause 6.2a, or ii) CAPIF as specified in 3GPP technical specifications: 23.434 and TS 33.122, clause 6.5.2. Cryptographic keys/certificates for IKEv2, TLS, etc. authentication in NDS/IP are protected EVIDENCE Verification that the SEAL server and the VAL server use TLS with OAuth or CAPIF for authentication and authorization following profiles in TS 33.210, TS 33.310, and TS 33.122. Verification can involve looking at product documentation and establishing test TLS or CAPIF connections to ensure that only protocol versions and cryptographic algorithms mandated by the 3GPP profiles are supported by the network function. Verification with a key management utility that the keys/certificates for IKEv2, TLS, etc. authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 23.434 3GPP TS 33.122, cl. 6.5,2 3GPP TS 33.210, cl. 6.2 3GPP TS 33.310, cl. 6.2a 3GPP TS 33.434, cl. 5.1.1.8
SO12-054	TC330	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEAL server	SA	Private, (Hybrid), (Public)	Færdig	SEAL-E interface between SEAL servers is protected with NDS/IP	SEAL-E interface between SEAL servers is protected with NDS/IP as specified in TS 33.210. Cryptographic keys/certificates for IKEv2, TLS, etc. authentication in NDS/IP are protected EVIDENCE Verification of packet captures on the SEAL server confirms the use of TLS, IPsec, etc. for integrity, confidentiality, and replay protection. Verification with a key management utility that the keys/certificates for IKEv2, TLS, etc. authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.1.1.9
SO12-055	TC334	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SKM server	SA	Private, (Hybrid), (Public)	Færdig	Transfer of key material from SKM server to SKM client over HTTP are protected with TLS	Transfer of key material from SKM server to SKM client over HTTP are protected with TLS as profiled in clause 6.2a of 3GPP TS 33.310 EVIDENCE Verification that the SKM server supports HTTPS with TLS as profiled in clause 6.2a of 3GPP TS 33.310. 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. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 5.3
SO12-056	TC353	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Enforce isolation of containers	For container: controls to enforce isolation: - Namespaces controls what resources a container can see. The isolated resources include process pids, filesystem mounts, network stack, user UIDs, etc. - Cgroups ensures that one container cannot consume more resources (cpu, memory, storage, network) than its fair share. - Capabilities protects the container from any malicious exploits that target services running without root privileges. - Seccomp allows administrators to define system call security that must be blocked during container runtime. Seccomp policies are defined using JSON files. EVIDENCE Use of testing and analysis tools to verify: - That containers are executed as runtime processes within given namespaces. - That Cgroups is used to control the different resources. - That an application running within a container is executed only with the necessary capability. - That Seccomp policies are defined using JSON files. - That the container during its execution calls the Seccomp () system to execute a Berckeley Packet Filter (bpf) program. Such tools include: - To detect containers with known vulnerabilities: free tools (Clair, ThreatMapper, Trivy), commercial (Snyk, anchore, Aqua Security's MicroScanner, JFrog Xray, Qualys) - To detect secrets in images: ggshield, SecretScanner - To detect misconfigurations in Kubernetes: kubeaudit, kubesec.io, kube-bench - To detect misconfigurations in Docker: inspec.io, dev-sec.io, Docker Bench for Security	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 023 , cl.6.1 OWASP - Kubernetes Security Cheat Sheet, cl. 'Use Kubernetes namespaces to properly isolate your Kubernetes resources', 'Container Sandboxing' OWASP - Docker Security Cheat Sheet, cl. 'RULE #5', 'RULE #6'
SO12-061	TC380	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Applications, SDN Resources, SDN Infrastructure layer, SDN controller, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	A high availability architecture is implemented for key SDN components to ensure operational service is maintained	A high availability architecture is implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design should include primary and secondary IP links with, where possible, diverse routing to prevent a single point of network failure. EVIDENCE Documentation is available containing the default SDN controller configuration. Verify that SDN controllers are designed and configured to support primary and secondary IP links. Verify that this feature is available in a configuration file, and that it is activated by default. Each interface of the network product is bound to two IP addresses within the SDN controller. Block the primary IP at the SDN controller and send a packet from the network product 1 to the network product 2 with the primary IP. Then, verify that the packet is correctly routed and received by the network product 2 (logged by the network traffic analyser) with the secondary IP.	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	GSMA FS.33, Control 50
SO12-062	TC381	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Applications, SDN Resources, SDN Infrastructure layer, SDN controller, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable	The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration or MANO layer to maintain operating services under circumstances that may render the orchestration platform unavailable. EVIDENCE Security architecture documentation confirms that SDN and NFV are operationally independent. Verify via tests that MANO layer can continue providing services while SDN is unavailable and vice versa: - Turn off SDN services and verify that requests sent to the MANO layer are correctly processed and that any running MANO service does not crash. - Turn off MANO services and verify that requests sent to the SDN are correctly processed and that any running SDN service does not crash.	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	GSMA FS.33, Control 72
SO12-063	TC382	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	For the security protection at the transport layer on NFV interfaces, TLS shall be supported	For the security protection at the transport layer on NFV interfaces, TLS (TLSv1.3 is recommended) shall be supported. For the mutual authentication of the NFV components, NFV interfaces shall support mTLS via X.509v3 certificates. IETF RFC 5246 (TLS 1.2) and RFC 8446 (TLS 1.3) shall be used. Both the client (e.g., VIM as API consumer) and the server (e.g., NFVI as API producer) require a certificate, and both sides authenticate each other using their public/private key pair. NFV interfaces shall support authorization using OAuth 2.0. For interfaces/APIs, not supporting TLS protocol, should support IPsec with IKEv2 certificated-based authentication. EVIDENCE Network product documentation containing information about supported TLS, IPsec with IKEv2, OAuth protocols and certificates is provided by the vendor. Verification by looking at product documentation to ensure that only protocol versions and cryptographic algorithms mandated by the profile are supported by the network function. TLS: - Check that compliance with the TLS profile (in 3GPP technical specifications: 33.210, clause 6.2 and 33.310, clause 6.2a) can be inferred from detailed provisions in the network product documentation. - Establish a secure