Federal Office
for Information Security

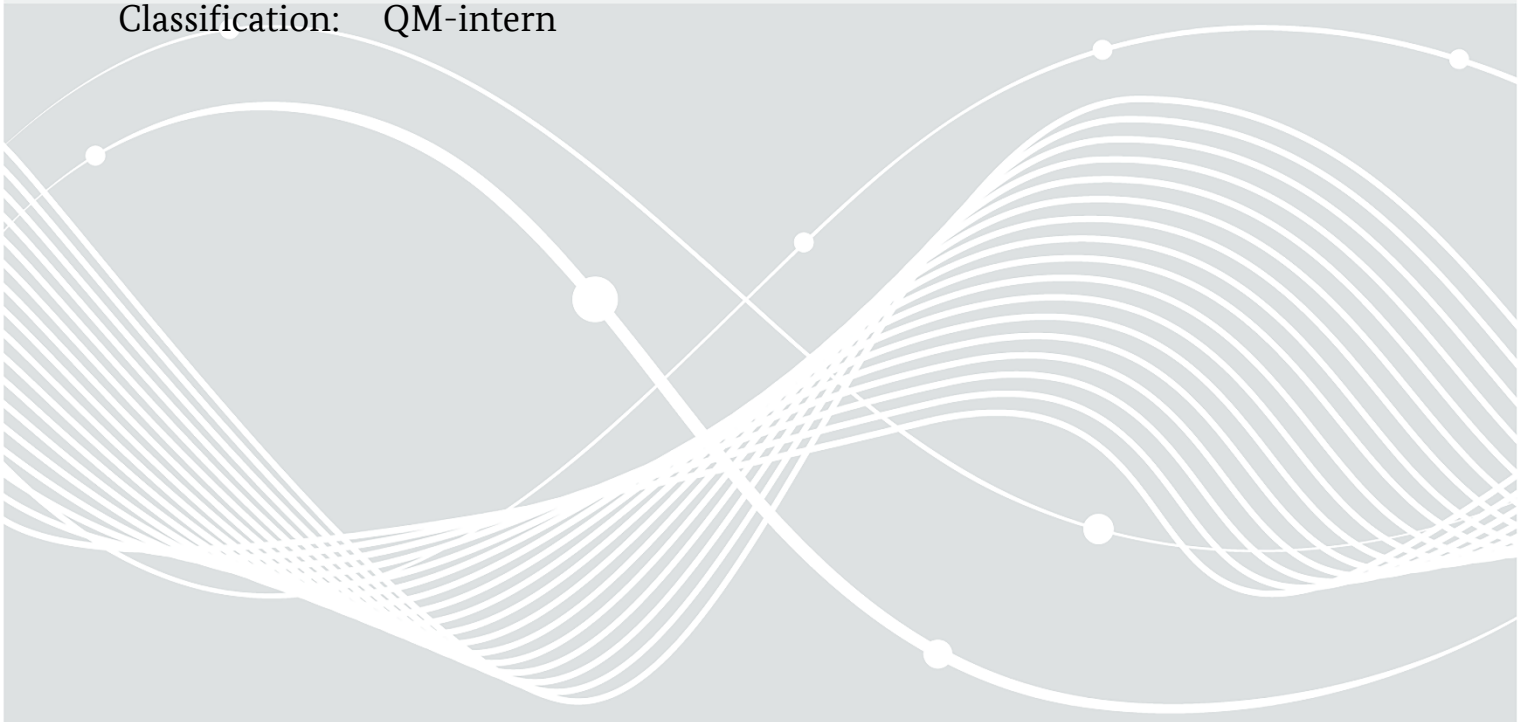
Application Notes and Interpretations of the Scheme NESAS CCS-GI (AIS)

AIS-N2 (courtesy translation)

Version 1.4 dated 2024-10-01

Process Owner: RL S 26

Classification: QM-intern



Federal Office for Information Security
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 800 2741 000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Change history

Version	*Date*	*Status*	*Change*
1.0	2022-07-01		Initial release
1.1	2022-11-30		First processing of the document and the refinements
1.2	2023-08-31		Revision: • Inclusion of corrections and improvements regarding the overall conduction of SCAS tests • Clear assignment of responsibilities regarding the evaluation activities
1.2.1	2024-02-01		Revision: • Inclusion of updates, corrections and improvements to the chapter "SCAS refinements".
1.3	2024-06-01	Courtesy Translation	Revision: • Clarification on the application of generic requirement documents • Inclusion of additional requirement documents • Adaptation of the refinements for new 3GPP release
1.3.1	2024-08-15	Courtesy Translation	Revision: • Changed the status of the translation

1.4	2024-10-01	Courtesy Translation	Revision:
			• Definition SBOM added
			• Adaption of SCAS refinements
			• General Refinements section 2.2.2:
			  • Revision of G8,
			  • Addition of G9
			• Additions to the data exchange in section 2.4.4.4

Table 1: History of changes

AIS-N2, Version 1.4

Date	2024-10-01
Status	Courtesy Translation
Topic	Network product evaluation requirements for NESAS CCS-GI
Issued by	Certification body of the BSI
Distribution list	Recognised evaluation facilities[1] BSI-internal

[1] Includes all evaluators in the evaluation facilities recognised by BSI for evaluations in accordance with NESAS CCS-GI.

Table of Contents

1 Background

The “Network Equipment Security Assurance Scheme” (NESAS) is a framework for assuring and improving security in mobile networks. NESAS is thus creating a basis for evaluating defined security properties of IT products that serve to provide a mobile network infrastructure, referred to below as network products.

For verification, the corresponding network products must be developed by the vendor in accordance with pre-audited development and lifecycle processes. Compliance with the audited processes and product-specific security requirements is then verified in an evaluation at an evaluation facility.

The certification procedure used by the BSI is based on the GSMA-NESAS evaluation scheme, which was developed by the Groupe Speciale Mobile Association (GSMA).

This document contains the rules and guidelines for network product evaluation. It lists the applicable SCAS documents and network product classes, specifies refinements for SCAS documents, and clarifies decision paths for the network product evaluation. Eventual refinements include quotations of the original text provided in the respective SCAS document, which may include errors present in the SCAS document. Furthermore, this document includes outlines for the evaluation plan and the evaluation technical report documents. The AIS is for mandatory use.

Future updates of this document will be published if needed. The applicable versions (including updates) of accepted versions of the SCAS documents, see Chapter 2.1.1, will be published in the document “Verzeichnisse” (Indexes) [Verzeichnisse].

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

2 Application notes and interpretation

2.1 Product classes and SCAS documents

This chapter lists the applicable SCAS documents and network product classes.

2.1.1 Applicable SCAS documents

The SCAS documents applicable for the NESAS CCS-GI certification are listed in Table 2.

TS	*Title*
33.116	Security Assurance Specification (SCAS) for the MME network product class
33.117	Catalogue of general security assurance requirements
33.216	SCAS for the evolved Node B (eNB) network product class
33.226	Security assurance for IP Multimedia Subsystem (IMS)
33.250	SCAS for the PDN (packet data network) gateway (PGW) network product class
33.326	SCAS for the Network Slice-Specific Authentication and Authorization Function (NSSAAF)
33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
33.512	5G SCAS; Access and Mobility management Function (AMF)
33.513	5G SCAS; User Plane Function (UPF)
33.514	5G SCAS for the Unified Data Management (UDM) network product class
33.515	5G SCAS for the Session Management Function (SMF) network product class
33.516	5G SCAS for the Authentication Server Function (AUSF) network product class
33.517	5G SCAS for the Security Edge Protection Proxy (SEPP) network product class
33.518	5G SCAS for the Network Repository Function (NRF) network product class
33.519	5G SCAS for the Network Exposure Function (NEF) network product class
33.520	5G SCAS for Non-3GPP InterWorking Function (N3IWF)
33.521	5G SCAS; Network Data Analytics Function (NWDAF)
33.522	5G SCAS; Service Communication Proxy (SCP)
33.523	5G SCAS; Split gNB product classes
33.526	Security assurance specification for the Management Function
33.527	Security Assurance Specification (SCAS) for 3GPP virtualized network products
33.528	Security Assurance Specification (SCAS) for the Policy Control Function (PCF)
33.537	Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)

Table 2: Applicable SCAS documents

The currently valid and accepted version of the SCAS documents for NESAS CCS-GI is given by the BSI document “Verzeichnisse” (Indexes) [Verzeichnisse] (i.e. list of all applicable documents for certifications).The application form for a NESAS CCS-GI certification requires the information about the product class of the network product under evaluation. The dedicated list of product classes is presented in Table 3 below.

Product class	*SCAS document*
MME network equipment (MME)	TS 33.116
evolved Node B (eNB)	TS 33.216
IP Multimedia Systems (IMS)	TS 33.226
PGW network equipment (PGW)	TS 33.250
Network Slice-Specific Authentication and Authorization Function (NSSAF)	TS 33.326
next generation Node B (gNodeB)	TS 33.511
Access and Mobility manag. Func. (AMF)	TS 33.512
User Plane Function (UPF)	TS 33.513
Unified Data Management (UDM)	TS 33.514
Session Management Function (SMF)	TS 33.515
Authentication Server Function (AUSF)	TS 33.516
Security Edge Protection Proxy (SEPP)	TS 33.517
Network Repository Function (NRF)	TS 33.518
Network Exposure Function (NEF)	TS 33.519
Non-3GPP InterWorking Function (N3IWF)	TS 33.520
Network Data Analytics Function (NWDAF)	TS 33.521
Service Communication Proxy (SCP)	TS 33.522
Split gNode B (Split gNB)	TS 33.523
Policy Control Function (PCF)	TS 33.528
Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF)	TS 33.537

Table 3: Mapping of product classes and applicable SCAS documents

Only these listed product classes are available for certification. For all product classes, an additional evaluation according to TS 33.117 is mandatory. If the architectural overview for the network product under evaluation provides evidence of architectural choices or interfaces, for which an applicable, generic SCAS document exists, an evaluation according to the relevant generic SCAS document is mandatory as well. A list of possible generic SCAS documents with this regards include:

- TS 33.526
- TS 33.527

Any choice of generic SCAS documents for evaluation shall be approved prior to evaluation by the certification body. The certification body may require the inclusion of generic SCAS documents, if the architectural choices or additional interfaces documented by the vendor, make this inclusion useful. The inclusion of additional generic SCAS documents for a network product by the certification body may be required at any time throughout the evaluation process, if evidence of interfaces covered by generic SCAS documents arises.

For unknown or new product types the certification body shall be contacted prior to formally requesting a certification.

The network product should be tested within the runtime execution hardware or the virtualization and orchestration environment recommended by the vendor. If the network product can be executed on different runtime, orchestration, virtualization and execution environments, for which the vendor assumes equal behaviour when conducting the SCAS tests, these platforms are considered different configurations of the network product. These platforms shall be listed by the evaluation facility and examined with regards to equivalent behaviour in order to be covered by the certificate.

Generally, the network product should be fully deployable in the test facility location.

2.2 General Refinements

2.2.1 Introduction

This subchapter directly refers to the applicable SCAS documents given in Chapter 2.1.1. and lists general and single document related refinements. All refinements are for mandatory use. Crossed out text is replaced or clarified by underlined text. Every refinement has a unique identification in the format *SCAS-Document-ID_*.

The certification body should be contacted for individual decisions, if necessary.

2.2.2 Refinements

G1: If specific tests cannot be executed, a detailed description of the reasons for the non-testability must be provided.

G2: All vendor documentation verified by the evaluation facility must be provided as test evidence.

G3: All tools used for a test shall be documented in respective evidences with their unique name, version and configuration.

G4: The tester shall document every executed test step thoroughly with the effectively used tools, commands, parameters, configuration etc.

G5: Tests for software components shall be applied to every instance of the software with a different version or configuration (e.g. multiple web servers in the Network Product under test).

G6: All evidence requested in the SCAS documents shall be produced.

G7: For all SCAS tests that generate network traffic, this traffic shall be stored as part of the evidence documentation and should be provided to the certification body upon request (e.g. as PCAP files). If this is not possible or requires an unreasonable amount of effort the certification body shall be contacted as soon as possible, usually before commencing the tests.

G8: All tests have to be executed and test results and further evidence have to be stored in a way so that the test can be re-executed by the same evaluation facility again. Settings performed by the evaluator on the network product to conform with the requirements provided by the preconditions, shall be provided as part of the evidences.

G9: Encrypted network packets shall be provided as evidences in the original encryption and with required key materiel for decryption.

2.3 SCAS refinements

2.3.1 TS 33.117 (General Requirements)

2.3.1.1 Refinement ID R_33.117_4.2.3.2.2

Section 4.2.3.2.2 Protecting data and information -- Confidential System Internal Data

Valid as of SCAS version: 16.7.0

Requirement Reference: In accordance with industry best practice.

Requirement Description: When the system is not under maintenance, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such functions could be, for example, local or remote O&M CLI or GUI, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).

Threat References: TR 33.926 [4], clause 5.3.6.4, Insecure Data Storage

Test case:

Test Name: TC_CONFIDENTIAL_SYSTEM_INTERNAL_DATA

Purpose:

Verify that no system function reveals sensitive data in the clear

Procedure and execution steps:

Pre-Condition:

The vendor shall provide documentation describing how confidential system internal information that could possibly be revealed in clear-text is handled by system functions.

A list of all system functions in the network product, information on how to enable and execute them should be provided as a part of the vendor's documentation. A system function is every function implemented in the network product needed by the services/functionalities provided by the network product itself.

Execution Steps

Execute the following steps:

1. Review the documentation provided by the vendor describing how confidential system internal information is handled by system functions.
2. The tester checks if all system functions as described in the product documentation (e.g. local or remote O&M CLI or GUI, logging messages, alarms, error messages, configuration file exports, stack traces) whether they reveal any confidential system internal data in the clear (for example, passphrases).

Expected Results:

There should be no confidential system internal data revealed in the clear by each system function.

Expected format of evidence:

Evidence suitable for the interface, e.g. screenshot containing the operational results.

In case of non-GUI applications (e.g. REST-Request/Response, Stack Trace...) a log file is required.

2.3.1.2 Refinement ID R_33.117_4.2.3.4.1.2_3

Section 4.2.3.4.1.2 Accounts shall allow unambiguous identification of the user.

Valid as of SCAS version: 16.7.0

Test Case: TC_ACCOUNT_NUMBER

Test Purpose: To ensure that a minimum number of individual accounts per user data base is supported. The minimum number is defined in the requirement description of this clause.

Procedure and execution steps:

Pre-Condition:

All user data bases for names and credentials supported by the network product are identified in the documentation accompanying the network product.

The vendor shall supply documentation for each user data base supported by the network product, containing the account creation mechanism and the minimum number of idividual accounts per user data base.

Execution Steps:

The accredited evaluator's test lab is required to execute the following steps:

1. Create accounts until the minimum number of accounts is reached.

Expected Results:

Successful creation of the minimum number of accounts.

Expected Format of Evidence:

Test report that lists the reviewed documentation, reviewed user databases, and the findings.

2.3.1.3 Refinement ID R_33.117_4.2.3.4.2.2

Requirement Name: Deletion or disablement of predefined accounts.

