Federal Office
for Information Security

BSI TR-03148-P:
Test Specification

Conformance Tests for secure Broadband Routers
in compliance to BSI TR-03148

Version: 1.1
Date: 30/04/2020

Document history

Version	Date	Editor	Description
1.1	30/04/2020	BSI	Initial public release version

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: router-tr@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Tables

1 Introduction

The Technical Guideline [BSI TR-03148] specifies the requirements for a secure Broadband Router. The current document extends [BSI TR-03148] by defining conformity criteria for broadband routers and specifying tests which verify that the provided interfaces and functionalities fulfill the requirements defined in the referenced Technical Guideline.

1.1 Structure of this Document

The document is structured as follows: The first Section contains an introduction, basic definitions and this description of the structure of the document. In Section 2 the requirements of the test environment are described. Section 3 defines the implementation conformance statement (ICS). The ICS specifies information the applicant has to provide in order to apply for a conformity test. The test cases that are to be performed by the tester are defined in Section 4.

1.2 Definitions

This Section defines terms and abbreviations that will be used frequently in this Test Specification.

Term	Definition
Applicant	Organization on behalf a specific DUT should be tested according to [TR-03148] and the corresponding Test Specification [TR-03148-P]. The applicant does not necessarily have to be the manufacturer.
Application	A computer program that is designed for a particular purpose or task
Broadband	A term for various modern high speed internet access technologies unspecified in this document, in opposition to former internet access technologies such as dial-up modems
Client software	An application executed on the router providing client functionalities. Using this software the router is able to connect to services provided by other IT systems in the WAN or LAN network environment. A typical client software implemented on a router is represented by a web-client using openssl to connect to an internet service providing firmware update packages.
Community WLAN	A WLAN used by a larger user group with participants unknown to the end-user and logically separated from the private WLAN.
Customized (state)	A state of the DUT. The end-user has changed the configuration of the DUT to his personal needs differing from the initialized state and thus left the initialized state.
DUT	Device Under Test is a term used for the router, when it is subject to testing.
End-User	The primary user of the router's functionalities
Factory Setting (state)	A state of the DUT. The DUT is assembled and a firmware with manufacturer settings is installed on the DUT. The DUT offers an interface for a third party (e.g. IAP) or the end-user to put the DUT into operation. In this state the DUT may however contain inactive presets for the connection to the infrastructure of common IAPs and a pre-configured WLAN interface according to [BSI TR-03148], Section 3.1.2: WLAN Interface. If the DUT is automatically configured by the first boot (e.g. TR069), the device changes its state from *factory setting* to *initialized*.

Term	Definition
Firewall	A rule based packet filter enhancing the gateway functionality of a router to filtering the incoming and outgoing data traffic in a network. Thus the packet filter protects the devices in a network from unwanted access.
Firmware	A complete collection of software running on the router, including the operating system and the installed applications
Firmware Package	A packed version of the firmware that is provided by the manufacturer (see above)
Gateway	A device functionality that allows two separate devices that share no interface to communicate via their shared interfaces with the device acting as gateway. Further it is a network device that interconnects networks with different network protocol technologies and performs the necessary protocol conversions.
Guest WLAN	A WLAN used by guests of the end-user with explicit allowance to do so and logically separated from the private WLAN.
Initialized (state)	A state of the DUT. The DUT has been put into operation by the end-user. This state is often reached by performing an assisted initial configuration of the DUT (e.g. using a configuration wizard) including the selection of a preset for the connection to the infrastructure of the end-users IAP. This state is also referenced by the words “after initialization”.
Interface	A shared technological boundary that connects external and/ or internal subsystems implemented in hardware (e.g. LAN interface) or software (i.e. protocol interface)
Internet	A globally interconnected network infrastructure coordinated by the Internet Assigned Numbers Authority (IANA)
Internet Access	A connection to the Internet and the possibility of a device to connect to other entities through the Internet
Internet Access Provider	A service provider offering Internet Access to end-users
Internet Gateway Functionality	An Internet gateway’s functionality is to establish a connection to the infrastructure of an Internet Access Provider (IAP) to provide Internet access for the end-user
LAN	A data communications system that lies within a limited spatial area, has a specific user group and is not a public telecommunications network
Manufacturer	Assembles the router as a hardware component or has a third party assemble the router in his name or trade mark and provides the firmware and applications necessary for the operation of the router
Network Management Functionality	Functionalities for the management of the end-user’s private network containing (but not limited to) administration features of the network, management features for devices in the network and network separation.
Port	A number that is always associated with an IP address and the protocol type of the communication in order to communicate to end points
Private Network	A network that is only privately accessed (as opposed to public) as described in [TR-03148], Section 3.1: Private Network
Private WLAN	A WLAN used by the end-user and others with explicit allowance by the end-user.