connection between a network product and a peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test. - Try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile. IPsec: - Verify that a secure IPsec ESP connection can be established after an IKEv2 certificate-based authentication. The tester triggers communication between a network product and a test entity that has a legitimate IKEv2 certificate-based authentication credential. IPsec ESP connection between the network product and the entity with correct credentials can be established. Verify that TLS or IPsec protocols are used for communicating NFV interfaces. This can be confirmed by checking packet captures or by setting up test connections. OAuth 2.0: - Verification failure of mandatory claims in the access token: the network product under the test rejects the NF service consumer's service request based on Oauth 2.0 error response defined in RFC 6749. - Verification failure of optional claims in the access token: if the network product under the test understands these optional claims (list of S-NSSAIs, list of NSIs, NF Set ID, additional scope), it rejects the NF service consumer's service request based on Oauth 2.0 error response defined in RFC 6749. Verification with a key management utility that the keys/certificates for TLS or IPsec with IKEv2 authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs.	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	IETF RFC 5246 and IETF RFC 8446 3GPP TS 33.210, cl. 6.2 and 3GPP TS 33.310, cl. 6.2a ETSI GS NFV-SEC 022, cl. Annex B
SO12-064	TC388	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	(Private), Hybrid, (Public)	Færdig	For the security of MEC interfaces, IPsec for the N4 interface to protect the confidentiality and integrity of signaling data is implemented	For the security of MEC interfaces, IPsec for the N4 interface to protect the confidentiality and integrity of signaling data is implemented. The management interface provides a TLS channel for secure transmission, enabling data security on the management plane. The security deployment solution is provided to comprehensively protect MEC interfaces. For example, an IPsec gateway can be deployed on the N4/N3/N6/N9 interface for encrypted transmission of user data, and a firewall can be deployed on the MEC to defend against DDoS and other traffic attacks. EVIDENCE Verification of successful IPsec tunnel over N4/N3/N6/N9 interfaces. Verification of packet captures on the interfaces under the test confirms the use of IPsec. Verification of successful TLS channel on the management plane. Verification of packet captures on the interface under the test confirms the use of TLS. Verification with a key management utility that the keys/certificates for TLS or IPsec authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as HSMs. Diagnostic tools confirm that firewalls and gateways, if any, are activated.	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI White Paper No. 46, cl. 2.2, 3.2
SO12-065	TC057	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.5 3GPP TS 33.216 3GPP TS 33.511-519
SO12-066	TC153	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Regular and effective patch management	Regular and effective patch management. Ideally, applying patches is fully automated. EVIDENCE Check for presence of patch management tools notifying of patch releases. All patches, especially those to critical or sensitive network components or functions, are reviewed and subjected to security testing in controlled environment prior to deployment	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 001, cl. 7.2.2 ISO/IEC 27002:2022, cl. 8.8 NIST.SP.800-53-Rev.5, MA-3

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO12-067	TC160	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VNF, SDN Controller	SA	Private, Hybrid, (Public)	Færdig	Regular and effective vulnerability management program	Regular and effective vulnerability management program that includes vulnerability assessments on initial deployment and subsequent periodic scans for deployed network components. Security scans should cover the whole NFV, and not just the network functions layer. EVIDENCE Verify that documented processes and tools are in place to track public and vendor/supplier databases of disclosed vulnerabilities. Verify via system logs and scan/test reports that vulnerability scanning tools are activated and periodic scans are performed for newly deployed network components, in particular for products supplied by suppliers considered to be high-risk. 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. Verify that all NFV and SDN nodes undergo regular automated security scans, which cover among others the whole operating system, virtualization layer, MANO and VNFs. Such verification activities include checking the output of scan results generated by vulnerability scanners and a list of discovered vulnerabilities/identified discrepancies.	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 001, cl. 7.2.2 ITU-T X.1038, cl. 7.2.2 R-25 3GPP TS 33.117, cl. 4.4.3
SO12-070	TC379	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	MANO is kept in sync about a VNF application software modification	MANO is kept in sync about a VNF application software modification. Such a modification may be performed without requiring termination of the VNF instance with the prior VNF application software version. EVIDENCE Verify that the information about a VNF instance stored in MANO is updated as a result of a VNF application software modification	d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-IFA 011, cl. 5.7
SO12-074	TC003	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, All network functions	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.2.2.2.3/4.2.2.2.4 3GPP TS 33.501, cl. 13.4.1
SO12-075	TC011	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, AUSF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 14.1
SO12-076	TC012	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, AUSF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.15/14.1
SO12-077	TC030	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.2.4.3.1 3GPP TS 33.517, cl. 4.2.2.5
SO12-078	TC034	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 13.2.3.4 3GPP TS 33.517, cl. 4.2.2.8
SO12-079	TC055	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.2 3GPP TS 33.216 3GPP TS 33.511-519
SO12-080	TC058	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.5 3GPP TS 33.216 3GPP TS 33.511-519
SO12-081	TC151	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, VIM	SA	Private, Hybrid, (Public)	Færdig	Integrity protection of data store used for VNF and CNF images	Integrity protection of data store used for VNF and CNF images. EVIDENCE Manual inspection of VNF and CNF images confirms that their integrity is protected with cryptographic tools such as a digital signature or a hash. Verify that VMs and Containers cannot be created with tampered images.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 014, cl. 5.2-c.1.1.4