Requirement Reference: In accordance with industry best practice.

Requirement Description: All predefined or default accounts shall be deleted or disabled. Many systems have default accounts (e.g. guest, ctxsys), some of which are preconfigured with or without known passwords. These standard users shall be deleted or disabled. Should this measure not be possible the accounts shall be locked for remote login. In any case disabled or locked accounts shall be configured with a complex password as specified in clause 4.2.3.4.3.1 Password Structure. This is necessary to prevent unauthorized use of such an account in case of misconfiguration.

Exceptions to this requirement to delete or disable accounts are accounts that are used only internally on the system involved and that are required for one or more applications on the system to function. Also for these accounts remote access or local login shall be forbidden to prevent abusive use by users of the system.

Threat References: TR 33.926 [4], clause 5.3.3.1, Default Accounts

Test Case:

Test Name: TC_PREDEFINED_ACCOUNT_DELETION

Purpose:

To ensure that predefined accounts are deleted or disabled unless there is specific exception as defined in the requirement 4.2.3.4.2.2.

Procedure and execution steps:

Pre-Conditions:

1. All predefined accounts are identified in the documentation accompanying the Network Product.
2. Instructions of how administrator user can view all existing accounts in the database are provided in the documentation accompanying the Network Product.

NOTE: No test is provided here for finding undocumented hard coded accounts as such tests can be impossible to define in a general way.

Execution Steps:

1. Check in documentation of the existence of any documented predefined account and what is the reason for existence.
2. After login via account with necessary access rights (e.g. Admin) search in the database for any undocumented account.
3. Check the password complexity of such existing predefined accounts according to the test provided in clause 4.2.3.4.3.1.
4. Attempt local (if applicable) and remote login to such predefined accounts.

Expected Results:

1. Predefined accounts are either deleted/ disabled or, if existing, the reason is in accordance with the requirement exception.
2. If there are active predefined accounts in accordance with the requirement exception then there is no local and remote login possibility.
3. If predefined account is either disabled or locked then it shall anyway fulfil the complex password requirements as specified in clause 4.2.3.4.3.1 after enabling or unlocking it.

Expected format of evidence:

- List of documented and undocumented accounts.
- Evidence ~~can~~shall be presented in the form of screenshot/screen-capture on showing for example a remote login failure or complexity of a password of e.g. locked or disabled accounts.
- Log files containing the results of local and remote login attempts

2.3.1.4 Refinement ID R_33.117_4.2.3.4.3.2

Section 4.2.3.4.3.2 Password changes

Valid as of SCAS version: 16.7.0

Requirement Name: Password changes

Requirement Reference: In accordance with industry best practice

Requirement Description:

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry.

Previously used passwords shall not be allowed up to a certain number (Password History).

The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its default value shall be 3. This means that the network product shall store at least the three previously set passwords. The maximum number of passwords that the network product can store for each user is up to the vendor.

When a password is about to expire a password expiry notification shall be provided to the user.

Above requirements shall be applicable for all passwords used(e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.

Threat References: TR 33.926 [4], clause 5.3.3.2, Weak Password Policies

Test case:

Test Name: TC_PASSWORD_CHANGES

Purpose:

- To check whether the network product is provisioned with the functionality that enables its user to change the password at any time.
- The network product enforces password change after initial login.
- To verify the new password adheres to the password management policy and also to verify whether it has password expiry rule.
- The network product is configured to disallow specified number of previously used passwords (Password History).

Procedure and execution steps:

Pre-Conditions:

1. Tester has account with username and password in the network product.
2. Network product vendor will provide documentation for password management policy which should include details on how to change the password, configure password expiry rule and disallowing specified number of previously used passwords.
3. The network product vendor shall supply information on how many passwords the network product can store for each user in the password history.
4. The tester has privilege to modify the number of disallowed previously used password.

Execution Steps

Execute the following steps:

A. Positive Test

Case 1:

- Test case to enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

1. The tester logs into network product application using a privileged account.
2. The tester configures the password expiry rules for a user Y such that the network product application generates password expiry notification for user Y to force user Y to change the password.
3. The tester logs out as a privileged user and logs on as user Y.

4. The tester is prompted to change his password and creates a new password by following the password policy management.
5. The network product application confirms change in password by, for example, displaying "Password Changed Successfully".
6. The tester successfully logs-in the network product application as user Y using the new password.

Case 3:

1. The tester logs into network product application using a privileged account.
2. Tester configures the network product application for number of disallowed previously used passwords to x with x > 0, preferably x = 3
3. The tester requests for a password change for user Y.
4. The tester logs out of the privileged account and logs on as user Y
5. The tester creates a new password by following the password policy management.
6. If the password is not equal to any of the x previously used passwords, the network product application still accepts the new password and displays "Password Changed Successfully" or an equivalent success message.

B. Negative Test

Case 1:

- Test case to enforce password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

- No negative test case for this scenario.

Case 3:

1. The tester logs into network product application using privileged account.
2. Tester configures the network product application for number of disallowed previously used passwords to x (with x > 0, preferably x = 3) for user Y.
3. The tester logs out of the privileged account and logs in as user Y
4. The tester requests for a password change.
5. The tester sets the new password to a value that is among the last x passwords used previously x times.

Expected Results:

A. Positive Test

Case 1:

- Expected result for enforcing password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

- User Y receives a password expiry notification, is forced to change their password and the Tester can successfully change the password.

Case 3:

- Tester can successfully change the password.

B. Negative Test

- If the negative test case passes, this shows that network product application does not work properly and it violates the requirement.

Case 1:

- Expected result for enforcing password change after initial login is covered in clause 4.2.3.4.2.3.

Case 2:

- No negative test case for this scenario.

Case 3:

- The tester cannot successfully change the password.

Expected format of evidence:

- Evidence suitable for the interface, e.g. screenshot contains the operation result.
- Add screenshot of the password expiry notification for Test Case A.2.
- Document the configured number of disallowed previously used passwords, the last x passwords for user Y and attempted password changes for Test Case A.3 and B.3.

2.3.1.5 Refinement ID R_33.117_4.2.3.4.4.1

Section 4.2.3.4.4.1 Network Product Management and Maintenance interfaces

Valid as of SCAS version: 16.7.0

Test Case: TC_MUTUAL_AUTHENTICATION-ON_NETWORK_PRODUCT_MANAGEMENT_PROTOCOLS

Test Purpose: There is mutual authentication of entities for management interfaces on the network product.

Procedure and execution steps:

Pre-Condition:

Documentation that lists each of the management protocols and describes the authentication mechanism used for each one.

Execution Steps:

1. The tester checks that the authentication mechanisms have been configured on the network product.
2. For each management interface:
    a. The tester triggers communication between network product and a test entity that has a legitimate authentication credential.
    b. Then, the tester triggers communication between network product and a test entity that doesn't have a legitimate authentication credential.

Expected Results:

- Mutual authentication is successful and communication between network product and the entity with correct credentials can be established.
- Mutual authentication fails and communication between the network product and the entity with incorrect credentials cannot be established.

Expected Format of Evidence:

- Logs of successful and failed communication attempts.
- Test result pass/fail recorded by tester.

2.3.1.6 Refinement ID R_33.117_4.2.3.4.6.1

Section 4.2.3.4.6.1 Authorization policy

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: verify authorization policy is in place and that user access and data access in the system are according to the authorization policy.

Procedure and execution steps:

Pre-Condition:

Documentation describing the authorization policy defined for the system including details on the lowest access rights assigned to user accounts, access to data, application execution and components.

Execution Steps:

1. Verify in vendor documentation that the authorization policy in the system applies the principle of least privilege
2. Assign access rights (e.g. read only) to user accounts, data files, and applications.
3. Operations, that are allowed and disallowed as per authorization policy (as defined in the network product documentation), are attempted via the different user accounts, data files, and applications.

Expected Results:

1. User accounts, data files, and applications are allowed to be accessed (e.g. able to read but not write to a file, able to execute an application as a user account without administrator rights, etc.) according to the access rights assigned.
2. User accounts, data files, and applications are not allowed to be accessed above the access rights assigned (e.g. able to write to a read only file, able to execute an application as an administrator, etc.).

Expected Format of Evidence:

- Log of attempted operations, result of step 3.
- Pass/fail results as recorded by the tester.

2.3.1.7 Refinement ID R_33.117_4.2.3.4.6.2

Section 4.2.3.4.6.2 Role-based access control

Valid as of SCAS version: 16.7.0

Requirement Name: Role-based access control

Requirement Reference: In accordance with industry best practice

Requirement Description:

The network product shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The domains could be Fault Management (FM), Performance Management (PM), System Admin, etc. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform, i.e. the specific operation command or command group (e.g. View, Modify, Execute).

The network product supports RBAC, in particular, for O&M privilege management for network product Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface.

Threat References: TR 33.926 [4], clause 5.3.8.2, Over-Privileged Processes/Services

Test case:

Purpose:

Verify that users are granted access with role-based privileges.

Procedure and execution steps:

Pre-Conditions:

Documentation describing the role based access control system including details on which user roles are defined.

Execution Steps

1. User accounts which are assigned to different access roles are created (at least one user per existing role).
2. Operations, that are allowed and disallowed by different roles (as defined in the network product documentation), are attempted via the different user accounts.

Expected Results:

1. Users that are assigned to a role that is not allowed to execute an operation are prevented from executing the operation.
2. Users that are assigned to a role that is allowed to execute an operation can successfully execute the operation.

Expected format of evidence:

Pass/fail results as recorded by the tester.

2.3.1.8 Refinement ID R_33.117_4.2.3.6.2

Section 4.2.3.6.2 Log transfer to centralized storage

Valid as of SCAS version: 16.7.0

Requirement Name: Log transfer to centralized storage

Requirement Reference: In accordance with industry best practice

Requirement Description:

1. The Network Product shall support forwarding of security event logging data to an external system. Secure transport protocols in accordance with clause 4.2.3.2.4, shall be used.
2. Log functions should support secure uploading of log files to a central location or to an external system for the Network Product that is logging.

Threat References: TR 33.926 [4], clause 5.3.4.4, Log Tampering

Test Name: TC_LOG TRANS_TO_CENTR STORAGE

Purpose:

To ensure log shall be transferred to centralized storage.

Procedure and execution steps:

Pre-Conditions:

- The vendor shall list the protocols which transfer security event logging data (in accordance with clause 4.2.3.2.4).
- The session between network product and central location or external system for network product log functions has been set up.
- The tester has privilege to operate network product and related logs can be outputted.

Execution Steps

1. The tester configures the network product to forward event logs to an external system (according to bullet a) of requirement) and related logs are sent out.
2. The tester checks whether the used transport protocol is secure protocol (in accordance with clause 4.2.3.2.4).
3. The tester checks whether the central location or external system for network product log functions has stored the related logs.
4. The tester configures the network product for secure upload of event log files to an external system (according to bullet b) of requirement) and performs a log file upload.
5. The tester checks whether the used transport protocol for log file upload is a secure protocol (in accordance with clause 4.2.3.2.4).
6. The tester checks whether the central location or external system for network product log functions has stored the related logs.
7. The tester verifies that all actually used transport protocols are equal to the ones stated in the vendor documentation

Expected Results:

- The listed transport protocols are secure protocols.
- The used transport protocol for log file upload is a secure standard protocol.
- The tester finds that the central location or external system for network product log functions has stored the related logs.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- Settings, protocols and configurations used,
- Screenshot
- Test result (Passed or not)

2.3.1.9 Refinement ID R_33.117_4.3.3.1.2_4

Section 4.3.3.1.2 Minimized kernel network functions

Valid as of SCAS version: 16.7.0

Test Name: TC_ IP_MULTICAST_HANDLING

Purpose:

Verify that IP Multicast is disabled by default on the network product. In particular this test case verifies that packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) are not handled by the network product.

Procedure and execution steps:

Pre-Conditions:

- Network traffic analyser on the network product or an external traffic analyser directly connected to the network product is available.
- Network product

Capability:

NOT applicable in certain deployment scenarios where multicast needs to be enabled.

Execution Steps

1. If the feature is available in a configuration file, verify that it is disabled by default.
2. Verify that none of the network product's interfaces is configured for handling IP packets from multicast addresses and therefore not running Multicast (e.g. typing command ip maddr or ifconfig on any Unix® based platform)

Expected Results:

No interface is running multicast protocols (demonstrated by the command output of step 2, e.g. an empty list of multicast addresses attached to the interfaces queried by the *ip maddr* command)

Expected format of evidence:

Screenshot containing command output.

2.3.1.10 Refinement ID R_33.117_4.3.4.3

Section 4.3.4.3 No unused HTTP methods

Valid as of SCAS version: 16.7.0

Requirement Name: No unused HTTP methods

Requirement Reference: In accordance with industry best practice

Requirement Description:

HTTP methods that are not required shall be deactivated. Standard requests to web servers use GET, HEAD, and POST. If other methods are required, e.g, PUT, DELETE, PATCH, they shall not introduce security leaks such as TRACK or TRACE.

Threat References: TR 33.926 [4] clause 5.3.6.11, Unnecessary Services

Test Case:

Test Name: TC_NO_UNUSED_HTTP_METHODS

Purpose:

Verify that the Web server has deactivated all HTTP methods that are not required.

Procedure and execution steps

Pre-Conditions:

- The tester has needed administrative privileges.
- A tester machine is available.
- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.
- vendor provides list of enabled and necessary HTTP methods

Execution Steps

- Check that relevant system settings and configurations are in place to ensure fulfilment of the requirement.

Expected Results:

- System settings and configurations have been found and in normal operation, for all Web components of the system, to ensure that unneeded HTTP methods are deactivated.

Expected format of evidence:

A testing report providing the following information:

- Log files and screen shots of test executions
- web server log showing denial of disabled HTTP methods
- part of web server config showing enabled/disabled HTTP methods
- Test result (Passed or not)

2.3.1.11 Refinement ID R_33.117_4.3.4.6

Section 4.3.4.6 No CGI or other scripting for uploads

Valid as of SCAS version: 16.7.0

Test Case: TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS

Test Purpose: To test whether the upload directory is equal to the CGI/Scripting directory.

Pre-Condition:

If the web server is configured with CGI/Scripting on, this test applies.

Execution Steps:

Execute the following steps:

1. The tester checks whether the upload directory is configured to be different from the CGI/Scripting directory.
2. The tester checks whether the web server has no write permissions for CGI/scripting directories.

Expected Results:

The configured upload directory is different from the CGI/Scripting directory.

Additional evidence might be provided that shows that the web server has no write rights for the CGI/Scripting directory.

Expected Format of Evidence:

- A part of the configuration file ~~/~~ and optionally screenshot of the configuration showing that the web server is properly configured.
- Console output of access rights for CGI/scripting directory

2.3.1.12 Refinement ID R_33.117_4.3.4.10

Section 4.3.4.10 No directory listings

Valid as of SCAS version: 16.7.0

Requirement Name: No directory listings / Directory Browsing.

Requirement Reference: In accordance with industry best practice

Requirement Description: Directory listings (indexing) / "Directory browsing" shall be deactivated.