Term	Definition
Public Network	A network that is publicly accessible (as opposed to privately) as described in [TR-03148], Section 3.2: Public Network
Router	A device that connects two networks, offering access to a WAN (and to the Internet using a modem) for the local user devices in the private network via a LAN and/ or WLAN (this covers integrated devices, i.e., devices encapsulating various components such as a modem, switch and access point in a single physical entity)
Service	An application (usually permanently) executed on the router providing a certain functionality on a defined interface. A typical service implemented on a router is represented by a web server listening on TCP port 80. Please note that client services are defined as "client software" (see above).
VPN	A network that is virtually not physically made private (encrypted) and therefore limited to a specific user group, but may use public networks as a physical basis
WAN	In opposition to LAN, a public telecommunications network that extends over a large geographical distance
Wi-Fi	Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing according to [IEEE-802.11].
WLAN	A wireless radio communications access technology based on specification [IEEE 802.11i] used in short range. Also known as RLAN. A WLAN interface does not have to be necessarily a Wi-Fi Certified solution.

Table 1: Definitions

2 Test Environment and Elements

This Section defines requirements of the test environment that MUST be fulfilled in order to perform the test cases as defined in this Test Specification.

2.1 Overview Interfaces

The interfaces to be considered for the test cases described in this Test Specification represent the interfaces defined in the reference specification [BSI TR-03148] Section 3.

WAN interfaces, which are not accessible from the public internet (e.g. management VLANs, VLANs for VoIP or IP TV) are not in scope of this Test Specification.

2.2 DUT

In this specification the Device Under Testing (DUT) is a single broadband router as defined in [BSI TR-03148] Section 2.

2.3 Test Operator

The test operator (also referred to as tester) MUST have the knowledge and technical ability to perform the tests as described in Section 4.

Equipment of the tester

The Test Procedures defined in the following Section 4 assume that the tester has access to a native internet access compatible with the DUT to be tested. If the DUT requires an internet access of a specific network provider than this fact has to be considered. The applicant or the manufacturer may support the testing with their test equipment and laboratory environment.

The testers WLAN equipment that is used for functional testing MUST be certified by the Wi-Fi Alliance according to [IEEE 802.11i] at least.

3 Implementation Conformance Statement

The purpose of the Implementation Conformance Statement (ICS) is the declaration of supported functionalities of the DUT to be approved by the tester/ testing laboratory. The declarations of the applicant are used for the determination of test cases to be performed.

The Implementation Conformance Statement MUST be filled in completely by the applicant. The information of the filled ICS MUST be documented in the test report.

3.1 General

3.1.1 Documentation

This Implementation Conformance Statement (ICS) is supported by the following documents delivered by the applicant. By filling in this ICS the author should refer to this references using additional page or Section indications.

User Guidance

The following documentation is part of the DUT delivery to the end-user. Paper format as well as digital formats delivered on any kind of data medium or by hyperlinks (e.g. PDF documentation for online access) should be considered.

Reference	Document title, version, date, author, hyperlink if needful
[userguide]	

Table 2: User Guidance Reference

Technical Documentation

The following documentation supports the testing of the DUT. Typically this documentation is not available for the end-user.

Reference	Document title, version, date, author, hyperlink if needful
[adminguide]	

Table 3: Technical Documentation Reference

3.1.2 Identification of the DUT

Hardware and firmware of the DUT under test can be identified by the following information.

marketing name:	
hardware version/ part number:	
serial number:	
firmware version in *factory setting*:	

Table 4: Identification of the DUT

3.2 Applicability of Test Requirements

The applicant is asked to fill in the following Table 5: Applicability of Test Requirements. Each Test Requirement is referred by its wording. Using the tick boxes the applicant can indicate

☐ Yes The applicant states, that the DUT is compliant to this specific Test Requirement.

☐ No The applicant states, that the DUT is NOT compliant to this specific Test Requirement.
In this case the applicant should use the "Notes:" field of the respective Test Requirement to provide further details.