SO12-082	TC159	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI	SA	Private, Hybrid, (Public)	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) (e.g. TPM, HSM) which serves as the initial root of trust for sensitive virtualized components. HBRT ensures boot integrity by computing a measurement of system sensitive components such as platform firmware, BIOS, bootloader, OS kernel, and other system components that can be securely stored in and verified by HBRT during boot. To provide a trusted hardware platform, the hardware (blade servers) should support Intel TXT, SGX, AMD SEV or ARM Trustzone silicon-based security functionality implemented with a TPM that stores measurements of the entire hypervisor or CIS stack and boot process. EVIDENCE Verify that documentation of the host system describes support for HBRT. Verify via a guest OS that HBRT can be used for attestation. Verify whether blade servers support a trusted HW platform (e.g. Intel TXT, SGX, AMD SEV or ARM Trustzone). For example, using any suitable command line tools. Tamper a BIOS or a file in the host OS kernel and restart the host. Then, check that the boot operation is verified by a trusted HW platform and fails when using a tampered BIOS or a file in the host OS kernel.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 012, cl. 5.1 3GPP TR 33.818, cl. 5.2.5.7.7.4
SO12-083	TC161	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVO, VIM	SA	Private, Hybrid, (Public)	Færdig	VNF package integrity is validated by NFVO upon its reception using the signature generated and provided by the VNF Provider	VNF package integrity is validated by NFVO upon its reception using the signature generated and provided by the VNF Provider. VNF package artifacts/configuration files that are separate from the VNF/CNF package itself containing sensitive information (e.g., LI VNFs, keys, PII, passwords or other critical configuration data) are protected from unauthorized disclosure. VNF package is to be successfully authenticated and verified during instantiation to the NFVI from the trust packages repository. EVIDENCE Verify that integrity of VNF packages is ensured with cryptographic tools such as a digital signature or a hash during onboarding. Verify that confidentiality of sensitive VNF package artifacts/configuration files is ensured with cryptographic tools such as an encryption during onboarding. Verify that VNF manager does not accept VNF packages if the integrity checks fail during insantitation. Verify that sensitive VNF package artifacts/configuration files can be decrypted before instantiation with the provided keys. Verification (tests) steps: 1. Review the documentation provided by the vendor describing how VNF package integrity is verified; 2. During VNF package onboarding, the tester uploads a valid VNF package into a NFVO. The NFVO verifies the integrity of the VNF package by validating the digital signature of the VNF package using the certificate of VNF vendor according to the documentation. During VNF instantiation, the VIM selects a VNF image with a correct integrity protection value from the image repository to instantiate the VNF image; 3. During VNF package onboarding, the tester uploads an invalid VNF package into an NFVO. The NFVO validates the digital signature of the VNF package using the certificate of VNF vendor. During VNF instantiation, the VIM selects a VNF image with an incorrect integrity protection value from the image repository to instantiate the VNF image.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 021, cl. 5.1/5.2/6.3/6.4/6.5 3GPP TR 33.818, cl. 5.2.5.5.3.3.5.1
SO12-084	TC164	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, SDN Controller	SA	Private, Hybrid, (Public)	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	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-18, R-22
SO12-085	TC197	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116, cl. 4.2.2.3.2 3GPP TS 33.401, cl. 7.2.4.3.1
SO12-086	TC198	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116, cl. 4.2.2.6.1 3GPP TS 33.401, cl. 15.1
SO12-087	TC316	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NWDAF, UDM, AMF, SMF, PCF, NEF, BSF	SA	Private, (Hybrid), (Public)	Færdig	NWDAF always determines a recent NF instance serving a UE before retrieving data related to it, unless, the NWDAF has already obtained this information due to recent operations related to this UE	NWDAF always determines a recent NF instance serving a UE before retrieving data related to it, unless, the NWDAF has already obtained this information due to recent operations related to this UE EVIDENCE Upon subscribing to analytics results for a test UE, the data retrieved from the NWDAF is from an NF which served the UE most recently. Verification includes inspecting timestams in the logs at various NFs that have served the test UE recently	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.521, cl. 4.2.2
SO12-088	TC342	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The HMEE (e.g. Intel TXT, Trusted Execution Environments (TEE) like GlobalPlatform TEE, Intel SGX) is to be used for executing sensitive functions within the VNF	The HMEE (e.g. Intel TXT, Trusted Execution Environments (TEE) like GlobalPlatform TEE, Intel SGX) is to be used for executing sensitive functions within the VNF, such as LI and information elements marked as private (e.g., the SIDF de-concealing the SUPI from the SUCI). Utilizing an HMEE within the NFVI may solve the issue of Virtual Network Function (VNF) isolation, memory introspection, and confidentiality of data-in-use in both virtualized and containerized environments. EVIDENCE Document describing the deployed hardware resources that have an HMEE enabled, and how they can be used.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 6.5 ETSI GS NFV-SEC 009 , cl. 6.16 ETSI GS NFV-SEC 025 , cl. 5.1.1

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO12-089	TC350	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	A chain of trust (CoT) is established during the boot process of the NFVI	A chain of trust (CoT) is established during the boot process of the NFVI. The chain is extended to include attestation of the VNF when it is first instantiated on top of the NFVI. After each step, the results of attestation and corresponding measurements are maintained by a verifier for subsequent access: 1. Attestation of the Server / Hardware Resource, which will act as the attester for the OS 2. Attestation of the OS 3. Attestation of the Virtualisation Layer software 4. The virtualisation layer software (e.g., hypervisor or container engine) measures the virtual instance and VNF software, and reports the results to the verifier 5. The verifier validates the measurements against the attestation results from steps 1-4 6. The NFVI begins to run the VNF If any step in the attestation process fails, the CoT cannot be expanded further and a recovery procedure should be activated to handle the failure. EVIDENCE Document describing the attestation process to enable the software integrity state to be reported and verified in order to determine its trustworthiness. Verification of attestation evidence from NFVI is performed by a verifier external to NFVI to support remote attestation. Documented process on how to verify the attestation evidence by an external verifier. Further, the process includes the recovery process to handle attestation process failures.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 6.6, 6.7