Threat References: TR 33.926 [4], clause 5.3.6.9, File/Directory Read Permissions Misuse

Test Case:

Test Name: TC_NO_DIRECTORY_LISTINGS

Purpose:

To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

Procedure and execution steps

Pre-Conditions:

- The tester has administrative privileges
- A tester machine is available.
- The tester should have configured a script, or an automatic assessment tool adapted in line with the Requirement Description..

Execution Steps

1. The tester checks the web server configuration that Directory listings (indexing) / "Directory browsing" has been deactivated in all Web server components.
2. Verify whether it is possible to list/browse web server directories.

Expected Results:

- Evidence that Directory listing / Directory browsing has been deactivated in all Web server components.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions
- part of web server configuration showing that directory listing/browsing is disabled
- web server log denying directory listing/browsing
- Test result (Passed or not)

2.3.1.13 Refinement ID R_33.117_4.3.4.12

Section 4.3.4.12 Web server information in error pages

Valid as of SCAS version: 16.7.0

Requirement Name: Web server information in error pages.

Requirement Reference: In accordance with industry best practice

Requirement Description: User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.

Threat References: TR 33.926 [4], 5.3.6.5, System Fingerprinting

Test Case:

Test Name: TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION

Purpose:

To verify that error pages and error messages do not include information about the web server.

Procedure and execution steps

Pre-Conditions:

- The tester has needed administrative privileges.
- A tester machine is available.

- The tester should have configured a script, or an automatic assessment tool adapted in line with the Requirement Description.
- The vendor provides a list of potential parameters, suitable to trigger events resulting in an http error 4xx and 5xx

Execution Steps

- The tester verifies the correctness of the vendor listing of all web server error pages and messages (e.g. from web server configuration).
- The tester verifies~~checks~~ that (all listed) generated error pages and error messages do not include information about the web server by sending appropriate requests or trigger error page generation otherwise.

Expected Results:

- Evidence that generated error pages and error messages do not include information about the web server.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions
- part of web server config showing error page handling (if applicable)
- error pages templates (if applicable)
- Test result (Passed or not)

2.3.1.14 Refinement ID R_33.117_4.3.5.1

Section 4.3.5.1 Traffic Separation

Valid as of SCAS version: 16.7.0

Requirement Name: Traffic Separation

Requirement Reference: In accordance with industry best practice

Requirement Description:

The network product shall 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. See RFC 3871 [3] for further information.

Threat References: TR 33.926 [4], clause 5.3.6.15, lack of GNP traffic isolation

Test case:

Test Name: TC_TRAFFIC_SEPARATION

Purpose:

To test whether traffic belonging to different network domains is separated.

Procedure and execution steps:

Pre-Condition:

NOTE: This test applies if the network product is meant to handle traffic from different network domains, e.g. both O&M and control plane traffic.

- The network product has at least two separate (logical) interfaces dedicated to different network domains. The vendor provides this domain related information for the tester. Network products for which the test applies and that fail to meet this precondition fail the test by definition.
- Vendor documentation describing how traffic separation is implemented on the network product and how traffic separation can be configured.
- Vendor documentation listing all traffic domains and interfaces.

Execution Steps

Execute the following steps:

1. The tester verifies whether the vendor documented traffic separation mechanism is suitable according to the requirement description (RFC 3871 [3]).
2. The tester checks whether the network product refuses traffic intended for one network domain on all interfaces meant for the other network domain, and vice versa.
3. Step ~~1~~2 is to be performed for all pairs of different network domains.

Expected Results:

The two tests are successful.

Traffic should not be passed to a domain from which it did not originate.

Expected format of evidence:

A PASS or FAIL.

2.3.1.15 Refinement ID R_33.117_4.3.6.3

Section 4.3.6.3 Unique key values in IEs

Valid as of SCAS version: 16.7.0

Requirement Name: Validation of the unique key values in IEs.

Requirement Reference: TS 29.501 Principles and Guidelines for Services Definition [13], clause 6.2.

Requirement Description: For data structures where values are accessible using names (sometimes referred to as keys), e.g. a JSON object, the name is expected to be unique. The occurrence of the same name (or key) twice within such a structure leads to an error and the rejection of the message.

Threat References: TR 33.926 [4], clause 6.3.2.2, JSON Parser not Robust

Test Case:

~~NOTE: This requirement can also be verified as part of Robustness and Protocol fuzzing tests as defined in clause 4.4.4 Robustness and fuzz testing according to referenced requirements.~~

This Test is mandatory if applicable for the interface.

Purpose:

Verify that the API implementation fullfills the requirements as specified in 29.501 [13], clause 6.2.

Pre-Conditions:

Test environment with network product under test so that the tester is able to send HTTP requests with keys (valid and duplicate) in message IE payload towards the network product under test. Rest of the network and network products may be simulated.

Execution Steps

1. The test equipment sends HTTP requests with duplicate keys in message IE payload to the network product under test.
2. The test equipment sends valid requests to network product under test

Expected Results:

1. Network product under tests responses with an error message
2. Network product under test still responses normally to valid requests

Expected format of evidence:

- A testing report provided by the testing agency which will consist of the following information:
- The used tool(s) name and version information,
- Settings and configurations used
- The output log file of the chosen tool that displays the results (passed/failed).
- Test result (Passed or not)
- Log/evidence tracing possible crashes
- Information of any input causing unspecified, undocumented, or unexpected behaviour

2.3.1.16 Refinement ID R_33.117_4.3.6.4

Section 4.3.6.4 The valid format and range of values for IEs

Valid as of SCAS version: 16.7.0

Requirement Name: Validation of the IEs limits.

Requirement Reference: TS 29.501 Principles and Guidelines for Services Definition [13], clause 6.2

Requirement Description: The valid format and range of values for each IE, when applicable, is defined unambiguously:

- For each message the number of leaf IEs does not exceed 2048K.
- The maximum size of the JSON body of any HTTP request does not exceed 16 million octets.
- The maximum nesting depth of leaves does not exceed 32.

Threat References: TR 33.926 [4], clause 6.3.2.2, JSON Parser not Robust

Test Case:

~~NOTE 1: This requirement can also be verified as part of Robustness and Protocol fuzzing tests as defined in clause 4.4.4 Robustness and fuzz testing according to referenced requirements.~~

This Test is mandatory if applicable for the interface.

Purpose:

Verify that the API implementation fullfills the requirements as specified in 29.501[13], clause 6.2.

Pre-Conditions:

Test environment with network product under test so that the tester is able to send HTTP requests with “out of bound IEs” towards the network product under test.. Rest of the network may be simulated.

NOTE 2: IEs having invalid format and/or not in the defined range of values can be considered as out of bound IEs.

Execution Steps

1. For all requirements stated in TS 29.501[13], clause 6.2, the test equipment sends at least 2 different HTTP requests with out of bounds IEs towards the network product under test.

Expected Results:

- Network product under tests responses with an error message.

Expected format of evidence:

A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information,
- Settings and configurations used.
- The output log file of the chosen tool that displays the results (passed/failed).
- Test result (Passed or not).
- Log/evidence tracing possible crashes.
- Information of any input causing unspecified, undocumented, or unexpected behaviour.

2.3.1.17 Refinement ID R_33.117_4.4.4

Section 4.4.4 Robustness and fuzz testing

Valid as of SCAS version: 16.7.0

Requirement Name: Robustness and fuzz testing

Requirement Reference: 4.2.6.2.2. – Interface Robustness

Requirement Description:

It shall be ensured that externally reachable services are robust enough to detect or dismiss unexpected or malformed input.

Threat References: TR 33.926 [4], clause 5.3.7, Denial of service

Test case:

Test Name: TC_BVT_ROBUSTNESS AND FUZZ TESTING

Purpose:

To verify that the network product provides externally reachable services which are robust against unexpected or malformed input. The target of this test are the protocol stacks (e.g. diameter stack) rather than the applications (e.g. web app).

Procedure and execution steps:

Pre-Conditions:

- The tester has the privileges to log in the network product and to access all system resources (e.g. log files)
- A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
  - all interfaces providing IP-based protocols;
  - the available transport layer protocols on these interfaces;
  - their open ports and associated services;
  - and a free-form description of their purposes.

NOTE: This list is to be validated as part of the BVT port scanning activity.

- The robustness and fuzzing tools that are selected for this test shall be capable to identify input which causes the Network Product to behave in an unspecified, undocumented, or unexpected manner.
- Fuzz testing tools are a highly sophisticated technology and adaptation to the individual protocols in question is needed to be effective. Therefore, there is a lack of effective fuzz testing tools available especially for protocols proprietary to the Telco industry. Taking into account note 4 in clause 7.2.4 of TR 33.916 [19], test labs shall acquire fuzz testing tools for those protocols where commercially feasible.
- It needs to be taken into account that fuzz testing tools might show drastic differences in terms of effectiveness. The tester is expected to recognize faults, misuse, or crashes in the protocol under test to determine the level of effectiveness of the available tools.
- The requirements provided by the document [AIS-50] and the documents reference herin shall be considered in the execution of this test case. Testing in accordance with [AIS-50] and the referenced documents shall be performed according to the requirements for EAL 2
- A network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product and on a tester machine is available.

Execution Steps

The tester is required to execute the following steps:

1. Execution of fuzzing tools against the protocols available via interfaces providing IP-based protocols of the Network Product for a coverage of tests sufficient to be effective.
2. Execution of robustness test tools against the protocols available via interfaces providing IP-based protocols of the Network Product for a coverage of tests sufficient to be effective.

For both step 1 and 2:

1. Using a network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product, the tester verifies that the packets are processed correctly by the network product.
2. The testers verifies that the network product and any running network service does not crash.
3. The execution of tests shall run sufficient times. Additional information may be taken from [AIS-50] and the herein referenced documents.
    a. To fulfil the test requirements of 4.2.3.3.4 the tester shall ensure that all input error classes are explicitly covered by the test (e.g. by manually crafting invalid input).
    b. To fulfil the test requirements of 4.2.6.2.2 the tester shall ensure that at least all examples of the requirements are covered.

Expected Results:

A list of all of the protocols of the network product reachable externally on an IP-based interface, together with an indication whether robustness and fuzz testing tools have been used against them, shall be part of the testing documentation. If no tool can be acquired for a protocol, ~~a free form statement should explain why not~~ the vendor shall provide detailed information about the protocol to enable the test lab to adapt a general purpose robustness or fuzzing tool.

The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.

Any input causing unspecified, undocumented, or unexpected behaviour, and a description of this behaviour shall be highlighted in the testing documentation.

COTS fuzzing tools, by their nature, may have an acceptable failure rate (e.g. 0.1%) due to different non-deterministic variables in their implementation. At some point the tool's documentation may even mention

that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NE or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

Expected format of evidence:

- A testing report provided by the testing agency which will consist of the following information:
- The used tool(s) name and version information,
- Settings and configurations used
- The output log file of the chosen tool that displays the results (passed/failed).
- Screenshot
- Test result (Passed or not)
- Log/evidence tracing possible crashes
- Any input causing unspecified, undocumented, or unexpected behaviour

2.3.2 TS 33.511 (gNB)

2.3.2.1 Refinement ID R_33.511_4.2.2.1.4

Section 4.2.2.1.4 RRC integrity check failure

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify that RRC integrity check failure is handled correctly by the gNB.

Pre-Conditions:

Test environment with a UE. The UE may be simulated. RRC integrity protection is activated at the gNB.

Execution Steps

1. The UE sends a RRC message to the gNB without MAC-I~~; or~~
2. The UE sends a RRC message to the gNB with a wrong MAC-I.
3. The gNB verifies the integrity of the RRC message from the UE.

Expected Results:

The RRC message is discarded by the gNB after step 1a) ~~or~~and after step 2b).

Expected Format of Evidence:

Sample copies of the log files.

2.3.2.2 Refinement ID R_33.511_4.2.2.1.5

Section 4.2.2.1.5 UP integrity check failure

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify that UP integrity check failure is handled correctly by the gNB.

Pre-Conditions:

Test environment with a UE. The UE may be simulated. UP integrity protection is activated at the gNB.

Execution Steps

1. The UE sends a PDCP PDU to the gNB without MAC-I.~~; or~~
2. The UE sends a PDCP PDU to the gNB with a wrong MAC-I.
3. The gNB verifies the integrity of the PDCP PDU from the UE.

Expected Results:

The PDCP PDU is discarded by the gNB after step 1a) ~~or~~and after step 2b).

Expected Format of Evidence:

Evidence suitable for the interface e.g. Screenshot containing the operational results. Sample copies of the log files.

2.3.2.3 Refinement ID R_33.511_4.2.2.1.8

Section 4.2.2.1.8 Replay protection of user data between the UE and the gNB

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: To verify that the user data packets are replay protected over the NG RAN air interface.

Test Name: TC-UP-DATA-REPLAY_gNB

Pre-Condition:

- The gNB network product shall be connected in emulated/real network environments. The UE may be simulated.
- The tester shall have access to the NG RAN air interface.
- The tester shall active the user plane integrity protection of the RRC-signalling packets.

Execution Steps:

1. The tester shall capture the user plane data sent between UE and gNB using any network analyser over the NG RAN air interface.
2. Tester shall filter user plane data packets sent between UE and gNB.
3. Tester shall replay the captured user plane packets or shall use any packet crafting tool to create a user plane packet similar to the captured user plane packet and replay to the gNB.
4. Tester shall check whether the replayed user plane packets were processed by the gNB by verifying the gNB log files or capturing over NG RAN air interface to see if any corresponding response message is received from the gNB.
5. Tester shall confirm that gNB provides replay protection by dropping/ignoring the replayed packet if the gNB logs the corresponding event or no corresponding response is received from the gNB to the replayed packet.
6. Tester shall verify from the result that if the replayed user plane packets are not accepted by gNB, the NG RAN air interface is replay protected.

Expected Results:

The user plane packets sent between the UE and gNB over the NG air interface is replay protected.

Expected Format of Evidence:

- Evidence suitable for the interface, e.g. Screenshot containing the operational results.
- Log files

2.3.2.4 Refinement ID R_33.511_4.2.2.1.14

Section 4.2.2.1.14 Bidding down prevention in Xn-handovers

Valid as of SCAS version: 17.3.0

Test Case: TC-Xn-handover_bid_down_gNB

Test Purpose: Verify that bidding down is prevented in Xn-handovers.

Pre-Conditions:

Test environment with source gNB and target gNB, and the source gNB may be simulated.

Execution Steps:

The target gNB sends the path-switch messages to the AMF.

Expected Results:

The UE ~~NR~~5G security capabilities and the UP security policy with corresponding PDU session ID as received from the source gNB are in the path-switch message.

Expected Format of Evidence:

Snapshots containing the result

2.3.3 TS 33.515 (SMF)

2.3.3.1 Refinement ID R_33.515_4.2.2.1.3

Section 4.2.2.1.3 Security functional requirements on the SMF checking UP security policy

Valid as of SCAS version: 16.4.0

Requirement Name: UP security policy check.

Requirement Reference: TS 33.501 [8], clause 6.6.1

Requirement Description: According to TS 33.501 [8], clause 6.6.1,the SMF verifies that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF sends its locally stored UE's UP security policy of the corresponding PDU sessions to the target gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF logs capabilities for this event and may take additional measures, such as raising an alarm.

Threat References: TR 33.926 [4], clause J.2.2.4, Unchecked UP security policy.