☐ N/A The applicant states, that the specific Test Requirement is Not Applicable for the DUT.
In this case the applicant should use the "Notes:" field of the respective Test Requirement to provide further details. A "MUST" Requirement cannot be N/A.
Note: The tester later decides, if the details provided by the applicant are sufficient (See Section 4: Test Cases for details) to skip the Test Requirement.

The keywords “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [IETF RFC 2119]. The keywords “CONDITIONAL” and “IF” mean that the usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

For further explanations and additional notes for the tester regarding these keywords refer to Section 4, Test Cases. The relevant keywords are **HIGHLIGHTED** in the following Table.

TR	Description of TR	Yes	No	N/A
Module A - Private Network				
TR.A.1	A DUT **MUST** offer a Local Area Network (LAN) or WLAN interface to offer access to the Internet for the local user devices in the private network. *Notes:*	☐	☐	☐
TR.A.2	In factory setting the DUT **SHOULD** restrict access to a defined list of services provided to devices connected on the LAN and WLAN interface by the DUT. *Notes:*	☐	☐	☐
TR.A.3	Only a minimal selection of services **SHOULD** be available on the LAN and WLAN interface of the DUT. *Notes:*	☐	☐	☐
TR.A.4	All services provided by the DUT **MUST** be documented by the manufacturer including the port(s) or port ranges used. *Notes:*	☐	☐	☐
TR.A.5	If one of the service offered by the DUT is deactivated during operation of the DUT the corresponding port(s) **MUST** be closed. *Notes:*	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.A.6	The WLAN interface **MUST** at least be implemented according to [IEEE 802.11i]. *Notes:*	☐	☐	☐
TR.A.7	In factory setting the Extended Service Set Identifier (ESSID) **SHOULD NOT** contain any information that consists of or is derived from data or parts of data that depend on the DUT model itself. *Notes:*	☐	☐	☐
TR.A.8	The DUT **MUST** allow an authenticated end-user to change the ESSID. *Notes:*	☐	☐	☐
TR.A.9	The DUT **MUST** support encryption according to Wi-Fi Protected Access II (WPA2) based on [IEEE 802.11i] or more up to date versions for every private or guest WLAN. *Notes:*	☐	☐	☐
TR.A.10	If WLAN is activated in factory setting the supported encryption **MUST** be activated in factory setting. *Notes:*	☐	☐	☐
TR.A.11	The passphrase (pre-shared key, PSK) configured in factory setting **SHOULD** have a length of at least 20 digits and **MUST NOT** contain information that consists of or is derived from data or parts of data that depend on the DUT itself. *Notes:*	☐	☐	☐
TR.A.12	All private cryptographic keys and secrets **MUST NOT** be shared by multiple devices in the factory setting and initialized state. *Notes:*	☐	☐	☐
TR.A.13	The DUT **MUST** allow an authenticated end-user to set the passphrase (PSK) to a different value. *Notes*:	☐	☐	☐
TR.A.14	Changing the PSK **SHOULD** be supported by a mechanism showing the strength of the new desired PSK based on the number of digits and classes of digits with a mechanism comparable to the given example mechanism for passwords described in [TR-03148]. *Notes*:	☐	☐	☐
TR.A.15	The DUT **MAY** implement Wi-Fi Simple Configuration (WSC) according to [WSC2]. *Notes*:	☐	☐	☐
TR.A.16	Personal Identification Number (PIN) based WPS **MAY** only be used, if the feature is deactivated in the initialized state and a new PIN is generated for each newly registered device. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.A.17	Performing WPS based on Near Field Communication (NFC) **SHOULD** be deactivated in the initialized state. *Notes*:	☐	☐	☐
TR.A.18	A user-configured guest WLAN **SHOULD** fulfill the requirements of a Private WLAN (refer to Section 4.2.2.1 above) as well. *Notes*:	☐	☐	☐
TR.A.19	The guest WLAN **SHOULD** be deactivated using factory setting and **MUST NOT** allow any communication with devices that are connected to the private WLAN or LAN interface. *Notes*:	☐	☐	☐
TR.A.20	The guest WLAN **MUST NOT** allow access to the configuration of the DUT. *Notes*:	☐	☐	☐
TR.A.21	A community WLAN **MUST** be restricted to allowing Internet Access to the devices connected to this WLAN. Connection to other devices connected to the LAN interface, private WLAN or guest WLAN **MUST NOT** be allowed by the DUT. *Notes*:	☐	☐	☐
TR.A.22	The community WLAN **MUST NOT** allow access to the configuration of the DUT. *Notes*:	☐	☐	☐
Module B - Public Network				
TR.B.1	The requirements to the corresponding WAN interface **MUST** be fulfilled by all instances of the interface in scenarios where the DUT is connected to more than one Internet Service. *Notes*:	☐	☐	☐
TR.B.2	Only a minimal selection of services **MUST** be available to the public network. *Notes*:	☐	☐	☐
TR.B.3	The services used for Voice over IP (VoIP) telephony **MUST** only be available if the DUT is already configured to use VoIP. If VoIP is deactivated on the DUT these services **MUST** not be available. *Notes*:	☐	☐	☐
TR.B.4	The services used for remote configuration **MUST** only be available if the DUT is configured to use remote configuration. If remote configuration is deactivated on the DUT these services **MUST** not be available. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.B.5	All services provided by the DUT **MUST** be documented by the manufacturer including the port(s) or port ranges used. *Notes*:	☐	☐	☐
TR.B.6	If one of the services offered by the DUT is deactivated during operation of the DUT the corresponding port(s) **MUST** be closed. *Notes*:	☐	☐	☐
TR.B.7	After initialization the DUT **MUST** have access to an Internet Service provided by an Internet Access Provider (IAP) through a Wide Area Network (WAN) interface. *Notes*:	☐	☐	☐
TR.B.8	After initialization the DUT **MUST** restrict access on the WAN interface to a defined list of services provided by the DUT. *Notes*:	☐	☐	☐
Module C - Functionalities				
TR.C.1	Functionalities, which are deactivated as a factory setting **MUST** be made transparent to the end-user IF they become activated during initialization. *Notes*:	☐	☐	☐
TR.C.2	Functionalities **MUST NOT** be hidden from the end-user. *Notes*:	☐	☐	☐
Module D - Configuration and Information				
TR.D.1	All access methods allowing the end-user to configure the DUT and/ or access information from the current or past state of the DUT and its services in all three states (factory setting, initialized and customized) are in scope of the Module D Test Requirements. *Notes*:	☐	☐	☐