SO12-090	TC390	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, INTEGRITY OF NETWORK AND INFORMATION SYSTEMS, Virtualization infrastructure, MEC host, MEC platform, MEC application, MEC orchestrator	SA	(Private), Hybrid, (Public)	Færdig	Critical MEC components need to be implemented in HMEEs	Critical MEC components (e.g. security end points and crypto functions) need to be implemented in HMEEs (Hardware Mediated Execution Environments) e.g. Intel SGX or ARM TrustZone. EVIDENCE Check a document describing secure services provided by trusted HW platforms, and how to use them to verify whether blade servers support a trusted HW platform (e.g. Intel TXT, SGX, AMD SEV or ARM Trustzone) for secure storage, root of trust and secure boot. Identification of tamper resistant modules installed in the system using any suitable command line tools, or any other suitable means of determination. Verify that the execution of cryptographic operations is configured to be based on a tamper resistant module, and that those operations use crypto materials provided by the tamper resistant module (e.g., random number, session keys, etc.). This verification can be carried out by the following test, among others: Establish a TLS/DTLS (profile defined in TS 33.310 and TS 33.210) or IPsec/IKE (profile defined in TS 33.210) secure connection and verify that all protocol versions and combinations of cryptographic algorithms that are mandated by the security profile are provided by the tamper resistant module.	e) Set up state of the art controls to protect integrity of systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI White Paper No. 46, cl. 2.2
SO13-001	TC191	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116, cl. 4.2.2.3.4 3GPP TS 33.401, cl. 5.1.3.1
SO13-002	TC194	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, MME	NSA	Private, (Hybrid), (Public)	Færdig	All NAS signaling messages 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.401, cl. 5.1.4.1/8.1
SO13-003	TC195	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, MME	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116, cl. 4.2.2.3.3 3GPP TS 33.401, cl. 5.1.4.1
SO13-004	TC201	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, eNB	NSA	Private, (Hybrid), (Public)	Færdig	eNB ensures confidentiality and integrity protection of control plane data	eNB ensures confidentiality and integrity protection of control plane data on X2-C and S1-MME interfaces 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-005	TC202	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, eNB	NSA	Private, (Hybrid), (Public)	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 the transport of user data over S1-U and X2-U interfaces is integrity, confidentially and replay-protected	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-006	TC203	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, eNB	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-007	TC204	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, eNB	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-008	TC205	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, eNB	NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-009	TC315	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NWDAF	SA	Private, (Hybrid), (Public)	Færdig	NWDAF applies data masking on integration analysis of personal data	NWDAF applies data masking on integration analysis of personal data EVIDENCE Verify that retrieving analytics results from the NWDAF after creating an account does not contain any personal data of UE's users such as the subscriber permanent identifier (SUPI)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.521, cl. 4.2.1.2.6
SO13-010	TC351	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The hypervisor and/or CIS supports the encryption granularity down to per VM or per Container	The hypervisor and/or CIS supports the encryption granularity down to per VM or per Container. After the hypervisor/CIS has used the key to decrypt the workload, it shall delete any local copy of the key. EVIDENCE A document describing the encryption/decryption mechanisms of VM or container workload and the secure destruction of cryptographic materials. Verify using testing tools that the workload is encrypted according to the documentation. Verify that the decryption process has been performed according to the documentation. Verify that the destruction process of the used cryptographic key(s) for encryption or decryption is applied. Verify that the used key is unavailable (e.g. zeroed).	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 025 , cl. 6.2.3
SO13-011	TC355	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	VM or container swap encryption	VM or container swap encryption (e.g. dm-crypt linux based tool) EVIDENCE A document containing the tools used for encrypting swapped VM or container and their configuration. Verification through a test machine (e.g. network traffic analyser) that a swapped VM or container to a hard disk is 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	IEEE Communications Magazine – NFV: Security Threats and Best Practices, cl. 'Encrypting VNF Volume/swap areas'

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO13-012	TC017	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.8.2 3GPP TS 33.514, cl. 4.2.1.1
SO13-013	TC002	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, All network functions	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.310, cl. 6.1 3GPP TS 33.501, cl. 5.9
SO13-014	TC005	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-015	TC008	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-016	TC026	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.3.2/13.2/Annex G
SO13-017	TC032	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-018	TC033	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, SEPP	SA	Private, (Hybrid), (Public)	Færdig	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-019	TC041	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.3.2/5.11 3GPP TS 33.511, cl. 4.2.2.1.6
SO13-020	TC043	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO13-021	TC048	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.9.4 3GPP TS 33.511, cl. 4.2.2.1.13
SO13-022	TC049	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501 6.10.2.1 3GPP TS 33.511 4.2.2.1.18
SO13-023	TC121	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, IAB donor	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, Annex M
SO13-024	TC136	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, Service Based Interfaces, Os-Ma-Nfvo	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.1.1
SO13-025	TC137	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.2.1
SO13-026	TC139	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.3.1
SO13-027	TC140	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, Network Slice Instance	SA	Private, Hybrid, (Public)	Færdig	Negotiation of slice characteristics such as bandwidth, latency, and reliability between a communication service customer and an MNO 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 MNO should have replay, integrity, and confidentiality protection with TLS. Version 1.2 or 1.3 of TLS are recommended. Cryptographic keys/certificates for TLS authentication are protected EVIDENCE Verify by successfully setting up test connections with slice management interface and negotiating different slice characteristics via TLS. Verification with a key management utility that the keys/certificates for TLS authentication are protected in the system keystore or similar tool (Java KeyStore, AWS KMS, etc.), in secure memory, or protected with hardware security tools such as TPMs/TEEs	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.811, cl. 4.4.1
SO13-028	TC170	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, SDN Infrastructure layer	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ENISA Threat Landscape and Good Practice Guide for Software Defined Networks/5G, cl. 5.3