TEST CASE:

Test Name: TC_UP_SECURITY_POLICY _SMF

Purpose:

Verify that the SMF checks the UP security policy that is sent by the ng-eNB/gNB during handover.

Pre-Conditions:

The SMF under test is preconfigured with a UE UP security policy.

Execution

1. The tester sends the Nsmf_PDUSession_UpdateSMContext Request message to the SMF under test. A UE UP security policy different than the one preconfigured at the SMF under test is included in the Request message.

2. The tester captures the Nsmf_PDUSession_UpdateSMContext Response message sent from the SMF under test.

Expected Results:

The preconfigured UE security policy is contained in the 'n2SmInfo' IE in the captured Response message.

Expected format of evidence:

- Files containing the triggered HTTP messages (e.g. pcap trace).
- UE UP security policy configured in the SMF.

2.3.4 TS 33.517 (SEPP)

2.3.4.1 Refinement ID R_33.517_4.2.2.5

Section 4.2.2.5 Confidential IEs replacement handling in original N32-f message

Valid as of SCAS version: 16.4.0

Test Case:

Test Purpose Verify that the SEPP under test correctly replaces information elements requiring encryption with the value " encBlockIdx ".

Pre-Conditions:

- System documentation of the SEPP under test, which details how raw public keys/certificates of peer SEPPs are to be configured and how internal log files can be accessed.
- A second SEPP instance for N32 communication with the SEPP under test, which allows for the creation of custom N32-f messages. This system may be simulated.
- Both SEPPs are to be configured with a raw public key/certificate of their communication peer to be able to establish a N32-c connection.
- An arbitrary Data-type encryption policy which includes at least one information element requiring encryption on N32-f. The SEPP under test is to be configured with this policy.

Execution Steps

1. Both SEPPs establish a mutual N32-c connection.
2. Via the PLMN-internal interface, the tester provides the SEPP under test with a message to be forwarded to the peer SEPP on N32. This message needs to contain at least one information element that requires encryption according to the locally configured Data-type encryption policy.
3. The tester captures the related N32-f message after transformation by the SEPP under test.

Expected Results:

Information elements in the original message that require encryption according to the Data-type encryption policy are replaced with the value " encBlockIdx ".

Expected Format of Evidence:

- Evidence suitable for the interface, e.g. text representation of the captured N32-f message.
- Configured data-type encryption policy of SEPP
- Initial N32-f message before encryption

2.3.5 TS 33.519 (NEF)

2.3.5.1 Refinement ID R_33.519_4.2.2.1.1

Section 4.2.2.1.1 Authentication on application function

Valid as of SCAS version: 16.2.0

Test Case:

Test Purpose To verify that the NEF can authenticate application function and establish TLS connection towards the application server with certificate based authentication, and may authenticate application function and establish TLS connection towards the application server with pre-shared key based authentication.

Test Name: TC_CP_AUTH_AF_NEF

Pre-Condition:

- The NEF network product shall be connected in emulated/real network environments.
- In order to establish TLS connections to the NEF network product, the application function shall offer a feature that is supported by the NEF network product, including protocol version and combination of cryptographic algorithms.
- The application function and the NEF network product shall support certificate based authentication, and may support pre-shared key based authentication.
- If the NEF network product does not support CAPIF as specified in clause 6.2.5.1 in TS 23.501 [3], the certificates or the pre-shared key shall be provisioned in the NEF network product.
- If the NEF network product supports CAPIF, the certificates or the pre-shared key shall be provisioned in the CAPIF core function, the CAPIF core function shall be able to select appropriate authentication method as defined in the sub-clause 6.5.2 in TS 33.122 [4].

Execution Steps:

1. If certificate based authentication is used, provision correct certificate on the application function, if pre-shared key based authentication is used, provision same pre-shared key on the application function.
2. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether a TLS connection is established successfully.
3. If certificate based authentication is used, provision incorrect certificate on the application function, if pre-shared key based authentication is used, provision different pre-shared key on the application function.
4. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether no new TLS connection is established.

Note: All supported TLS authentication methods shall be tested.

Expected Results:

Only one TLS connection is established at step 2.

Expected Format of Evidence:

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

2.3.6 TS 33.521 (NWDAF)

2.3.6.1 Refinement ID R_33.521_4.2.1.2.6

Section 4.2.1.2.6 Protecting data and information – Data masking on integration analysis

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose Verify that no privacy information of operators' users is revealed to the party who is not allowed to have.

Test Name:

Pre-Condition:

The vendor shall provide the documentation describing how to create an account for accessing the analytics results.

Privacy information list (should be specified based on local policy, regulation and others).

Execution Steps:

1. Review the documentation provided by the vendor describing how to create the account for accessing the analytics results provided by the NWDAF.
2. The tester creates the account, and retrieves the analytics results from the NWDAF using the account.

Expected Results:

The tester can create the account, and the ~~account does~~ analytics results do not reveal subscriber permanent identifier~~.~~ Nor any other data listed in privacy information list.

Expected Format of Evidence:

Evidence suitable for the interface, e.g. screenshot containing the results.

2.3.7 TS 33.326 (NSSAAF)

2.3.7.1 Refinement ID R_33.326_4.2.2

Section 4.2.2 AAA-S authorization in re-authentication and revocation scenarios

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose Verify that the AAA-S is authorized to send the re-authentication or revocation.

Test Name: TC_NSSAAF_AAAS_AUTHORIZATION_REAUTH_REVOCATION

Pre-Conditions:

- The tester shall prepare two configurations of the mapping table for a positive case (AAA-S matches the S-NSSAI) and negative case (AAA-S does not match the S-NSSAI)
- Test environment with AAA-S and AAA-P, which may be simulated. The NSAAF under test is connected with AAA-S ~~and AAA-P~~.
  - A document describes the mapping between S-NSSAI and AAA-S server.

Execution Steps

1. The tester shall send the re-authentication and revocation message for a poitive case (AAA-S matches the S-NSSAI) and a negative case (AAA-S does not match the S-NSSAI)

2. The AAA-S sends Re-authentication or revocation message to the NSSAAF including the S-NSSAI and the GPSI.
3. The NSSAAF checks whether the AAA-S can be matched against with the S-NSSAI based on the mapping table.

Expected Results:

The NSSAAF rejects the re-authentication or revocation (negative case) or pass the re-authentication or revocation (positive case).

Expected Format of Evidence:

– Save the logs and the communication flow in a .pcap file.

2.3.8 TS 33.116 (MME)

2.3.8.1 Refinement ID R_33.116_4.2.2.2.1

Section 4.2.2.2.1 Access with 2G SIM forbidden

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that access to EPS with a 2G SIM is not possible

Test Name:

Pre-Condition: Test environment with HSS. HSS may be simulated

Execution Steps

During authentication procedure, ~~Include~~ include 2G authentication vector in authentication data response from HSS.

Expected Results:

MME rejects UE authentication when receiving 2G authentication vector from HSS.

NOTE: When both MME and HSS function correctly 2G authentication vector are never included in authentication data response from HSS to MME.

Expected Format of Evidence:

– *.pcap files of communication flow while authentication attempt and rejection of UE

2.3.8.2 Refinement ID R_33.116_4.2.2.2.2

Section 4.2.2.2.2 Re-synchronization

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that Re-synchronization procedure works correctly

Test Name:

Pre-Condition: Test environment with UE and HSS. UE and HSS may be simulated.

Execution Steps: The MME receives an AUTHENTICATION FAILURE message, with the EMM cause #21 "synch failure" and a re synchronization token AUTS.

Expected Results: The MME includes the stored RAND and the received AUTS in the authentication data request to the HSS.

Expected Format of Evidence:

- *.pcap files of communication flow between UE, MME and HSS

NOTE: When RAND and AUTS are not included in the authentication data request to the HSS then the HSS will return a new authentication vector (AV) based on its current value of the sequence number SQNHE (cf. TS 33.102, clause 6.3.5) A new authentication procedure between MME and UE using this new AV will be successful just the same if the cause of the synchronisation failure was the sending of a "stale" challenge, i.e. one that the UE had seen before or deemed to be too old. But if the cause of the synchronisation failure was a problem with the sequence number SQNHE in the HSS (which should be very rare), and the RAND and AUTS are not included in the authentication data request to the HSS, then an update of SQNHE based on AUTS will not occur in the HSS, and the new authentication procedure between MME and UE using the new AV will fail again. This can be considered a security-relevant failure case as it may lead to a subscriber being shut out from the system permanently.

2.3.8.3 Refinement ID R_33.116_4.2.2.2.3

Section 4.2.2.2.3 Integrity check of Attach message

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that secure user identification by means of integrity check of Attach request works correctly.

Test Name:

Pre-Condition: Test environment with new and old MME. New MME may be simulated.

Execution Steps: The old MME receives an Identification Request message from the new MME with incorrect integrity protection.

Expected Results: The old MME sends a response indicating that the user identity cannot be retrieved.

Expected Format of Evidence:

- *.pcap files of communication flow between old and new MME

2.3.8.4 Refinement ID R_33.116_4.2.2.2.4

Section 4.2.2.2.4 Not forwarding EPS authentication data to SGSN

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that EPS authentication data remains in the EPC.

Test Name:

Pre-Condition: Test environment with MME and SGSN. SGSN may be simulated.

Execution Steps: The MME receives an Identification Request message from the SGSN.

Expected Results: The response to the SGSN does not include EPS authentication data.

Expected Format of Evidence:

- *.pcap files of communication flow between MME and SGSN

2.3.8.5 Refinement ID R_33.116_4.2.2.2.5

Section 4.2.2.2.5 Not forwarding unused EPS authentication data between different security domains

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that unused EPS authentication data remains in the same serving domain.

Test Name:

Pre-Condition: Test environment with old and new MME in different serving domains. New MME may be simulated.

Execution Steps: The old MME receives an Identification Request message from the new MME.

Expected Results: The response to the new MME does not include unused EPS authentication data.

Expected Format of Evidence:

- *.pcap files of communication flow between old and new MME

2.3.8.6 Refinement ID R_33.116_4.2.2.3.1

Section 4.2.2.3.1 Bidding down prevention

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that bidding down by eliminating certain UE capabilities on the interface from UE to MME is not possible.

Test Name:

Pre-Condition: Test environment with UE. UE may be simulated.

Execution Steps: Attach request message includes security capabilities of the UE.

Expected Results: MME includes the same security capabilities of the UE in the SECURITY MODE COMMAND message.

Expected Format of Evidence:

- *.pcap files of communication flow between UE and MME

2.3.8.7 Refinement ID R_33.116_4.2.2.3.2

Section 4.2.2.3.2 NAS integrity algorithm selection and use

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that NAS integrity protection algorithm is selected and applied correctly.

Test Name:

Pre-Condition: Test environment with UE. UE may be simulated.

Execution Steps: The MME sends the SECURITY MODE COMMAND message. The UE replies with the SECURITY MODE COMPLETE message.

Expected Results:

1. The MME has selected the integrity algorithm which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities. The MME checks the message authentication code on the SECURITY MODE COMPLETE message.
2. The MAC in the SECURITY MODE COMPLETE is verified, and the NAS integrity protection algorithm is selected and applied correctly.

Expected Format of Evidence:

- *.pcap of communication flow between UE and MME
- part of MME configuration showing ordered list of integrity protection algorithms

2.3.8.8 Refinement ID R_33.116_4.2.2.3.3

Section 4.2.2.3.3 NAS NULL integrity protection

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that NAS NULL integrity protection algorithm is used correctly.

Test Name:

Pre-Condition: Test environment with UE. UE may be simulated.

Execution Steps: The MME sends the SECURITY MODE COMMAND message after successful UE authentication.

Expected Results: The selected integrity algorithm is different from EIA0.

Expected Format of Evidence:

- *.pcap files of communication flow between UE and MME

2.3.8.9 Refinement ID R_33.116_4.2.2.3.4

Section 4.2.2.3.4 NAS confidentiality protection

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that NAS confidentiality protection algorithm is applied correctly.

Test Name:

Pre-Condition:

- Test environment with UE. UE may be simulated.
- UE and MME are configured such that MME selects an confidentiality protection algorithm other than EEA0 in SECURITY MODE COMMAND message.

Execution Steps: The MME receives the SECURITY MODE COMPLETE message without confidentiality protection.

Expected Results: ~~If a confidentiality algorithm different from EEA0 was selected t~~The MME rejects the message by sending a NAS SECURITY MODE REJECT message.

Expected Format of Evidence:

- *.pcap files of communication flow between UE and MME

2.3.8.10 Refinement ID R_33.116_4.2.2.4.1

Section 4.2.2.4.1 Bidding down prevention in X2-handovers

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that bidding down is prevented in X2-handovers.

Test Name:

Pre-Condition: Test environment with (target) eNB. eNB may be simulated.

The MME is configured to log the event of a UE EPS security capability mismatch.

Execution Steps: The MME receives the path-switch message with the UE EPS security capabilities different from the ones stored in the MME for that UE.

Expected Results: The MME identifies the UE security capabilities mismatch and logs the event.

Expected Format of Evidence:

- *.pcap files of communication flow between target eNB and MME
- UE security capabilities stored in MME
- part of MME logs showing mismatch detection

2.3.8.11 Refinement ID R_33.116_4.2.2.4.2

Section 4.2.2.4.2 NAS integrity protection algorithm selection in MME change

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that NAS integrity protection algorithm is selected correctly.

Test Name:

Pre-Condition:

- Test environment with source and target MME. Source MME may be simulated.
- Source and target MME have different configurations of ordered lists of NAS algorithms

Execution Steps: The target MME receives the UE EPS security capabilities and the NAS algorithms used by the source MME from the source MME over the S10 interface. The target MME selects the NAS algorithms which have the highest priority according to the ordered lists and is present in the UE security capabilities. ~~The lists are assumed such that the algorithms selected by the target MME are different from the ones received from the source MME.~~

Expected Results: The target MME initiates a NAS security mode command procedure and include the chosen algorithms and the UE security capabilities.

Expected Format of Evidence:

- *.pcap files of communication flow between target MME and source MME
- UE security capabilities
- Ordered lists of NAS algorithms at target and source MME

2.3.8.12 Refinement ID R_33.116_4.2.2.5.1

Section 4.2.2.5.1 No access with 2G SIM via idle mode mobility

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that 2G subscribers cannot obtain service in EPS via idle mode mobility.

Test Name:

Pre-Condition: Test environment with source SGSN and target MME. Source SGSN may be simulated.

Execution Steps: The target MME receives the MM context in the Context Response indicating GSM security mode

Expected Results: The MME aborts the procedure by acknowledging the Context Response from the SGSN with an appropriate failure cause.

Expected Format of Evidence:

- *.pcap files of communication flow between MME and SGSN

2.3.8.13 Refinement ID R_33.116_4.2.2.5.2

Section 4.2.2.5.2 No access with 2G SIM via handover

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that GSM subscribers cannot obtain service in EPS via handovers.

Test Name:

Pre-Condition: Test environment with source SGSN and target MME. Source SGSN may be simulated.

Execution Steps: The target MME receives the MM context in the Forward Rel~~L~~ocation Request message indicating GSM security mode.