TR.D.2	Access to the configuration of the DUT **MUST** at least be secured by a password in the initialized and customized state. The DUT **MAY** offer a higher level of security by providing alternative authentication mechanisms. *Notes*:	☐	☐	☐
TR.D.3	If the DUT offers configuration through a web interface the complete communication to access the configuration **SHOULD** be secured using HTTP over Transport Layer Security (TLS) support according to [TR-02102-2] Section 3: Recommendations. *Notes*:	☐	☐	☐
TR.D.4	In factory setting the DUT **MUST** allow end-user access to the configuration only using an interface of the private network. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.D.5	If the DUT allows to access the configuration over an interface of the public network (Module B) as a customization feature this communication **MUST** be encrypted using TLS according to [TR-02102-2] Section 3: Recommendations. This access method **MUST** be deactivated in factory setting. *Notes*:	☐	☐	☐
TR.D.6	The end-user **SHOULD** be able to configure the port to be used for access to the configuration via the WAN interface. *Notes*:	☐	☐	☐
TR.D.7	If the DUT offers an option to save the current configuration to a file, this file **SHOULD** be encrypted and **SHOULD** be protected by a user selected password. The end-user **SHOULD** be assisted upon setting the password by a mechanism indicating the strength of the password by a mechanism similar to the one described for access to the configuration (refer to Section 4.4.3, Passwords). *Notes*:	☐	☐	☐
TR.D.8	To export and/ or import the DUT settings the end-user **MUST** be successfully authenticated at the device. *Notes*:	☐	☐	☐
TR.D.9	The preset password used for user authentication **MUST** contain at least 8 characters, including at least two of the following kinds of characters: uppercase letters [A-Z], lowercase letters [a-z], special characters [e.g. ?, !, $, etc.] or numeric characters [0-9]. *Notes*:	☐	☐	☐
TR.D.10	The DUT **MUST** allow an authenticated end-user to change the password after entering the previous password. *Notes*:	☐	☐	☐
TR.D.11	The password authentication mechanism **MUST** be protected against brute force attacks. *Notes*:	☐	☐	☐
TR.D.12	The session of an authenticated end-user **MUST** be protected against session hijacking attacks. At minimum session time outs and Cross-Site-Request-Forgery (CSRF) tokens must be implemented. *Notes*:	☐	☐	☐
TR.D.13	The DUT **MUST NOT** be initialized with accounts undocumented to the end-user. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.D.14	The mechanism indicating the password strength is based on the entropy of the password entered by the user. The entropy **MAY** be estimated by considering the password length and combination of different kind of characters used. *Notes*:	☐	☐	☐
TR.D.15	This mechanism **MUST** prevent the user from selecting a weak password without being warned about doing so. *Notes*:	☐	☐	☐
TR.D.16	The preset password used with factory setting **MUST NOT** contain information that consists of or is derived from data or parts of data that depend on the DUT itself. *Notes*:	☐	☐	☐
TR.D.17	The preset password used with factory setting **MUST NOT** be shared by multiple devices of the same manufacturer. *Notes*:	☐	☐	☐
TR.D.18	The session of an authenticated end-user **MUST** be protected against session hijacking attacks. At minimum session time outs and CSRF tokens **MUST** be implemented. *Notes*:	☐	☐	☐
TR.D.19	The DUT **MUST NOT** be initialized with accounts undocumented to the end-user. *Notes*:	☐	☐	☐
TR.D.20	All private cryptographic keys and secrets used for alternative authentication mechanisms **MUST NOT** be shared by multiple devices in the factory setting and initialized state. *Notes*:	☐	☐	☐
TR.D.21	The DUT **MUST** provide security relevant information to the authenticated end-user. This information **SHOULD** be made available at a central source of information (e.g. on a specific site on the configuration interface). *Notes*:	☐	☐	☐
TR.D.22	The DUT **SHOULD** provide a functionality to send (push) notifications of security relevant events to the end-user. This communication **MUST** always be encrypted, if the distant communication endpoint supports encryption. If the distant communication endpoint supports TLS this encryption method **MUST** be used. For TLS the requirements of [TR-02102-2], Section 3: Recommendations, are mandatory. The DUT **MUST** restrict the supported cipher suites for alternative encryption methods to the suites listed in [TR-02102-2] Section 3. The functionality to send (push) notifications **MUST** only be activated upon the end-users request. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.D.23	The DUT **MUST** allow the end-user to display the version number of the firmware currently installed on the DUT. The DUT **MAY** additionally show an estimate date of the firmware. *Notes*:	☐	☐	☐
TR.D.24	If the DUT has obtained knowledge that the firmware installed on it is currently out-of-date the DUT **MUST** inform the end-user about this with a meaningful message. *Notes*:	☐	☐	☐
TR.D.25	As soon as a decision is made by the manufacturer to not support for the DUT anymore the same mechanism **MUST** be used by the manufacturer to inform the end-user about the End of Service (EoS) of the DUT as required by TR.E.10. *Notes*:	☐	☐	☐
TR.D.26	The DUT **MUST** allow the end-user to display the current state (active/ inactive) of the firewall as well as it **MUST** display the rule set currently set up by the end-user. *Notes*:	☐	☐	☐
TR.D.27	If the DUT offers remote configuration the status of this functionality (active/ inactive) **MUST** be made available to the end-user. *Notes*:	☐	☐	☐
TR.D.28	The DUT **MUST** allow the end-user to retrieve information about the last or more login attempt(s). If the login attempt was made after initialization, the information about the last login attempt(s) **MUST** consist of the time and date of the login attempt, the IP address and the MAC address of the device from which the login attempt was made from. *Notes*:	☐	☐	☐
TR.D.29	The DUT **MUST** display a summary page for the currently active services on all interfaces. This especially refers to those services optionally provided by the DUT. The DUT **SHOULD** display exact details on the services running. *Notes*:	☐	☐	☐