SO13-029	TC335	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, VAL server	SA	Private, (Hybrid), (Public)	Færdig	Configuration and user profile data sent from the VAL server in the network to a VAL UE is integrity, confidentiality, and replay protected	Configuration and user profile data sent from the VAL server in the network to a VAL UE is integrity, confidentiality, and replay protected EVIDENCE Packet captures at the VAL server confirm that protocol such as TLS which provide encryption, integrity protection, and replay protection are used from sending configuration and user profile data	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 4.1
SO13-030	TC337	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, HSE	SA	Private, (Hybrid), (Public)	Færdig	Control and user plane EMSDP messages between the HSE and BEST UE are integrity protected protected with algorithms such as 128-NIA1, 128-NIA2 or 128-NIA3	Control and user plane EMSDP messages between the HSE and BEST UE are integrity protected protected with algorithms such as 128-NIA1, 128-NIA2 or 128-NIA3 EVIDENCE Packet captures at the HSE show that control and user plane packets between HSE and BEST UE are integrity protected	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.163, cl. 6.2 3GPP TS 33.401, cl. Annex B.2
SO13-031	TC338	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, HSE	SA	Private, (Hybrid), (Public)	Færdig	Control and user plane EMSDP messages between the HSE and BEST UE are confidentiality protected protected with algorithms such as 128-NEA1, 128-NEA2 or 128-NEA3	Control and user plane EMSDP messages between the HSE and BEST UE are confidentiality protected protected with algorithms such as 128-NEA1, 128-NEA2 or 128-NEA3 EVIDENCE Packet captures at the HSE show that control and user plane packets between HSE and BEST UE are ciphered	c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.163, cl. 6.2 3GPP TS 33.401, cl. Annex B.1
SO13-032	TC006	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.5.2 3GPP TS 33.512, cl. 4.2.2.3.2
SO13-033	TC007	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, AMF	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.4/6.7.1 3GPP TS 33.512, cl. 4.2.2.4.2
SO13-034	TC044	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO13-035	TC045	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.3.3 3GPP TS 33.511, cl. 4.2.2.1.7
SO13-036	TC046	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.3.2 3GPP TS 33.511, cl. 4.2.2.1.2/4.2.2.1.8
SO13-037	TC047	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, USE OF ENCRYPTION, gNB	SA and NSA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO14-001	TC015	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.8.2
SO14-002	TC016	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.8.2
SO14-003	TC018	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UDM	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.1.4.1a 3GPP TS 33.514, cl. 4.2.2.2
SO14-004	TC114	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UDM, AUSF	SA	Private, (Hybrid), (Public)	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. A null-scheme may be used in the following cases: (1) if the UE is making an unauthenticated emergency session and does not have a 5G-GUTI to the chosen PLMN, (2) if the home network has configured "null-scheme" to be used, or (3) if the home network has not provisioned the public key needed to generate a SUCI 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 or one of the special conditions for using a null-scheme is met	a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.12
SO14-005	TC120	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, AUSF, SEAF, AMF, gNB, N3IWF	SA	Private, Hybrid, (Public)	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 and Annex A 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 6.2/Annex A
SO14-006	TC143	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NSSAI	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.813, cl. 6.5
SO14-008	TC025	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, SEPP	SA	Private, (Hybrid), (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.9.3.2 3GPP TS 33.517, cl. 4.2.2.2
SO14-009	TC319	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, AAnF	SA	Private, (Hybrid), (Public)	Færdig	AKMA Application Key (KAF) has a maximum lifetime	AKMA Application Key (KAF) has a maximum lifetime EVIDENCE Verify that the Naanf_AKMA_ApplicationKey_Get response message from the AAnF to the AF contains the KAF lifetime. Verify via AF logs that a KAF cannot be used for AKMA authentication after its lifetime has expired	c) Implement policy for management of cryptographic keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.535, cl. 4.4.2
SO14-010	TC158	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NSM, SDN Controller	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 012, cl. 5.1.2 Rec. ITU-T X.1038, cl. 7.2.2 R-19
SO14-011	TC352	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The hypervisor and/or CIS supports an external key management	The hypervisor and/or CIS supports an external key management. Interface with the key management system is done through a standardized protocol. At least Key Management Interoperability Protocol (KMIP) as defined by OASIS KMIP SPEC should be supported. The key management system uses a tamper resistant module, such as HSM. The tamper-resistant module storing the key(s) shall be certified e.g. Common Criteria, FIPS 140-2 Level 3. EVIDENCE A document describing the supported KMIP and how to use it securely. Verify that the implemented protocol is robust against unexpected input. Verify that the execution of this protocol is based on tamper resistant modules such as HSMs. Verify that the protocol is using crypto materials provided by the tamper resistant module (e.g. random number, session keys, etc.)	c) Implement policy for management of cryptographic keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 025 , cl. 6.2.3
SO14-012	TC364	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	NFV components to employ certificates	In NFV, the components to employ certificates include: •NFV should employ certificates which can be used for images signing and verification during onboarding and registration. •MANO and VNFs should employ certificates which can be used in order to establish secure connections between them. •NFVO employs certificates in order to establish secure management connections with VIM and VNFM. •NFVI employs certificate(s) in order to establish secure connections with MANO interfaces. The certificate policy should be consistent with the Internet X.509 Certificate Policy and Certification Practices Framework as defined in IETF RFC 3647. Certificates are continuously monitored, with the ability to generate audits and keep on top of expirations and renewals to avoid any disruption in NFV services. EVIDENCE MNO has a documented certification management process for distributing Public Key Certificates (PKC) to authenticate, authorize, and encrypt links between NFV components. Verify that a Certificate Policy is developed and documented by MNOs in accordance with their regional and national requirements. Verify that a documented renewal procedure (preferably automatic) of certificates prior to their expiration is in place.	c) Implement policy for management of cryptographic keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GR NFV-SEC 005