Expected Results: The MME aborts the procedure by responding to the Forward Relocation Request from the SGSN with an appropriate failure cause.

Expected Format of Evidence:

- *.pcap files of communication flow between MME and SGSN

2.3.8.14 Refinement ID R_33.116_4.2.2.5.3

Section 4.2.2.5.3 No access with 2G SIM via SRVCC

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Verify that GSM subscribers cannot obtain service in EPS via SRVCC into E-UTRAN.

Test Name:

Pre-Condition: Test environment with source MSC server and target MME. Source MSC server may be simulated.

Execution Steps: The target MME receives the GPRS Kc' and the CKSN'PS in the CS to PS handover request.

Expected Results: The MME rejects the request.

Expected Format of Evidence:

- *.pcap files of communication flow between MME and MSC server

2.3.8.15 Refinement ID R_33.116_4.2.2.6.1

Section 4.2.2.6.1 Authentication failure for emergency bearers

Valid as of SCAS version: 17.0.0

Test Case:

Test Purpose: Ensure that the MME enforces that only emergency bearers can be used without successful authentication.

Test Name:

Pre-Condition: Test environment with MME and UE. UE may be simulated. The serving network policy allows unauthenticated IMS Emergency Sessions.

Execution Steps: The UE sends the initial attach request for EPS emergency bearer services, then the MME initiates an authentication, which fails. The UE attached for EPS emergency bearer services sends the PDN Connectivity request for EPS non-emergency bearer services.

Expected Results: The MME allows to continue the setup of the emergency bearer, and will reject the PDN Connectivity request for EPS non-emergency bearer services.

Expected Format of Evidence:

- *.pcap files of communication flow between MME and UE

2.3.9 TS 33.216 (eNB)

2.3.9.1 Refinement ID R_33.216_4.2.2.1.3

Section 4.2.2.1.3 User plane data ciphering and deciphering at the eNB

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: To verify that the user data packets are confidentiality protected over the air interface.

Test Name: TC-DATA-CIP-eNB-Uu

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and the MME may be simulated,
- The tester can capture the messages via the air interface.
- The tester shall enable the user plane ciphering protection and ensure EEA0 is not used.

Execution Steps:

1. The UE sends an attach request to the MME.
2. The MME sends a KeNB and the UE security capability to the eNB.
3. eNB selects an algorithm and sends AS SMC to the UE,
4. eNB receive AS SMP from the UE.

Expected Results:

User plane packets sent by the eNB after eNB sending AS SMC is ciphered.

Expected Format of Evidence:

- Evidence suitable for the interface e.g. Screenshot containing the operational results.
- Log files of eNB (test step 3 and 4)
- PCAP files of communication flow between eNB and UE
- List of algorithms configured in eNB
- Selected algorithm

2.3.9.2 Refinement ID R_33.216_4.2.2.1.5

Section 4.2.2.1.5 AS algorithms selection

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: Verify that the eNB selects the algorithms with the highest priority in its configured list.

Test Name:

Pre-Condition: Test environment with the eNB has been pre-configured with allowed security algorithms with priority.

Execution Steps:

1. The UE sends attach request message to the eNB.
2. The eNB receives S1 context setup request message.
3. The eNB sends the SECURITY MODE COMMAND message.
4. The UE replies with the AS SECURITY MODE COMPLETE message.

Expected Results:

1. The eNB initiates the SECURITY MODE COMMAND message that includes the chosen algorithm with the highest priority according to the ordered lists and is contained in the UE EPS security capabilities.
2. The MAC in the AS SECURITY MODE COMPLETE message is verified, and the AS protection algorithms are selected and applied correctly.

Expected Format of Evidence:

- Sample copies of the log files.
- PCAP files
- Ordered list of security algorithms

2.3.9.3 Refinement ID R_33.216_4.2.2.1.6

Section 4.2.2.1.6 Verify RRC integrity protection

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: Verify that the message is discarded in case of failed integrity check (i.e. faulty or missing MAC-I).

Test Name:

Pre-Condition: Test environment with RRC Protection is activated at the eNB.

Execution Steps:

Positive:

1. The eNB receives a RRC message with a right MAC-I.

Negative:

1. The eNB receives a RRC message with a wrong MAC-I ~~or~~
2. The eNB receives a RRC message with a missing MAC-I.

Expected Results: The RRC message is discarded in the negative test.

Expected Format of Evidence:

- Sample copies of the log files.

- PCAP files

2.3.9.4 Refinement ID R_33.216_4.2.2.1.7

Section 4.2.2.1.7 The selection of EIA0

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: Verify that AS NULL integrity algorithm is used correctly.

Test Name:

Pre-Condition:

Test environment with a UE . The UE may be simulated.

The vendor shall provide documentation describing how EIA0 is disabled or enabled.

Execution Steps:

Positive:

1. ~~The eNB receives a UE security capability only containing EIA0 from S1 context setup message~~. The UE initiates an emergency registration.
2. The eNB sends AS SMC to the UE.

Negative:

1. The UE initiates a non-emergency registration. ~~The eNB receives a UE security capability that contains EIA0 and other integrity algorithm(s).~~
2. The eNB sends AS SMC to the UE.

Expected Results: EIA0 is only selected in the Positive test.

Expected Format of Evidence:

- Sample copies of the log files.
- List of algorithms configured in eNB and UE

2.3.9.5 Refinement ID R_33.216_4.2.2.1.8

Section 4.2.2.1.8 Key refresh at the eNB

Valid as of SCAS version: 16.7.0

Test Case: 1

Test Purpose: Verify that the eNB performs KeNB refresh when PDCP COUNTs are about to wrap around.

Test Name: TC_ENB_KEY_REFRESH_ PDCP_COUNT

Pre-Condition: The UE may be simulated.

Execution Steps:

1. The eNB sends AS Security Mode Command message to the UE, and the UE responds with the AS Security M~~S~~ode C~~M~~omplete message~~C~~.
2. The UE sends RRC messages or UP messages to the eNB with an increasing PDCP COUNT until the value wraps around.

Expected Results: The eNB triggers an intra-cell handover and takes a new KeNB into use.

Expected Format of Evidence:

- Part of log that shows the PDCP COUNT wraping around and the intra-cell handover. This part can be presented, for example as a screenshot.
- PCAP files

Test Case: 2

Test Purpose: Verify that the eNB performs KeNB refresh when DRB-IDs are about to be reused under the following conditions:

- the successive Radio Bearer establishment uses the same RB identity while the PDCP COUNT is reset to 0, or
- the PDCP COUNT is reset to 0 but the RB identity is increased after multiple calls and wraps around.

Test Name: TC_ENB_KEY_REFRESH_DRB_ID

Pre-Condition: The UE and MME may be simulated.

Execution Steps:

1. The eNB sends the AS Security Mode Command message to the UE.
2. The UE responds with the AS Security Mode Complete message.
3. A DRB is set up.
4. DRB is set up and torn down for multiple times within one active radio connection without the UE going to idle (e.g. by the UE making multiple IMS calls, or by the MME requesting bearer setup and bearer deactivation), until the DRB ID is reused.

Expected Results: Before DRB ID reuse, the eNB takes a new KeNB into use by e.g. triggering an intra-cell handover or triggering a transition from RRC_CONNECTED to RRC_IDLE or RRC_INACTIVE and then back to RRC_CONNECTED.

Expected Format of Evidence:

- Part of log that shows all the DRB identities and the intra-cell handover or the transition from RRC_CONNECTED to RRC_IDLE or RRC_INACTIVE and then back to RRC_CONNECTED. This part can be presented, for example, as a screenshot.
- PCAP files

2.3.9.6 Refinement ID R_33.216_4.2.2.1.9

Section 4.2.2.1.9 AS Security Mode Command Procedure

Valid as of SCAS version: 16.7.0

Test Case:

Requirement Reference: TS 33.401 [3], clause ~~7.4.2~~ 7.2.4.5

Test Purpose: Verify that AS integrity protection algorithm is selected and applied correctly.

Test Name:

Pre-Condition: Test environment with UE. UE may be simulated.

Execution Steps: The eNB sends the SECURITY MODE COMMAND message. The UE replies with the SECURITY MODE COMPLETE message.

Expected Results:

1. The eNB has selected the integrity algorithm which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities. The eNB checks the message authentication code on the SECURITY MODE COMPLETE message.
2. The MAC in the SECURITY MODE COMPLETE is verified, and the AS integrity protection algorithm is selected and applied correctly.

Expected Format of Evidence:

- Snapshots containing the result.
- Ordered list of integrity protection algorithms configured in eNB
- Log files
- PCAP files

2.3.9.7 Refinement ID R_33.216_4.2.2.1.10

Section 4.2.2.1.10 Bidding down prevention in X2-handovers

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: Verify that bidding down is prevented in X2-handovers.

Test Name:

Pre-Condition: Test environment with source eNB and target eNB, and the source eNB may be simulated.

Execution Steps: The target eNB sends the path-switch message to the MME.

Expected Results: The UE EPS security capabilities received from the source eNB are in the path-switch message.

Expected Format of Evidence:

- Snapshots containing the result
- PCAP files
- Log files

2.3.9.8 Refinement ID R_33.216_4.2.2.1.11

Section 4.2.2.1.11 AS protection algorithm selection in eNB change

Valid as of SCAS version: 16.7.0

Test Purpose: Verify that AS protection algorithm is selected correctly.

Test Name:

Pre-Condition: Test environment with source eNB, target eNB and MME. Source eNB and MME may be simulated. Source and target eNB are configured with different ordered lists of security algorithms.

Execution Steps:

Test Case 1:

Source eNB transfers the ciphering and integrity algorithms used in the source cell to the target eNB in the handover request message.

~~Target eNB verifies the algorithms and selects AS algorithms which have the highest priority according to the ordered lists. Target eNB includes the algorithm in the handover command.~~

Test Case 2:

MME sends the UE EPS security capability to the Target eNB.

~~The target eNB selects the AS algorithms which have the highest priority according to the ordered lists in the HANDOVER COMMAND.~~

~~The above test cases assume that the algorithms selected by the target eNB are different from the ones received from the source eNB.~~

Expected Results:

~~1.~~ The AS protection algorithms are selected according to the ordered list of security algorithms in the target eNB and UE EPS security capabilities. ~~The UE checks the message authentication code on the handover command message.~~

2. The selected algorithms are included in the HANDOVER COMMAND. ~~The MAC in the handover complete message is verified, and the AS integrity protection algorithm is selected and applied correctly.~~

Expected Format of Evidence:

- Snapshots containing the result.
- PCAP files for both test cases
- Ordered list of security algorithms (source and target eNB)
- UE EPS security capabilities

2.3.9.9 Refinement ID R_33.216_4.2.2.1.12

Section 4.2.2.1.12 RRC and UP downlink ciphering at the eNB

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: To verify that the eNB performs RRC and UP downlink ciphering after sending the AS security mode command message.

Test Name: TC_eNB_DL_Cipher

Pre-Condition:

- The UE and eNB network products are connected in the test environment. UE may be simulated.
- The tester shall have access to the AS security context and the corresponding cryptographic keys (e.g. RRC and UP cipher keys).
- The eNB is configured to use ciphering algorithms different from NULL ciphering algorithm.
- The tester has access to Uu interface and ability to capture the Uu interface messages with the debug port enabled in the UE.

Execution Steps:

1. ~~The tester shall POWER ON the UE to trigger the registration procedures (Attach and SMC).~~ The tester performs packet capturing over the Uu interface using any packet analyser.
2. ~~The tester performs packet capturing over the Uu interface using any packet analyser.~~ The tester shall POWER ON the UE to trigger the registration procedures (Attach and SMC).
3. The tester filters the AS SMC command message and the following RRC and UP downlink packets from eNB to UE.

4. The tester proceeds the testing based on the parameters (algorithm identifier and algorithm distinguisher) present in the AS SMC command message. The tester verifies that the downlink packets filtered in step 3 are ciphered.

~~5. Case 1: If the parameters refer to null ciphering algorithm, the tester verifies that the downlink packets filtered in step 3 are unciphered.~~

~~6. Case 2: If the parameters refer to algorithms such as SNOW, AES, ZUC, the tester verifies that the downlink packets filtered in step 3 are ciphered.~~

The tester also checks if the packets are ciphered in accordance with the selected algorithm stated in the AS SMC command message.

NOTE: The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

Expected Results:

The downlink packets following the AS SMC command message are ciphered. ~~except NULL ciphering algorithm case.~~

Expected Format of Evidence:

- Evidence suitable for the interface, e.g. Screenshot contains the operation results.
- PCAP files

2.3.9.10 Refinement ID R_33.216_4.2.2.1.13

Section 4.2.2.1.13 Map a UE NR security capability

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: To verify that the eNB creates mapped UE NR security capabilities.

Test Name: TC_MAP_NR_SEC_CAP

Pre-Condition:

- The eNB and gNB network products are connected in the test environment. The gNB may be simulated.
- Tester shall have access to trigger dual connection to a gNB.
- The Tester shall have access to the X2 interface.

Execution Steps:

1. The MeNB does not receive UE NR security capabilities from S1 Initial Context Setup Request message.
2. The MeNB sends SN Addition Request Message to the SgNB.
3. The tester checkes if the NR security capabilities are included in SN Addition Request Message.

Expected Results: The SN Addition Request Message contains UE NR security capabilities, i.e. NEA0, 128-NEA1, 128-NEA2, 128-NEA3, NIA0, 128-NIA1, 128-NIA2, 128-NIA3

Expected Format of Evidence:

- Evidence suitable for the interface, e.g. Screenshot contains the operation results.
- PCAP files

2.3.9.11 Refinement ID R_33.216_4.2.2.1.14

Section 4.2.2.1.14 UE NR security capability is only sent to a SgNB

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: To verify that the UE NR security capabilities are only sent to a SgNB.

Test Name: TC_NR_SEC_CAP_SENT

Pre-Condition:

- The UE, gNB and eNB network products are connected in the test environment. UE and gNB may be simulated.
- The tester shall have access to the X2 interface.

Execution Steps:

1. The tester triggers MeNB to send SN addition Request message to a SgNB.
2. The tester triggers UE HO from MeNB to another eNB.
3. The tester checks if the UE NR security capabilities were sent in the X2 interface in both step 1 and step 2.

Expected Results: The UE NR security capabilities are only sent to the SgNB in test step 1.

Expected Format of Evidence:

- Evidence suitable for the interface, e.g. Screenshot contains the operation results.
- PCAP files

2.3.9.12 Refinement ID R_33.216_4.2.2.1.15

Section 4.2.2.1.15: Bidding down prevention in X2-handovers when target eNB receives a UE NR security capability

Valid as of SCAS version: 16.7.0

Test Case:

Test Purpose: Verify that bidding down is prevented in X2-handovers when target eNB receives a UE NR security capability.

Test Name: TC_BID_DOWN_X2

Pre-Condition: Test environment with source eNB and target eNB, and the source eNB may be simulated.

Execution Steps: The target eNB sends the S1-PATH SWITCH-REQUEST message~~path-switch message~~ to the MME.

Expected Results:

The received UE NR security capability is in the S1-PATH SWITCH-REQUEST ~~path-switch~~ message.