TR.D.30	The DUT **SHOULD** display information on the devices that are currently connected to the DUT and the interface being used for this connection. This information **MUST** include the devices IP address, MAC address and **SHOULD** contain information on the duration of the connection. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.D.31	The DUT **SHOULD** allow the end-user to display general information of security relevant events concerning the DUT itself including detected attacks on the secure operation or attempts to manipulate the DUT. If a login attempt was made after initialization the DUT **SHOULD** display the time and date of the login attempt and the IP address and the MAC address of the device the login attempt was made from. *Notes*:	☐	☐	☐
Module E - Firmware Updates				
TR.E.1	The DUT **MUST** have a functionality to update the firmware using a firmware package. *Notes*:	☐	☐	☐
TR.E.2	The DUT **MUST** allow the end-user to fully control such a firmware update and determine to initiate an online update and/ or manually update the firmware through the configuration interface. *Notes*:	☐	☐	☐
TR.E.3	The DUT **SHOULD** offer an option to automatically retrieve security relevant firmware updates from a trustworthy source over the Internet (WAN interface). *Notes*:	☐	☐	☐
TR.E.4	If the DUT offers an option to automatically retrieve firmware updates this functionality **SHOULD** be activated by default, but **MUST** be possible for the end-user to deactivate it when using customized settings. *Notes*:	☐	☐	☐
TR.E.5	The firmware update function of the DUT **MUST** check the authenticity of the firmware package before it is installed on the DUT. *Notes*:	☐	☐	☐
TR.E.6	The authenticity of a firmware package **SHOULD** be based on a digital signature that is applied to the firmware package by the manufacturer and checked by the DUT itself. For this purpose only signature schemes in accordance to [SOG-IS] Section 5.2 **MUST** be used. *Notes*:	☐	☐	☐
TR.E.7	The DUT **MUST NOT** automatically install any unsigned firmware. *Notes*:	☐	☐	☐
TR.E.8	The DUT **MAY** allow the installation of unsigned firmware IF a meaningful warning message has been shown to the authenticated end-user and the end-user accepts the installation of the unsigned firmware. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.E.9	The manufacturer of the DUT **MUST** provide information on how long firmware updates fixing common vulnerabilities and exposures that have a high severity will be made available. This information **SHOULD** be available on the manufacturer website. Additionally it **MAY** be made available on the DUT configuration interface. *Notes*:	☐	☐	☐
TR.E.10	The manufacturer **MUST** provide information if the DUT has reached the End of its Support (EoS) and will not receive firmware updates by the manufacturer anymore. This information (EoS) **MUST** be made available on the DUT configuration. *Notes*:	☐	☐	☐
TR.E.11	The manufacturer **MUST** provide firmware updates to fix common vulnerabilities and exposures of a high severity without culpable delay (without undue delay) after the manufacturer obtains knowledge. *Notes*:	☐	☐	☐
Module F - Firewall				
TR.F.1	The DUT **MUST** contain firewall functionalities that include the basic monitoring and controlling of how IP packets between the private network and the end-user (WLAN and LAN interface) on the one side and the public network i.e. Internet (WAN interface) on the other side are exchanged. The firewall **MUST** enforce rules for this kind of network traffic by implementing a packet filter. *Notes*:	☐	☐	☐
TR.F.2	The end-user **MUST** be able to configure the set of rules being used. *Notes*:	☐	☐	☐
TR.F.3	The firewall **MUST NOT** contain any port forwarding rules configured initially. *Notes*:	☐	☐	☐
TR.F.4	The DUT **MUST** allow the end-user to define rules for incoming and outgoing network traffic. *Notes*:	☐	☐	☐
TR.F.5	The firewall functionalities of the DUT **MUST** be enabled after initialization. After initialization the firewall **SHOULD** allow all outgoing communication from the private network and deny all not requested incoming communication from the public network. *Notes*:	☐	☐	☐
Module G - Domain Name System (DNS)				
TR.G.1	The DUT **SHOULD** allow the end-user to configure a different DNS server. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
TR.G.2	The DUT **SHOULD** implement mechanisms to prevent so called rebind attacks. *Notes*:	☐	☐	☐
TR.G.3	Source ports and transaction-IDs of the DNS protocol **MUST** be selected randomly by the DUT. *Notes*:	☐	☐	☐
TR.G.4	The DUT **MUST** support forwarding of DNSSEC packets according to [IETF RFC 6781]. *Notes*:	☐	☐	☐
TR.G.5	The DUT **MUST** support forwarding of DANE packets according to [IETF RFC 6698]. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
Module H - Dynamic Host Configuration Protocol (DHCP)				
TR.H.1	The DUT **MUST** support using Dynamic Host Configuration Protocol (DHCP) for devices connected on the LAN and WLAN interface. *Notes*:	☐	☐	☐
TR.H.2	The DUT **SHOULD** provide an option to manually set the DNS server being used by all devices connected to the DUT via DHCP. The DNS server configured in DHCP-Option 6 **SHOULD** be the DNS server manually configured or the DNS server provided by the IAP. *Notes*:	☐	☐	☐
Module I - Factory Reset				
TR.I.1	The DUT **MUST** allow an authenticated end-user to reset the DUT back to factory setting from an initialized or end-user customized state by deleting the personal data and settings of the end-user from the DUT. *Notes*:	☐	☐	☐
Module J - Internet Protocol version 6 (IPv6)				
TR.J.1	The DUT **SHOULD** implement Internet Protocol version 6 (IPv6) and offer its services accordingly. *Notes*:	☐	☐	☐
TR.J.2	It is **RECOMMENDED** that the DUT only supports the types of ICMPv6 messages marked with an "X" in Table 7 of [TR-03148]. *Notes*:	☐	☐	☐
TR.J.3	The DUT **MUST NOT** forward inbound IPv6 traffic, if it does not belong to a known connection. *Notes*:	☐	☐	☐
Module K - Remote Configuration				
TR.K.1	For retail devices that are not pre-configured with end-user specific settings no remote configuration **MUST** be active before initialization. *Notes*:	☐	☐	☐
TR.K.2	Remote configuration **MUST** only be allowed with an encrypted and (server-) authenticated connection according to [TR-02102-2] or other techniques fulfilling the same security requirements. *Notes*:	☐	☐	☐
TR.K.3	All private cryptographic keys and secrets **MUST NOT** be shared by multiple devices in the factory setting and initialized state. *Notes*:	☐	☐	☐
TR.K.4	It **MUST** be visible to the end-user if remote configuration is currently activated. *Notes*:	☐	☐	☐