SO14-013	TC383	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Certificate management	Any vendor default (e.g. self-signed) certificates should be removed and replaced with MNO generated certificates for NFV. Each MNO should develop a certificate policy in accordance with their regional and national requirements as described in ETSI GR NFV-SEC 005. Certificate Management Protocol version 2 (CMPv2) as specified in IETF RFC 4210 and 4211 could be used by NFV to obtain MNO-signed certificates. The handling of certificates, including certificate profiles, may follow the rules defined in 3GPP TS 33.310. EVIDENCE Documented certificate management policy shows how vendor default certificates are removed and replaced by those of MNO. Certificate management policy contains rules on management of the life cycle of a certificate. Documentation containing CMP profiles that specifies clearly which options and features of CMP are used and how. Tests via auditing tools show that the network product does not support vendor default certificates during deployment. Establish a CMPv2 connection between network products and certificate authority (CA) / registration authority (RA) by sending to the tester machine requests for generating, renewing, revoking and removing certificates as specified in 3GPP TS 33.310, IETF RFC 4210 and 4211. Verify that CMP protocol versions and combinations of algorithms that are mandated by the CMP profile are supported. Verification with a key management utility that the keys/certificates are protected with hardware security devices, such as hardware security modules (HSMs).	c) Implement policy for management of cryptographic keys	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	IETF RFC 4210 and 4211 3GPP TS 33.310 ETSI GR NFV-SEC 005, cl. 6,7,8,9,10
SO14-014	TC061	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO14-015	TC062	TELE, 5G, SECURITY OF SYSTEMS AND FACILITIES, PROTECTION OF SECURITY CRITICAL DATA, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, VSF, ISF, PSF, LCM proxy, MEC orchestrator, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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 * Before deploying any new network functions, all default passwords must be changed to have values consistent with administrative level accounts. 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.4.3 3GPP TS 33.216 3GPP TS 33.511-519

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO15-005	TC085	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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)	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.1 3GPP TS 33.216 3GPP TS 33.511-519
SO15-006	TC093	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.2 3GPP TS 33.216 3GPP TS 33.511-519
SO15-007	TC094	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.3 3GPP TS 33.216 3GPP TS 33.511-519
SO15-008	TC098	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.10 3GPP TS 33.216 3GPP TS 33.511-519
SO15-009	TC099	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.11 3GPP TS 33.216 3GPP TS 33.511-519
SO15-010	TC100	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.12 3GPP TS 33.216 3GPP TS 33.511-519
SO15-011	TC101	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.13 3GPP TS 33.216 3GPP TS 33.511-519
SO15-012	TC102	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.14 3GPP TS 33.216 3GPP TS 33.511-519
SO15-013	TC103	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.15 3GPP TS 33.216 3GPP TS 33.511-519
SO15-014	TC104	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.2 3GPP TS 33.216 3GPP TS 33.511-519
SO15-015	TC105	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.3 3GPP TS 33.216 3GPP TS 33.511-519
SO15-016	TC106	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.4 3GPP TS 33.216 3GPP TS 33.511-519
SO15-017	TC107	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.5 3GPP TS 33.216 3GPP TS 33.511-519
SO15-018	TC108	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.4.6 3GPP TS 33.216 3GPP TS 33.511-519
SO15-019	TC109	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.3.4.7 3GPP TS 33.511-519
SO15-020	TC110	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.3.4.8 3GPP TS 33.511-519
SO15-021	TC111	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.3.4.9 3GPP TS 33.511-519
SO15-022	TC112	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, O&M, control plane, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.117, cl. 4.3.5.1 3GPP TS 33.511-519 IETF RFC 3871, cl. 2.3.5 3GPP TR 33.818, cl. 5.2.5.5.8.5.1
SO15-023	TC156	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, VNF	SA	Private, Hybrid, (Public)	Færdig	VNFs should synchronize with trusted time sources	VNFs should synchronize with trusted time sources. The hardware layer shall maintain a suitably accurate clock within the NIC for timestamping to be read as a time source by VNFs, either directly or through a function abstracted in the hypervisor. Where supported, at least two different time sources are used from which all servers and network functions retrieve time information on a regular basis, so that the timestamps in logs are consistent. Network Providers shall install NICs that support time distribution using an appropriate technology such as PTP. If PTP is used, then the NICs shall utilize technology based on IEEE 1588TM Precision Time Protocol (PTP) or the derivative IEEE 802.1ASTM (gPTP). 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. Verify that at least two synchronized time sources across the hardware layer of NFV are configured, where supported. Verification could be carried out by: - Using the network traffic analyser, the tester verifies that the timestamp is received by the VNF from the configured synchronized time sources. - Reading and analysing the logged recorded timestamps by the VNF.	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 5.20 ETSI GS NFV-EVE 007, cl. 5.10

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO15-031	TC361	TELE, 5G, OPERATIONS MANAGEMENT, OPERATIONAL PROCEDURES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The number of allowed processes and resources within a VM or container is precisely defined and limited to the value stipulated in the VNF descriptor	The number of allowed processes and resources within a VM or container is precisely defined and limited to the value stipulated in the VNF descriptor. VNF vendors should define the CPU and Memory requirements of their VNFs, ie, the CPU and memory requirements to perform its functions under normal operating scenarios and the threshold limit value of CPU & memory requirements beyond which the NF should not be allowed to use. The virtualization layer should consider the CPU & Memory resource requirements & limits associated to each VNF provided by VNF vendors during onboarding and running of the VNF. EVIDENCE Verify that virtualization layer alerts the MANO in case the number of allowed processes and resources within a VM or container is exceeded. Regular verification whether VNF requirements are met by NFVI and MANO as required in the VNF descriptor. Verify that VNF vendors define the CPU and Memory requirements of their VNFs. Verify that those requirements are included within the VNF package.	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	OWASP Container Security Verification Standard, cl. V2 (2.4, 2.5), V3 (3.14), V9 (9.2), V12 (12.1, 12.2)
SO17-001	TC087	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.3 3GPP TS 33.216 3GPP TS 33.511-519
SO17-002	TC088	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.4 3GPP TS 33.216 3GPP TS 33.511-519
SO17-003	TC089	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.2.5 3GPP TS 33.216 3GPP TS 33.511-519