Expected Format of Evidence:

- Snapshots containing the result.
- PCAP files

2.3.9.13 Refinement ID R_33.216_4.2.2.1.16

Section 4.2.2.1.16: Integrity protection of user data between the UE and the eNB

Valid as of SCAS version: 18.0.0

Test Name: TC-UP-DATA-INT_eNB

Purpose: To verify that the user data packets are integrity protected over the Uu interface.

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE may be simulated.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.

Execution Steps:

1. The tester shall enable the user plane integrity protection and ensure that EIA0 is disabled at UE and eNB.
2. eNB sends RRCConnectionReconfiguration with integrity protection indication "on".
3. Check any User data sent by eNB after sending RRCConnectionReconfiguration and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is integrity protected.

Expected Format of Evidence:

- Evidence suitable for the interface e.g. Screenshot containing the operational results.

2.3.9.14 Refinement ID R_33.216_4.2.2.1.17

Section 4.2.2.1.17: Local UP integrity protection configuration

Valid as of SCAS version: 18.0.0

Test Name: TC_LOCAL_UP_INTEGRITY_PROTECTION_CONFIGURATION

Purpose: To verify that the eNB is locally configured with a UP integrity protection policy

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and MME may be simulated.
- The eNB is locally configured to activate UP integrity protection by default if no UP integrity protection policy is received from MME.
- EIA0 is disabled at UE and eNB.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.

Execution Steps:

4. MME sends EPS security capability with EIA7 indicating the UP integrity protection is supported by the UE. But the MME does not send a UP integrity protection policy to the eNB.
5. eNB sends RRCConnectionReconfiguration with integrity protection indication "on".
6. Check any User data sent by eNB after sending RRCConnectionReconfiguration and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is integrity protected according to the local configuration in the eNB.

Expected Format of Evidence:

- Evidence suitable for the interface e.g. Screenshot containing the operational results.
- Local configuration of UP integrity protection in the eNB

2.3.9.15 Refinement ID R_33.216_4.2.2.1.18

Section 4.2.2.1.18: UP IP policy selection

Valid as of SCAS version: 18.0.0

Test Name: TC_UP_IP_POLICY_Selection

Purpose: To verify that the ~~eNB has a locally configured~~ UP IP policy sent from MME is used by the eNB.

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and MME may be simulated.
- The eNB locally UP IP is set to NOT NEEDED.
- EIA0 is disabled at UE and eNB.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.

Execution Steps:

1. MME sends EPS security capability with EIA7 indicating the UP IP is supported by the UE. But the MME does sends a UP IP policy with REQUIRED to the eNB.
2. eNB sends RRCConnectionReconfiguration with integrity protection indication "on".
3. Check any User data sent by eNB after sending RRCConnectionReconfiguration and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is integrity protected according to the UP IP policy sent by MME.

Expected Format of Evidence:

- Evidence suitable for the interface e.g. Screenshot containing the operational results.
- UP integrity protection policy sent by MME

2.3.9.16 Refinement ID R_33.216_4.2.2.1.19

Section 4.2.2.1.19: UP IP policy selection in S1 Handover

Valid as of SCAS version: 18.0.0

Test Name: TC_UP_IP_POLICY_Selection_S1_Handover

Purpose: To verify that the eNB has correct selection on UP IP policy in S1 handover

Pre-Condition:

- The target eNB network product shall be connected in emulated/real network environments. UE, source eNB and MME may be simulated.
- ~~The target eNB locally UP IP is set to NOT NEEDED.~~
- EIA0 is disabled at UE and eNB.

- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.

Execution Steps:

Test Case 1:

1. The local UP IP configuration of the target eNB is set to NOT NEEDED.
2. MME sends EPS security capability with EIA7 indicating the UP IP is supported by the UE. And the MME sends a UP IP policy with REQUIRED to the target eNB.
3. Source eNB sends UP IP policy with NOT NEEDED in the source-to-target container to the target eNB.
4. The target eNB sends RRCConnectionReconfiguration with integrity protection indication "on".
5. Check any User data sent by the target eNB after sending RRCConnectionReconfiguration and before UE enters CM-Idle state is integrity protected.

Test Case 2:

1. The local UP IP configuration of the target eNB is set to NOT NEEDED.
2. MME sends EPS security capability with EIA7 indicating the UP IP is supported by the UE. And the MME does not send a UP IP policy to the target eNB.
3. Source eNB sends UP IP policy with REQUIRED in the source-to-target container to the target eNB.
4. The target eNB sends RRCConnectionReconfiguration with integrity protection indication "on".
5. Check any User data sent by the target eNB after sending RRCConnectionReconfiguration and before UE enters CM-Idle state is integrity protected.

Test Case 3:

1. The local UP IP configuration of the target eNB is set to REQUIRED.
2. MME sends EPS security capability with EIA7 indicating the UP IP is supported by the UE. And the MME does not send a UP IP policy to the target eNB.
3. Source eNB does not send UP IP policy in the source-to-target container to the target eNB.
4. The target eNB sends RRCConnectionReconfiguration with integrity protection indication "off".
5. Check any User data sent by the target eNB after sending RRCConnectionReconfiguration and before UE enters CM-Idle state is ~~not~~ integrity protected.

Expected Results:

For all test cases ~~1 and 2~~, any user plane packets sent between UE and the target eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is integrity protected.

~~For test case 3, any user plane packets sent between UE and eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is not integrity protected.~~

Expected Format of Evidence:

- Evidence suitable for the interface e.g. Screenshot containing the operational results.
- For each test case: Configuration of UP IP of target eNB, source eNB and UP IP policy sent by MME

2.3.9.17 Refinement ID R_33.216_4.2.2.1.20

Section 4.2.2.1.20: Bidding down prevention for UP IP Policy

Valid as of SCAS version: 18.0.0

Test Name:

Purpose: Verify that bidding down for UP IP policy is prevented in X2-handovers.

Pre-Condition:

- The target eNB network product shall be connected in emulated/real network environments. UE, source eNB and MME may be simulated.
- ~~The target eNB locally UP IP is set to NOT NEEDED.~~
- EIA0 is disabled at UE and eNB.

Execution Steps:

Test Case 1:

1. The local UP IP configuration of the target eNB is set to NOT NEEDED.
2. Source eNB sends EPS security capability with EIA7 indicating the UP IP is supported and UP IP policy with REQUIRED in Handover Request message to the target eNB.
3. The target eNB sends path-switch request message with UP IP policy with REQUIRED to the MME.

Test Case 2:

1. The local UP IP configuration of the target eNB is set to REQUIRED.
2. Source eNB sends EPS security capability with EIA7 indicating the UP IP is supported in Handover Request message to the target eNB. The source eNB does not send UP IP policy in the Handover Request message.
3. The target eNB sends path-switch request message with UP IP policy with ~~NOT NEEDED~~ REQUIRED to the MME.

Expected Results:

For test case 1 and 2, the UP IP policy with REQUIRED is in the path-switch request message.

~~For test case 2, the UP IP policy with NOT NEEDED is in the path-switch request message.~~

Expected Format of Evidence:

- Snapshots containing the result.
- For each test case: Configuration of UP IP of target eNB, source eNB and UP IP policy sent by MME

2.3.10 TS 33.226 (IMS)

2.3.10.1 Refinement ID R_33.226_4.2.2.2.1

Section 4.2.2.1.1: No de-registration during the authentication

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify the S-CSCF shall not de-register the registered UE when it fails an authentication during re-registration.

Test Name: TC_ NO_DE-REGISTRATION_AUTH_FAIL

Pre-Condition:

- S-CSCF under test is connected in simulated/real network environment including P-CSCF and HSS.

- The UE supporting IMS AKA has already been registered into the IMS network.
- The tester shall have access to the Mw interface between the P-CSCF and S-CSCF.
- The tester shall have access to the Cx interface between the HSS and S-CSCF.

Execution Steps:

1. During a new IMS AKA procedure, the UE initiates the re-registration scenario, the tester sends a SM7 register message including the IMPI, and an incorrect authentication response.
2. The S-CSCF under test retrieves the active XRES for that user and uses this to check the received authentication response

Expected Results:

The S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed.

The S-CSCF does not initiate de-registration procedure within the Registration expiration interval defined in TS 24.229 [6], i.e. send either Cx-Put (Public User Identity, Private User Identity, clear S CSCF name) or Cx-Put (Public User Identity, Private User Identity, keep S CSCF name) to the HSS. Or, the IMPU status in the HSS is registered within the Registration expiration interval defined in TS 24.229 [6].

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~

Save the logs and the communication flow in a .pcap file.

2.3.10.2 Refinement ID R_33.226_4.2.2.2.2

Section 4.2.2.2.2 Unprotected register message

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify whether the S CSCF authenticates the user by means of the AKA protocol, if the UE sends unprotected REGISTER messages, regardless whether the UE is already registered or not.

Test Name: TC_UNPROTECTED_REGISTER_MESSAGE

Pre-Condition:

- S-CSCF network product are connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF ~~under test~~.
- The UE and the P-CSCF are simulated.
- The UE supports a list of ordered integrity and encryption algorithms.
- The tester has access to the Gm interface between the UE and P-CSCF.
- The tester has access to the Mw interface between the P-CSCF and S-CSCF.
- The UE has an already active pair of security associations.

Execution Steps:

This test is performed in the Authenticated re-registration procedure, the UE has an already active pair of security associations.

1. The UE sends unprotected REGISTER messages (SM1) to the P-CSCF.
2. The P-CSCF sends unprotected REGISTER messages (SM2) to the S-CSCF under test.
3. The S-CSCF under test receives the SM2 from the P-CSCF.

4. The tester examines whether the S-CSCF under test sends SM4: Auth_Challenge to the P-CSCF to authenticate the user by means of the AKA protocol.

Expected Results:

The S-CSCF under test authenticates the user by means of the AKA protocol after receiving an unprotected REGISTER message.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.3 Refinement ID R_33.226_4.2.2.3.1

Section 4.2.2.3.1 High-priority algorithm selection

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify the P CSCF selects the highest priority algorithm combination on its own list which is also supported by the UE.

Test Name: TC_HIGH_PRIORITY_ALGORITHM_SELECTION

Pre-Condition:

- P-CSCF under test is connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF under test by the tester.
- The UE supporting IMS AKA may be simulated.
- The UE supports a list of integrity and encryption algorithms.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps:

This test is performed in the registration procedure, the UE sends a Register message towards the S CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

1. The UE sends SM1 with integrity and encryption algorithms list to the P-CSCF under test.
2. The P-CSCF under test receives the SM1 with integrity and encryption algorithms list. The P-CSCF under test selects algorithms.
3. The tester examines the selected algorithm combination in the SM6 sent from the P-CSCF under test to the UE via the Gm interface.

Expected Results: The selected algorithms are the first algorithm combination on its own list which is also supported by the UE.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file

2.3.10.4 Refinement ID R_33.226_4.2.2.3.2

Section 4.2.2.3.2 Bidding down on security association set-up

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose:

Verify the P CSCF checks whether the integrity and encryption algorithms list, SPI_P and Port_P received in SM7 is identical with the corresponding parameters sent in SM6.

Verify the P CSCF checks whether SPI_U and Port_U received in SM7 are identical with those received in SM1.

Verify whether the P CSCF abort the registration procedure, if the above checks are not successful.

Test Name: TC_BIDDING_DOWN_ON_SECURITY_ASSOCIATION_SET UP

Pre-Condition:

- The P-CSCF under test is connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF under test.
- The UE and the S-CSCF are simulated.
- The UE supports a list of ordered integrity and encryption algorithms. The list contains at least one encryption algorithm other than NULL algorithm.
- The tester has access to the Gm interface between the UE and P-CSCF.
- The tester has access to the Mw interface between the P-CSCF and S-CSCF.

Execution Steps:

This test is performed in the registration procedure, the UE sends a Register message towards the S CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

Test cases 1-4 are performed as follows:

1. The UE sends SM1 with the Security Parameter Index values (SPI_U) and the protected ports selected by the UE (Port_U) to the P-CSCF under test.
2. The P-CSCF under test receives the SM1 with the Security Parameter Index values *(SPI_U)* and the protected ports selected by the UE *(Port_U)*. The P-CSCF under test store the *SPI_U* and the *Port_U* received in the SM1.
3. The ~~P-CSCF under test~~ SM6 contains the *SPI_P*, the ports assigned by the P CSCF (Port_P) and a list of integrity and encryption algorithms supported by the P-CSCF under test. The P-CSCF under test sends SM6 to the UE.
4. The UE receives the SM6 from the P-CSCF under test.

Test case 1:

The UE contains the incorrect SPI_U and Port_U, which are different from SPI_U and Port_U sent in SM1, and SPI_P and Port_P received in SM6, and a list of integrity and encryption algorithms received in SM6 supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 2:

The UE contains the incorrect SPI_U and Port_U, which are different from SPI_U and Port_U sent in SM1, and incorrect SPI_P and Port_P, which are different from SPI_U and Port_U received in SM6, and a list of integrity and encryption algorithms received in SM6 supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 3:

The UE contains the SPI_U and Port_U sent in SM1, and incorrect SPI_P and Port_P, which are different from SPI_U and Port_U received in SM6, and a list of integrity and encryption algorithms supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 4:

The UE contains the SPI_U and Port_U sent in SM1, and SPI_P and Port_P received in SM6, and a list of integrity and encryption algorithms in the SM7 which are different from those sent by the P-CSCF under test in the SM6. The UE sends SM7 to the P-CSCF under test.

Expected Results:

For ~~text 2-5~~ test cases 1-4, the P-CSCF under test aborts the registration procedure, and sends a suitable 4xx response message to the UE.

Expected Format of Evidence: ~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.5 Refinement ID R_33.226_4.2.2.3.3

Section 4.2.2.3.3 Protection of IMS signalling in transfer

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify the IMS signalling protection mechanisms implemented in P-CSCF adherer to profiling given in clause 5.3.3 and 5.3.4 of TS 33.210 [5] with the addition that only algorithms that can be signalled according to Annex H of TS 33.203 [3] needs to be supported.

Test Name: TC_PROTECT_IMS_SIGNALLING_TRANSFER

Pre-Condition:

- P-CSCF network products are connected in simulated/real network environment.
- The UE supporting IMS AKA may be simulated.
- Tester shall have the knowledge of the security profiles for the IPSec ESP protection.
- Tester shall have the keys derived from the IMS AKA to negotiate the SA parameters required for IPSec ESP.

Execution Steps:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

Expected Results:

- The P-CSCF under test and the UE established ~~TLS~~ IPsec ESP if the ~~TLS~~ IPsec ESP profiles used by the UE are compliant with the profile requirements in TS 33.203[3] Annex H.
- The P-CSCF under test and the UE failed to establish ~~TLS~~ IPsec ESP if the ~~TLS~~ IPsec ESP profiles used by the UE are forbidden in TS 33.203 [3] Annex H.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.6 Refinement ID R_33.226_4.2.2.3.4

Section 4.2.2.3.4 Bidding down on security association set-up in case the P-CSCF policy requiring confidentiality

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify that the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network.

NOTE1: The test case below is optional, which only applies ~~to~~ if the P-CSCF policy requires confidentiality.