TR	Description of TR	Yes	No	N/A
Module L - Voice over IP (VoIP)				
TR.L.1	If the DUT provides support for Voice over IP (VoIP) this functionality **SHOULD** be implemented in a way that the end-user can turn off the functionality completely. *Notes*:	☐	☐	☐
TR.L.2	If the DUT provides support for Voice over IP (VoIP) this functionality **SHOULD** be implemented in a way that certain phone numbers can be blocked in a dedicated black list. *Notes*:	☐	☐	☐
TR.L.3	The DUT **MUST NOT** respond to SIP requests to unknown communication partners on the WAN interface. *Notes*:	☐	☐	☐
TR.L.4	The WAN interface does not have extensions that do not require an authentication (noauth). *Notes*:	☐	☐	☐
TR.L.5	The services providing VoIP functionalities **MUST** only be running as long as IP based communication is activated. *Notes*:	☐	☐	☐
Module M - Virtual Private Network (VPN)				
TR.M.1	If the DUT offers a Virtual Private Network (VPN) feature it **SHOULD** allow the end-user to configure it as a VPN server. *Notes*:	☐	☐	☐
TR.M.2	The cryptographic parameters for IPsec defined in [TR-02102-3] **SHOULD** be used accordingly. *Notes*:	☐	☐	☐
TR.M.3	All private cryptographic keys and secrets **MUST NOT** be shared by multiple devices in the factory setting and initialized state. *Notes*:	☐	☐	☐