SO17-004	TC154	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	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. Security configuration documentation indicates reviews and updates taking place annually, or when significant changes occur.	b) Implement policy/procedures for asset management and configuration control	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 001, cl. 7.1 CIS Benchmarks (Docker, VMWARE, Kubernetes)
SO17-005	TC155	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, NFV MANO	SA	Private, Hybrid, (Public)	Færdig	Instantiation of MANO components and managed entities is only possible in explicit geographic locations	Instantiation of MANO components and managed entities is only possible in 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 014, cl. 6
SO17-013	TC357	TELE, 5G, OPERATIONS MANAGEMENT, ASSET MANAGEMENT, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	Only currently supported software (applications, host OSs; hypervisors or CISs) is designated as authorized in the software inventory for NFV	Only currently supported software (applications, host OSs; hypervisors or CISs) is designated as authorized in the software inventory for NFV. Any unsupported software is designated as unauthorized. Only software currently supported by the software's vendor is added to the NFV's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. EVIDENCE Review of the software list to verify that the software in question is supported. If the software is unsupported, yet necessary for the operation of NFV, verify that the exception is documented, including a description of mitigating controls and residual risk acceptance.	b) Implement policy/procedures for asset management and configuration control	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	CIS Benchmarks (Docker, VMWARE, Kubernetes) OWASP Container Security Verification Standard, cl. V2 (2.3)
SO21-001	TC054	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, SDN Controller, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	Security measures such as firewalls and backup network/computational capacity to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic	Security measures such as firewalls and backup network/computational capacity to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic. System shall act in a controlled and predictable way if an overload situation cannot be prevented. If security measures are no longer sufficient, the system should not reach an undefined and potentially insecure state EVIDENCE Network products have detailed technical description of the overload control mechanisms. Test results verifying the operation of the overload control mechanisms.	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.3.1/4.2.3.3.3 3GPP TS 33.216 3GPP TS 33.511-519 ITU-T X.1038, cl. 7.2.2 R-16
SO21-002	TC069	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	System is protected from growing or dynamic content	System is protected from growing or dynamic content (e.g. log files, uploads) with countermeasures such as use of a dedicated filesystem separated from main system functions, quotas, or system monitoring tools to ensure that the scenario of a file system reaching its maximum capacity is avoided EVIDENCE Network product documentation contains a list of resources that are susceptible to being exhausted with countermeasures in place. Verify that initiating traffic that causes increase in log files or file uploading to exhaust the file system does not negatively affect the system operation because of countermeasures in place	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.4.1.1.1 3GPP TS 33.216 3GPP TS 33.511-519
SO21-003	TC095	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	Færdig	Network product should support a mechanism to prevent Syn Flood attacks and should enable this feature by default	Network product should support a mechanism to prevent Syn Flood attacks and should enable this feature by default. Such mechanisms can include using the TCP Syn Cookie technique in the TCP stack EVIDENCE Verification method: Use a tool to send a large amount of TCP Syn packets to a network product listening on a TCP port to verify that this does not affect its services or availability. Verify that the memory of the network product is not exhausted and there is no crash, despite the large number of the TCP Syn packets	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.4 3GPP TS 33.216 3GPP TS 33.511-519 IETF RFC 4987
SO21-004	TC123	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, AMF, MME	SA	Private, Hybrid, (Public)	Færdig	Mobility and handover between 5GS to EPS and vice-versa are handled properly	Mobility and handover between 5GS to EPS and vice-versa are handled in accordance with 3GPP technical specification 33.501, clauses 8.2, 8.3, 8.4, 8.5, and 8.6 EVIDENCE Verify that a test UE device can continue receiving service during mobility between 5GS to EPS and vice-versa. Packet captures on the N26 interface confirm successful handover for the test UE	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 8.2/8.3/8.4/8.5/8.6
SO21-005	TC134	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, gNB, AMF, MME	SA	Private, Hybrid, (Public)	Færdig	Security of 5G Single Radio Voice Call Continuity (SRVCC) should be ensured during handover from 5G to UTRAN	Security of 5G Single Radio Voice Call Continuity (SRVCC) should be ensured during handover from 5G to UTRAN in accordance with Annex J of 3GPP technical specification 33.501. EVIDENCE Packet captures on the AMF and MME_SRVCC confirm that SRVCC handover for a test UE is completed successfully	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, Annex J
SO21-006	TC168	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, SDN Controller	SA	Private, Hybrid, (Public)	Færdig	SDN control layer should support hardware management to discover hardware failure automatically and recover	SDN control layer should support hardware management to discover hardware failure automatically and recover EVIDENCE Check configuration files and diagnostic tools to verify that techniques such as watch ports, liveness checks, and fast-failover are supported by the SDN controller and are used in deployments	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-26
SO21-008	TC180	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, Customer facing service (CFS) portal	SA and NSA	(Private), Hybrid, (Public)	Færdig	Denial of service (DoS) protection mitigation is used in distributed edge deployments	Denial of service (DoS) protection mitigation is used in distributed edge deployments EVIDENCE Verification that tools such as 'ufw' are available for filtering packets headed for a target site. Confirmation that tools for blocking open ports and suspending facilities under attack are available and functional	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ISO/IEC 27011, cl. TEL 13.1.6 ITU-T X.1205
SO21-013	TC336	TELE, 5G, BUSINESS CONTINUITY MANAGEMENT, SERVICE CONTINUITY STRATEGY AND CONTINGENCY PLANS, VAL server	SA	Private, (Hybrid), (Public)	Færdig	VAL service should take measures to detect and mitigate DoS attacks to minimize the impact on the network and on VAL users	VAL service should take measures to detect and mitigate DoS attacks to minimize the impact on the network and on VAL users. EVIDENCE Verification that tools such as 'ufw' are available on the VAL server for filtering packets headed for a target site. Confirmation that tools for blocking open ports and suspending facilities under attack are available and functional	a) Implement a service continuity strategy for the communications networks and/or services provided	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.434, cl. 4.1