Test Name: TC_BIDDING_DOWN_ON_SECURITY_ASSOCIATION_SET UP

Pre-Condition:

- The P-CSCF policy requires confidentiality.
- The UE and the S-CSCF are simulated.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps:

This test is performed in the registration procedure, the UE sends a Register message towards the S CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

Test case 1:

1. The UE includes only UE integrity algorithms list in SM1 to the P-CSCF under test.
2. The P-CSCF under test receives SM1 ~~and sends SM2 to the S-CSCF.~~

Test case 2:

1. The UE includes UE integrity and encryption algorithms list in SM1 to the P-CSCF under test, where the encryption algorithms are NULL.
2. The P-CSCF under test receives SM1.

Expected Results: For both test cases, the P-CSCF sends a suitable error message to the UE.

NOTE 2: The suitable error message could be used to identify that the procedure is aborted.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~

Save the logs and the communication flow in a .pcap file.

2.3.10.7 Refinement ID R_33.226_4.2.2.3.5

Section 4.2.2.3.5 Different SPIs

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify the P-CSCF selects SPIs that are different than the SPIs sent by the UE.

Test Name: TC_DIFFERENT_SPIS

Pre-Condition:

- P-CSCF under test is connected in simulated/real network environment.
- The UE supporting IMS AKA may be simulated.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps:

This test is performed in the registration procedure, the UE sends a Register message towards the S CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

1. The UE sends SM1 with spi_uc (the SPI of the inbound SA at UE's the protected client port) and spi_us (the SPI of the inbound SA at the UE's protected server port) to the P-CSCF under test.
2. The P-CSCF under test receives the SM1 with spi_uc and spi_us. The P-CSCF under test selects spi_pc (the SPI of the inbound SA at the P CSCF's protected client port) and spi_ps (the SPI of the inbound SA at the P CSCF's protected server port).
3. The tester examines the spi_pc and spi_ps in the SM6 sent from the P-CSCF under test to the UE via the Gm interface.

Expected Results: The spi_pc and spi_ps are different than spi_uc and spi_us.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.8 Refinement ID R_33.226_4.2.2.4.1

Section 4.2.2.3.4 Encryption in network hiding

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose:

Verify the I-CSCF encrypts the hiding information elements when the I-CSCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the I-CSCF decrypts those information elements that were encrypted by the I-CSCF in this hiding network domain when the I-CSCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Test Name: TC_ENCRYPTION IN NETWORK HIDING

Pre-Condition:

- I-CSCF network products are connected in simulated/real network environment.
- The network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The same encryption and decryption key Kv is configured on the I-CSCFs under test by the tester.
- The encryption algorithm is configured on the I-CSCF under test by the tester.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and I-CSCF.
- The tester has access to the interface between the element outside the hiding network's domain and I-CSCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the encryption of the hiding information elements in the I-CSCF are implemented.

Test case 1: The I-CSCF forwards SIP messages to the outside of the hiding network's domain

1. The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the I-CSCF under test.
2. The I-CSCF under test forwards the SIP message to the network element outside the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The I-CSCF forwards SIP messages to the hiding network's domain

1. The network element outside the hiding network's domain sends a SIP message which contains information elements that were encrypted by the I-CSCF in this hiding network domain to the I-CSCF under test.
2. The I-CSCF under test forwards the SIP message to the network element in the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the I-CSCF under test encrypts the hiding information elements when the I-CSCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the I-CSCF under test decrypts those information elements that were encrypted by the I-CSCF in this hiding network domain when the I-CSCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.9 Refinement ID R_33.226_4.2.2.5.1

Section 4.2.2.5.1 Encryption in network hiding

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose:

Verify the IBCF encrypts the hiding information elements when the IBCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the IBCF decrypts those information elements that were encrypted by the IBCF in this hiding network domain when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Test Name: TC_ENCRYPTION IN NETWORK HIDING

Pre-Condition:

- IBCF network products are connected in simulated/real network environment.
- The encryption of the hiding information as the network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The same encryption and decryption key Kv is configured on the IBCFs under test by the tester.

- The encryption algorithm is configured on the IBCF under test by the tester.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and IBCF.
- The tester has access to the interface between the element outside the hiding network's domain and IBCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the encryption of the hiding information elements in the IBCF are implemented.

Test case 1: The IBCF forwards SIP messages to the outside of the hiding network's domain

1. The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the IBCF under test.
2. The IBCF under test forwards the SIP message to the network element outside the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The IBCF forwards SIP messages to the hiding network's domain

1. The network element outside the hiding network's domain sends a SIP message which contains information elements that were encrypted by the IBCF in this hiding network domain to the IBCF under test.
2. The IBCF under test forwards the SIP message to the network element in the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the IBCF under test encrypts the hiding information elements when the IBCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the IBCF under test decrypts those information elements that were encrypted by the IBCF in this hiding network domain when the IBCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.10 Refinement ID R_33.226_4.2.2.5.2

Section 4.2.2.5.2 Replacement in network hiding

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose:

Verify the IBCF replaces the hiding information elements to constant values when the IBCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the IBCF replaces the constant values that were replaced by the IBCF in this hiding network domain to the hiding information elements when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Test Name: TC_REPLACEMENT IN NETWORK HIDING

Pre-Condition:

- IBCF network products are connected in simulated/real network environment.
- The replacement of the hiding information as network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and IBCF.
- The tester has access to the interface between the element outside the hiding network's domain and IBCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the replacement of the hiding information elements in the IBCF are implemented.

Test case 1: The IBCF forwards SIP messages to the outside of the hiding network's domain

1. The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the IBCF under test.
2. The IBCF under test forwards the SIP message to the network element outside the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The IBCF forwards SIP messages to the hiding network's domain

1. The network element outside the hiding network's domain sends a SIP message which contains information elements that were ~~encrypted~~ replaced by the IBCF in this hiding network domain to the IBCF under test.
2. The IBCF under test forwards the SIP message to the network element in the hiding network's domain.
3. The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the IBCF under test replaces the hiding information elements to constant values when the IBCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the IBCF under test replaces the constant values that were replaced by the IBCF in this hiding network domain to the hiding information elements when the IBCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~ Save the logs and the communication flow in a .pcap file.

2.3.10.11 Refinement ID R_33.226_4.2.2.6.1

Section 4.2.2.6.1 User authorization

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify that the AS would reject the anonymous request if anonymous request is not allowed.

Test Name: TC_USER_AUTHORIZATION

Pre-Condition:

- The authorization policy of the AS does not allow anonymous request.
- The UE is simulated.
- The tester has access to the interface between the UE and AS.

Execution Steps:

The UE sends the anonymous request message towards the AS, in which the P-Asserted-Identity is set to "Anonymous".

Expected Results:

For test case, the AS either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~

Save the logs and the communication flow in a .pcap file.

2.3.10.12 Refinement ID R_33.226_4.2.2.6.2

Section 4.2.2.6.2 ID privacy

Valid as of SCAS version: 17.1.0

Test Case:

Test Purpose: Verify that the AS acting as originating UA should send the anonymous identity if privacy is required.

Test Name: TC_USER_AUTHORIZATION

Pre-Condition:

- The privacy of the P-Asserted-Identity is required in AS.
- The UE is simulated.

Execution Steps:

The AS under test sends the initial request for a dialog ~~or~~ and request for a standalone transaction.

Expected Results:

The display-name of the From header field of the initial request is set to "Anonymous".

The addr-spec of the From header field of the initial request is set to Anonymous User Identity.

Expected Format of Evidence:

~~Provide evidence of the check of the product documentation in plain text.~~

Save the logs and the communication flow in a .pcap file.

2.4 Evaluation process definitions

The network product evaluation is defined in Chapter 2.4.4 of the document “Produktzertifizierung: Programm Network Equipment Security Assurance Scheme (NESAS)” (Product Certification: Network Equipment Security Assurance Scheme (NESAS)) [NESAS-Produkte]. The following process definitions and requirements shall be applied in the context of a network product evaluation process.

The complete evaluation methodology for network products is defined by the set of NESAS CSS-GI documents including this AIS-N2 accompanied with the applicable SCAS documents.

2.4.1 Preconditions

The following development evidence (or artefacts) shall be available to the evaluation facility before test execution is started.

1. Full version of NESAS process audit report with all attachments
2. Compliance evidence with reference to every process audited
   - 2.a. Initial evidence template (i.e. part of the audit report)
   - 2.b. Network product related evidence (i.e. actual evidence from the development process)
3. Network product under evaluation
   - 3.a. E Including unique version number r
4. Network product documentation
5. Supporting operational (test) environment
6. Parts list of the network product including supporting operational (test) environment (e.g. network plan)
7. Supplementary information (e.g. license information, login accounts)
8. Supplementary developer resources (e.g. certification support, technical support)
9. A list of runtime, orchestration, virtualization and execution environments and their respective configurations, which the applicant considers equal to the deployment method chosen for the test environment
10. A software bill of materials, as defined in Annex A, that covers all libraries and packages present in the deployed network product. If a library or package maintained by the vendor is based on software whose license is listed under "OSI Licenses", then an SBOM entry for the latter software shall also be provided by the vendor. The field "Relevance for product functioning" can be omitted and the entry for "Purpose of the component" shall in this case refer to the library or package actually included in the product
11. An architectural overview of the product under evaluation, which includes:
    - 11.a. Description of underlying operating system including software and libraries used from the operating system
    - 11.b. Description of operation mechanisms, which are derived from the underlying operating system and are required to run the network product in the desired state. Such mechanisms may exemplarily include:
      - 11.b.i. systemd-services
      - 11.b.ii. systemd-timers
      - 11.b.iii. cronjobs
      - 11.b.iv. crontabs
      - 11.b.v. contents of /etc/rc.local

11.c. Description of the deployment architectures chosen for the network product and the optimizations taken for each deployment architecture

11.d. Description of non-3GPP-specified interfaces present in the network product. This especially covers:

11.d.i. Enumeration of all interfaces required for external access to the network product with detailed purpose for each interface.

11.d.ii. Description of administration and maintenance interfaces (OAM))

11.d.iii. Description of the corresponding OAM software, with regards to features, capabilities, security precautions, usage of OAM software in the test setup

2.4.2 Preparation

These steps shall be performed before the actual network product evaluation is executed:

1. Generate a test plan, which includes the audits, under consent of the certification body
2. Setup of test facilities
3. Network product test setup

2.4.3 Evidence evaluation

The evidence evaluation is expected to be a two-step check activity. First, the evaluator shall check that the provided evidence is originated from the actual development processes of the network product. Second, the evaluator shall check, whether the actually provided evidence satisfies the expected evidence.

If the evidence evaluation fails for severe reasons, the network product evaluation shall not be started. In case of minor fails, the evaluation facility shall contact the certification body to take an individual decision.

2.4.4 Network product evaluation

Network product evaluations are only valid when based on the applicable SCAS documents and available product classes defined in Chapter 2.1.

The evaluation facility performs the evaluation in a test facility utilizing test tools. The evaluation facility is the location where the network product under evaluation is located and tested. The test facility can be a third-party resource which is temporarily used by the evaluation facility but shall be fully independent during the test execution.

The network product evaluation is based on independent testing run by qualification controlled personnel of the evaluation facility.

The evaluation facility shall evaluate the list of accepted runtime, orchestration, virtualization and execution environments, for which the vendor assumes equal behaviour when conducting the SCAS tests, whether equal behaviour can be assumed. The results shall be listed together with each runtime and orchestration environment listed by the vendor.

The evaluation facility shall execute all tests in a manner, which supports the network product's interoperability and minimizes the test tools' effects on the tests. The evaluation facility shall justify and qualify the choices made for each test tool, with specific regards to the previous clause.

All test cases defined in the referenced SCAS documents shall be conducted in accordance with the test definition and the refinements provided by the certification body. Any deviation shall be approved by the certification body. The test cases shall yield the expected results, in accordance with the test case definitions, the required execution steps and the reference requirement document provided by the standards defining organisation and as laid out in the regulations by the certification body. Before the evaluation is performed, the evaluation facility shall describe the testing concept (including used facilities, test tools, etc.) and

describe the test setup from a high-level perspective. Additionally, the basic vulnerability testing (from SCAS 33.117) shall be described for the network product on a more detailed level.

The testing concept shall be approved by the certification body as part of the evaluation kick-off meeting. After the kick-off meeting, evaluation should be successfully finished within 6 months. If the evaluation is not finished within this timeframe, the certification body shall decide on the continuation of the certification process. All project specific decisions guided in the following paragraphs shall be documented in the evaluation technical report (ETR), see Chapter 2.5.2.

If test cases require the evaluation of the implementation of cryptographic operations and no specification by the issuing standards defining organisation on the cryptographic algorithm exists, the security evaluation facility shall chose appropriate and secure standards to evaluate the cryptographic operations. Any choices not referred to approved and valid SCAS documents or other related standards shall be documented.

The evaluation steps provided by the test cases included in TS 33.117 chapter 4.4 shall be executed ultimately prior to ETR finalisation and submission. The certification body may request retesting of the relevant test cases, in case of relevant new information arising in this regard.

If any SCAS test fails, the overall verdict of the evaluation shall be fail, too. If the overall evaluation verdict is fail, the vendor may provide an updated version of the network product, fixing the relevant issues providing non-conformity with the given evaluation requirements from the SCAS tests. If a revision is provided by the vendor, fixing previously discovered non-conformity issues with the relevant SCAS tests, only tests, where equal results for the relevant SCAS tests cannot be obtained, shall be reperformed.

The evaluation facility shall consider how functional security requirements covered by the SCAS test during the evaluation are provided by the network product and may make suggestions to the certification body on how SCAS-test cases might be adapted to keep them applicable, if necessary. As security functional requirements may be provided by the respective kernel, running in the network product, the evaluation scope is limited by the execution scope of the kernel used in the network product. If security functional requirements can be provided by the network product by multiple means (e.g. products deployed in containers), the evaluation facility shall consider each mean during the evaluation. If the network product regularly consists of or requires multiple, clustered (virtual) machines (e.g. when using orchestrators for containers), the vendor shall prove the equal configuration of all clustered machines to the evaluation facility. All runtime, orchestration, virtualization and execution environments mentioned by the vendor, aiming for equal results of the relevant and applicable SCAS tests, shall be evaluated in accordance with the requirements mentioned above.

2.4.4.1 Network product under evaluation

The network product under evaluation can offer a broad set of 3GPP functionality. Before any SCAS test is executed the network product has to be configured as specified by the vendor. It might be possible to have multiple configurations in the scope of the evaluation. The different configurations shall be described unambiguously and detailed by the vendor. Additionally, the configurations shall be documented by the evaluation facility.

In general, for all configurations the full set of selected SCAS tests should be executed by the evaluation facility. If configurations only differ in a very small aspect, the evaluation facility can explain in the testing concept, whether the deviations do not affect the successful execution of relevant SCAS tests.

If the network product under evaluation is capable of providing the services tested by the relevant SCAS tests under multiple internet protocol (IP) versions, all relevant IP versions shall be covered during testing. Otherwise, the evaluation facility shall add a note to the ETR stating IP version, for which the evaluation has been conducted.

2.4.4.2 Test tools and test setup

Prior to testing, all test tools used by the evaluation facility have to be validated by the evaluation facility for the specific use-cases. All test results generated by the tools are under responsibility of the evaluation facility.