Table 5: Applicability of Test Requirements

3.3 Module A - Private Network

Using the following Table 6 the applicant MUST identify all private network interfaces (LAN, WLAN) and associated services provided by the DUT. All services MUST be documented and the corresponding state of the DUT MUST be identified. If an identified service is available on additional interfaces after *initialization* or *customization* this MUST be noted in the description field. Please refer to implementation details such as but not limited to open source packages, libraries, proprietary implementations and/ or documentation.

Interface	State	Service[1]	Port/ Protocol	Description
	[*factory*]			
	[*initialized*]			
	[*customized*]			

Table 6: Private Network Interfaces and services of the DUT

In addition to the services provided by the DUT the following client implementations are present in the DUT's firmware. The applicant MUST identify corresponding interfaces (LAN, WLAN) and the states in which the client software could be used by the DUT. Please refer to implementation details such as but not limited to open source packages, libraries, proprietary implementations and/ or documentation.

Interface	State	Client software[2]	Description
	[*customized*]		
	[*initialized*]		
	[*factory*]		

Table 7: Private Network Interfaces and client software of the DUT

3.3.1 Local Area Network (LAN) Interfaces

No questions for the Implementation Conformance Statement.

3.3.2 WLAN Interfaces

The WLAN interfaces MUST at least be implemented according to [IEEE 802.11i]. The applicant MUST provide a statement of the DUT manufacturer about the compatibility of the implemented WLAN interface(s).

(answer) _____

_____

_____

1 Please refer to Table 1, Definitions, for the interpretation of this term.
2 Please refer to Table 1, Definitions, for the interpretation of this term.

If Wi-Fi Simple configuration (WSC) is supported by the DUT the implementation MUST be according to [WSC2]. The applicant MUST provide a statement of the DUT manufacturer about the implementation of WSC according to WSC2.