SO23-001	TC053	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.5 3GPP TS 33.216 3GPP TS 33.511-519
SO23-002	TC066	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	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
SO23-003	TC067	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.6.2 3GPP TS 33.216 3GPP TS 33.511-519
SO23-004	TC068	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, NFV-MANO, NFVI, MEC platform, MEC host, MEC application, VIM, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.6.3 3GPP TS 33.216 3GPP TS 33.511-519

ID	Gl. ID	Emneord	Standalone (SA) eller non-standalone (NSA)	Cloud deployment modeller (X) indikerer tekniske muligheder	Status	Anbefaling	Anvisning	Formål	I overensstemmelse med (EU)	Referencer
SO23-005	TC075	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	SA and NSA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.5.2 3GPP TS 33.216 3GPP TS 33.511-519
SO23-006	TC144	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020
SO23-007	TC147	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, Network Slice Instance	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," in IEEE Access, vol. 8, pp. 99999-100009, 2020
SO23-008	TC167	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, SDN Controller	SA	Private, Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	Rec. ITU-T X.1038, cl. 7.2.2 R-17
SO23-009	TC171	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, Application data traffic, MEC host	SA and NSA	(Private), Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS MEC 002, cl. 8.3
SO23-012	TC345	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The VNF supports comparing the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM	The VNF supports comparing the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF sends an alarm to the OAM if the two resource states are inconsistent. EVIDENCE Verify whether the VNF compares the owned resource state with the parsed resource state. Verify whether the VNF sends an alarm to the OAM if the two resource states are inconsistent: 1. Use the virtualisation layer to change the resource state of VNF (e.g. change vCPU size of the VNF). 2. Use the VNF to query the parsed resource state from the OAM. 3. Use the OAM to query the parsed resource state of the VNF from the VNFM and send the received resource state to the VNF. 4. Verify that the alarm is received by the OAM.	a) Implement monitoring and logging of critical systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.5.7.2
SO23-013	TC347	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The VNF alerts the OAM upon finding an abnormal situation	The VNF alerts the OAM upon finding an abnormal situation, e.g. a VNFCI is deleted by a VIM. VNF logs the access from the VIM. EVIDENCE Log to the VIM and delete a VM of a VNF. Check that VNF alerts the OAM. The alert from the VNF is found in the OAM. Check that VNF logs the alert.	a) Implement monitoring and logging of critical systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.6.7.2
SO23-014	TC349	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	When the VIM is compromised to change the hardware resource configuration, an alert is triggered by the hardware	When the VIM is compromised to change the hardware resource configuration, an alert is triggered by the hardware. When a compromised virtualisation layer tampers the hardware resource configuration which is received from the VIM to result in the configuration error of the hardware, the hardware triggers an alert. The administrator can check the alert and determine the potential attack reported by that alert. EVIDENCE Use the VIM to make an error in hardware resource configuration (e.g. error firmware upgrade) and check whether an alert is triggered. Tamper the hardware resource configuration the virtualisation layer received from the VIM. Check whether the hardware alerts when the tampered hardware resource configuration is implemented.	a) Implement monitoring and logging of critical systems	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.7.7.2 & 5.2.5.7.7.3
SO23-019	TC348	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	The virtualisation layer alerts the driver error to the administrator	The virtualisation layer alerts the driver error to the administrator. EVIDENCE Tamper a driver on the server and implement the executive environment creation. Check whether the virtualisation layer alerts the driver error.	e) Set up tools for automated collection and analysis of monitoring data and logs	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.818, cl. 5.2.5.6.7.3
SO23-020	TC356	TELE, 5G, MONITORING, AUDITING AND TESTING, MONITORING AND LOGGING POLICIES, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	All the NFV elements should submit security events to a centralised platform	All the NFV elements should submit security events (e.g. authentication, authorisation and accounting, login attempts, administration functions and configurations) to a centralised platform, which shall monitor and analyse in real time the messages for possible attempts at intrusion. It is also recommended that all audit logs are transferred to a log management platform outside the NFV to maintain their integrity and remove the risk of tampering. EVIDENCE Check that there is a documented audit log management process. Check in log registries that local logging has been enabled on all systems and networking devices. Check in system logs that system logging is enabled to include detailed information such as an event source, date, user, timestamp, and other useful elements. Check that appropriate logs are being aggregated to a central log management system for analysis and review.	e) Set up tools for automated collection and analysis of monitoring data and logs	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ETSI GS NFV-SEC 009, cl. 6.2 & 6.4
SO24-001	TC362	TELE, 5G, MONITORING, AUDITING AND TESTING, EXERCISE CONTINGENCY PLANS, NFVI, VNF, MANO	SA	Private, Hybrid, (Public)	Færdig	MANO and NFVI nodes are set up with redundancy, and ready to support high availability	MANO and NFVI nodes are set up with redundancy, and ready to support high availability. They are distributed across multiple data centers and availability zones. EVIDENCE A documented recovery plan explaining how the NFV system is deployed so as to provide isolation and redundancy. Verify that the MNO recovery plan considers redundancy (network, power and geographic). Verify that the MNO recovery plan identifies a fail-over location for the NFV system in the event current location is inoperable.	a) Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TR 33.848, cl. 5.23.3
SO25-002	TC181	TELE, 5G, MONITORING, AUDITING AND TESTING, NETWORK AND INFORMATION SYSTEMS TESTING, MEC applications, Edge Application Server (EAS)	SA and NSA	(Private), Hybrid, (Public)	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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	ISO/IEC 27011, cl. A.18.2.3
SO29-001	TC117	TELE, 5G, THREAT AWARENESS, INFORMING USERS ABOUT THREATS, AMF, MME, gNB, eNB	SA and NSA	Private, Hybrid, (Public)	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 MNO 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	ENISA 5G Security Controls Matrix 20230524: https://www.enisa.europa.eu/publications/5g-security-controls-matrix	3GPP TS 33.501, cl. 5.10.1