In general, test tools (and test tool suppliers) shall be independent from the network product vendor.

In case of specific test cases and scenarios, it may be necessary to utilize test tools provided by the network product vendor. This requires an individual decision by the certification body.

In general, all tests shall be executed in facilities controlled by the evaluation facility during testing. Any remote testing has to be declared to and approved by the certification body. Remote testing shall be organised in such a way that it ensures the laboratory's evaluation facility's impartiality.

The staff of the evaluation facility shall be present in the test facility generally and when performing remote testing. The valid functionality of the operational (test) environment shall be assured by the evaluation facility before executing the tests.

For the commissioning and installation of the network product under evaluation the evaluation facility is allowed to request support from the vendor. If this was necessary, it shall be clearly stated in the documentation of the evaluation facility. In this case the evaluation facility shall highlight which steps were not sufficiently documented in the network product documentation.

Independent of the evaluation strategy and utilized resources, ultimately, the evaluation facility is responsible for the evaluation results. The evaluation facility shall be able to re-execute all tests later.

2.4.4.3 Re-testing during an ongoing evaluation

The evaluation facility can run the full set of tests for re-testing of the network product.

Alternatively, the evaluation facility can reuse test results from the previous test execution. The evaluation facility has to give a rationale why these test results are still valid and the change of functionality in the updated network product has no impact. The final decision of the reuse of test results applies to the certification body. If the lab intends to reuse results, it is recommended that the lab contacts the certification body as soon as possible to enable efficient use of time.

2.4.4.4 Cooperation with the certification body

A good cooperation between the evaluation facility and the certification body is key for the success of every certification scheme. For the network product evaluation, the certification body has to understand the testing approaches of the evaluation facility on a detailed level.

To support this understanding, the certification body is allowed to witness test activities of the evaluation facility.

Additionally, if test execution and test results are not comprehensible, the certification body is allowed to request a specific retesting of the evaluation facility. In this case, the certification body will be witnessing the retesting.

All e-mail communication between evaluation facility and certification body has to include the certification ID issued by the certification body, written in square brackets, at the beginning of the e-mail’s subject line.

For data exchange during the evaluation the data exchange platform by the certification body, commonly "bscw.bund.de" should be used. Alternative data exchange platforms may be designated by the certification body. Data exchange platforms not provided by the certification body shall be approved by the certification body prior to usage.

Files uploaded to the data exchange platform shall be encrypted using OpenPGP for each recipient individually. The certification body shall be included with each data exchange as a recipient by using the valid process key.

If data is shared on the data exchange platform, all parties involved shall be informed by an e-mail.

2.5 Resulting Documents from Evaluation g

The evaluation facility has to provide some specific documents during the network product evaluation. Rather than providing document templates the following sections include the mandatory content, which has to be given in the specific documents.

All abbreviations and acronyms must be written out on first use.

All documents shall be provided in an accessible document, which conforms with the regulations given in Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0).

Eventual usage of specified writing conventions requires a designated chapter with details to the conventions employed. This chapter shall be provided as subchapter 3 to the annex.

Whenever a reference to vendor documentation, in any document provided by the evaluation facility, is made, the evaluation facility shall insert citations for the specific and relevant document using IEEE citation style[2].

In the future the certification body might provide specific document templates.

2.5.1 Evaluierungsplan

The evaluation plan of the evaluation facility shall follow the outline below:

1. Overview of the evaluation
   - 1.a. Points of contact
   - 1.b. Evaluation basis, e.g. selected SCAS documents
   - 1.c. Development processes
   - 1.d. Network product under evaluation, including unique version number
   - 1.e. Deliverables of the vendor
2. Technical evaluation plan details and schedule
   - 2.a. Tasks of the evaluation facility
   - 2.b. Personnel assignment, including competence justification
   - 2.c. Test facilities
   - 2.d. Test setup overview, including network diagram
   - 2.e. Deliverables of the evaluation facility
   - 2.f. Evaluation work plan
3. Certification tasks support, e.g. witness activities of the certification body
4. Test setup
5. Tools to be used for evaluation
   - 5.a. Operational (test) environment
   - 5.b. Evaluated configuration and configurations considered equal and to be covered by the certificate

[2] https://ieee-dataport.org/help/how-cite-references-ieee-documentation-style

2.5.2 Evaluation Technical Report (ETR)

The test setup has to be documented in a detailed way, as stated in the following outline, as part of the evaluation documentation in the ETR chapter 5. This documentation shall clearly state which components (i.e. network product under evaluation and additional operational (test) environment) are used and who provided each component for the test setup.

The Evaluation Technical Report (ETR) of the evaluation facility shall follow the outline below:

1. Basis of the evaluation
2. Evaluation objective / dependencies
   - 2.a. Referenced audit report and related documents
   - 2.b. Network product identification
   - 2.c. Evaluated configuration and deployment method
3. Requirements for evidence and evaluation
   - 3.a. List of relevant SCAS documents
4. Evaluation of developer/conformance evidence
   - 4.a. Used documents (from audit and network product)
   - 4.b. Check results
5. Test setup
   - 5.a. Tools used for evaluation
   - 5.b. Operational (test) environment
   - 5.c. Test setup overview
   - 5.d. Network product identification
   - 5.e. Evaluated configurations and deployment options
   - 5.f. Architectural overview
6. Network product evaluation results
   - 6.a. SCAS document A
     - 6.a.i. SCAS test A_ID1
     - 6.a.ii. SCAS test A_ID2
     - 6.a.iii. etc.
   - 6.b. SCAS document B
     - 6.b.i. SCAS test B_ID1
     - 6.b.ii. etc.
7. Summary
   - 7.a. Evaluation results
   - 7.b. Vulnerabilities
   - 7.c. Missing information and inconsistencies
   - 7.d. Necessary changes/improvements
   - 7.e. Conditions on the developer
   - 7.f. Conditions on the user
8. Final verdict
9. Annex

9.a. Glossary and list of acronyms

9.b. Bibliography

To provide a common understanding between the evaluation facility, the vendor and the certification body, the evaluation facility shall describe the architectural decisions taken during the network product's development as part of the architectural overview description. This description allows the improved assessment of results gathered in the SCAS tests conducted. The description shall include:

- Description of underlying operating system including software and libraries used from the operating system
- Description of operation mechanisms, which are derived from the underlying operating system and are required to run the network product in the desired state. Such mechanisms may exemplarily include:
  - systemd-services
  - systemd-timers
  - cronjobs
  - crontabs
  - contents of /etc/rc.local
- Description of the deployment architectures chosen for the network product and the optimizations taken for each deployment architecture
- Description of non-3GPP-specified interfaces present in the network product. This especially covers:
  - Enumeration of all interfaces required for external access to the network product with detailed purpose for each interface.
  - Description of administration and maintenance interfaces (OAM)
  - Description of the corresponding OAM software, with regards to features, capabilities, security precautions, usage of OAM software in the test setup

Each SCAS test shall be documented along the following structure:

Name	Content
Product version	Version number as set in application
SCAS test name	ID (e.g. TC_CONFIDENTIAL_ SYSTEM_INTERNAL_DATA)
Chapter 3GPP	Insert the chapter number of the SCAS test with the current version of the 3GPP SCAS document.
Tester	Tester name
Date	Date of test application
Reference / documentation	Reference to the SCAS document chapter with details to the test
Related SCAS document/version	SCAS document and 3GPP version
Procedure and execution steps	
Pre-condition (refinements only)	
Execution/steps (refinements only)	
Expected results (refinements only)	
Expected format of evidence (refinements only)	
Actual test results	
Verdict	Pass/fail

Table 4: Expected format of SCAS test documentation

2.6 Voting for a minor update or additional execution environment

In order to maintain certification, it is possible to include minor updates or additional execution environments in the existing security certificate. The requirements for this are defined in chapter 4 of the document “Produktzertifizierung: Programm Network Equipment Security Assurance Scheme (NESAS)” (Product Certification: Network Equipment Security Assurance Scheme (NESAS)) [NESAS-Produkte].

2.6.1 Impact Analysis Report as a precondition

As a base for an assessment, the applicant shall record the necessary information about a minor update or an additional execution environment in an Impact Analysis Report (IAR) and provid it together with a vote from the expert body (evaluation facility that evaluated the network product) and the application form to the certification body.

The evaluation facility shall have the following development evidence and information in the IAR for the vote:

1. Introduction - Information to uniquely identify
   - 1.a. the IAR (e.g. name, date, version number)
   - 1.b. the network product including unique version number in which the changes are reflected
   - 1.c. the underlying audit report (e.g. date, version number, identifier)
   - 1.d. the underlying ETR (e.g. date, version number, identifier)
   - 1.e. the persons who prepared the IAR and carried out the impact analysis and/or are responsible for it

1.f. the confidentiality of the document

2. Description of the changes

2.a. List of all changes to the network product

2.b. Description and justification of each listed change, including an analysis of the impact on the network product, the evaluated security performance and the original SCAS test used as a basis

3. Evidence of the changes (e. g: list of customised libraries and packages used to develop, build and deploy the network product

4. Conformance Evidence with reference to each audited process

4.a. Evidence of the application of the audited processes in the creation of the network product, as shown in the audit report.

The evaluation facility can obtain further information from the applicant in the IAR if this is required for the vote.

2.6.2 Vote as a result document of the inspection body

The evaluation facility shall draw conclusions on the basis of the IAR and the evidence provided and prepare a written assessment for the certification body

- That the changes described meet the definition of minor update or
- That the security statements of the certificate for the product are also valid in the added execution environment and that all applicable SCAS tests can be reproduced as in the evaluated execution environment.

The evaluation facility may obtain additional information and evidence and/or generate it for the assessment.

The assessment must be made in text form and contain a clear vote.

3 Comments

None

4 Coming into force

These AIS is valid with immediate effect and has to be applied in principle to all NESAS CCS-GI future certification proceedings unless agreed otherwise.

5 Reference documents

All references in this document and the NESAS CCS-GI glossary are located in the document “Verzeichnisse” (Indexes) [Verzeichnisse].

Annex

A. Software Bill of Materials

A Software Bill of Materials (SBOM) is a list of entries that adheres to a specific format, where each entry contains identifying information about a single component and possibly further associated information. The format used for an SBOM shall either be CycloneDX[3] (version 1.4 or above) or Software Package Data Exchange (SPDX)[4] (version 2.3 or above) in any representation supported by the respective format (e.g., JSON or XML).

Besides the actual list of component entries, an SBOM shall include the following information:

Attribute	*Definition*	*Recommended Format Field*	*Remarks*
Author	The name of the entity that created the SBOM.	SPDX: Creator/Creators[5] CycloneDX: "authors" property of "metadata" element[6]	The name of the legal entity, e.g., the company name, is sufficient as author information.
Timestamp	Date and time when the SBOM was created by the author.	SPDX: Created CycloneDX: "timestamp" property of "metadata" element	The timestamp shall follow the format mandated by the chosen SBOM format (SPDX or CycloneDX).

Table 5: Minimum set of attributes required for SBOM description.

A **component** is a unit of software, e.g., in the form of an application, a software library, an operating system, or firmware, which consists of one or more files. The SBOM entry for each component shall include at least the following information:

Attribute	*Definition*	*Recommended Format Field*	*Remarks*
Supplier name		SPDX: PackageSupplier[7] CycloneDX: "supplier" property of object under "components"[8]	For proprietary components, the name of the legal entity, e.g., the company name, is sufficient as supplier name. For Open Source components under licenses contained in [OSI Licenses], the name of the entity, project or service from which the component was obtained. Either a supplier of binary packages or as source code, shall be provided as supplier name (e.g., Python Package Index, Debian, Ubuntu, Github).
Component name		SPDX: PackageName[9] CycloneDX: "name" property of object under "components"[10]	The value given for this field should describe the most common and recognizable title or name of the component.

[3] https://cyclonedx.org/specification/overview/
[4] https://spdx.dev/specifications/
[5] https://spdx.github.io/spdx-spec/v2.3/document-creation-information/#68-creator-field
[6] https://cyclonedx.org/docs/1.4/json/#metadata_authors
[7] https://spdx.github.io/spdx-spec/v2.3/package-information/#75-package-supplier-field
[8] https://cyclonedx.org/docs/1.4/json/#components_items_name
[9] https://spdx.github.io/spdx-spec/v2.3/package-information/#75-package-supplier-field
[10] https://cyclonedx.org/docs/1.4/json/#components_items_name

Attribute	*Definition*	*Recommended Format Field*	*Remarks*
Version of the component		SPDX: PackageVersion[11] CycloneDX: "version" property of object under "components"[12]	Semantic Versioning[13] may preferably be used. If no official version identifier exists for the described component, then the identifier of the most recent version upon which the described component is based shall be provided. Furthermore, the applicant shall provide a summary of the changes between the most recent version upon which the described component is based and the one described by this SBOM entry in a separate document.
Support state of the component		SPDX: PackageSourceInfo[14] CycloneDX: An object with "nesasccsgi:support_state" as name under the "properties" property of object under "components"[15]	The assessment shall state whether the component is still actively maintained or if it has reached its end-of-life. If the component is considered actively maintained, it shall be stated whether the component is maintained by the vendor or a third party and evidence for the active maintenance shall be provided.
License of the component		SPDX: PackageLicenseDeclared[16] CycloneDX: "licenses" property of object under "components"[17]	If available, the corresponding license identifier from the SPDX license list18 shall be used. Otherwise, either the term "proprietary" or a custom identifier whose structure follows the format of an SPDX license expression19 shall be used.
Relevance for product functioning		SPDX: PackageDescription[20] CycloneDX: "description" property of object under "components"[21]	
Purpose of the component			The description shall cover at least all those functionalities that the product makes use of.

Table 6: Minimum set of attributes required per SBOM entry

If a specific component is included multiple times in the product (e.g., a specific version of a software library that is included in multiple applications running on the product), then only one corresponding entry in the SBOM is required. However, if multiple different versions of a particular component from a particular supplier are used in the product, then a separate entry must be provided for each included version of the component.

Templates that may be used to create an SBOM according to the above definition are available upon request at the certification body. Those templates contain the minimum number of fields in each SBOM

[11] https://spdx.github.io/spdx-spec/v2.3/package-information/#75-package-supplier-field
[12] https://cyclonedx.org/docs/1.4/json/#components_items_version
[13] https://semver.org/
[14] https://spdx.github.io/spdx-spec/v2.3/package-information/#712-source-information-field
[15] https://cyclonedx.org/docs/1.4/json/#components_items_properties
[16] https://spdx.github.io/spdx-spec/v2.3/package-information/#715-declared-license-field
[17] https://cyclonedx.org/docs/1.4/json/#components_items_licenses
[18] https://spdx.org/licenses/
[19] https://spdx.github.io/spdx-spec/v2.3/SPDX-license-expressions/
[20] https://spdx.github.io/spdx-spec/v2.3/package-information/#719-package-detailed-description-field
[21] https://cyclonedx.org/docs/1.4/json/#components_items_description

representation necessary to comply with the above requirements as well as those mandated by the respective format. Each placeholder in the template must be replaced with a correct entry that is conformant to the requirements of the corresponding format.