(answer) _____

_____

_____

The applicant MUST identify the DUT's WLAN Interface(s) and their features and refer to the documentation for the implementation details.

Interface	implemented	WLAN features	documentation reference
		guest WLAN	e.g. [reference according to appendix], section, page
		community WLAN	
		WPS - Push Button Configuration (PBC)	
		WPS - USB Flash Drive (UFD)	
		WPS - Personal Identification Number (PIN)	
		WPS - Near Field Communication (NFC)	

Table 8: WLAN features

The applicant MUST list all identifiers of private cryptographic keys and secrets (e.g. PSKs) used in the *factory setting* and *initialized* state by any WLAN access profile. A statement is necessary how these key(s) or secrets are generated and whether these key(s) or secrets are shared by multiple DUTs.

state	identifier of private keys or secrets	generated by/ unique per DUT	WLAN access profile
[*initialized*]			e.g. [WLAN access profile configured during setup, SSID printed on product label, can be changed by the end user]
[*factory*]			e.g. [factory default WLAN access profile, SSID printed on product label]

Table 9: WLAN cryptographic keys and secrets

The applicant MUST detail the mechanism showing the strength of a new desired PSK of a WLAN access profile.

(answer) _____

_____

_____

3.4 Module B - Public Network

Using the following Table 10 the applicant MUST identify all public network interfaces and associated services provided by the DUT. All services MUST be documented and the corresponding state of the DUT MUST be identified. If an identified service is available on additional interfaces after *initialization* or *customization* this MUST be noted in the description field. Please refer to implementation details such as but not limited to open source packages, libraries, proprietary implementations and/ or documentation.

Interface	Service	State[3]	Port/ Protocol	Description
		[*factory*]		
		[*initialized*]		
		[*customized*]		

Table 10: Public Network Interfaces and services of the DUT

In addition to the services provided by the DUT the following client implementations are present in the DUT's firmware. The applicant MUST identify corresponding interfaces and the states in which the client software could be used by the DUT. Refer to implementation details such as but not limited to open source packages, libraries, proprietary implementations and/ or documentation.

Interface	State	Client software[4]	Description
	[*customized*]		
	[*initialized*]		
	[*factory*]		

Table 11: Public Network Interfaces and client software of the DUT

3.4.1 Wide Area Network (WAN) Interfaces

No questions for the Implementation Conformance Statement.

3 Please refer to Table 1, Definitions, for the interpretation of this term.
4 Please refer to Table 1, Definitions, for the interpretation of this term.

3.5 Module C - Functionalities

The DUT provides the following functionalities. The applicant MUST list all functionalities according to the clarification given below. The applicant MUST provide information about the state(s) where active by default and MUST refer to the corresponding technical documentation (see Table 3, Technical Documentation Reference).

Clarification

Typical functionalities to be listed are e.g. WLAN support, DHCP client and server implementation, Firewall, IPv6, VoIP, ssh access, DynDNS client or VPN support, Smart Home functionalities, storage solutions like network attached storage (NAS), DECT support. Those functionalities are also typically listed in the marketing material of the manufacturer.

Note that also non security relevant functionalities are addressed by this Module C. The intention is to provide a complete list of the DUT's functionality to the tester. The tester should be able to decide the test scope and whether or not a functionality is security relevant.

It is not the intention of the following listing to provide details about obviously irrelevant functionalities like LEDs, buzzer, support for voice encryption, call forwarding, ESATA or USB connections.

Functionality	Default active in State(s)	Description and documentation reference
	[*customized*]	
	[*initialized*]	
	[*factory*]	

Table 12: Functionalities of the DUT

3.6 Module D - Configuration and Information

The DUT provides the following access methods to the functionalities allowing the end-user to

a) configure the DUT and/ or

b) access information from the current or past state of the DUT and its services.

Method	Description	Policy
web server	access the web server at TCP port 80 on the LAN interface	password policy A
ssh, telnet ...		password policy B
	documentation reference to specific implementations	OTP, 2-Factor

Table 13: List of access methods

If passwords are used to restrict access to a method listed in Table 13 the following password policies are implemented.

Policy	Description
password policy A	
password policy B	

Table 14: Password Policies

The following access methods accept a preset password for end-user authentication. The generation method for the preset password should be disclosed. The applicant MUST detail if the preset password is unique per device.

Method	Description	Generation method for the preset password	Password unique per device?
configuration assistant tool			yes/ no (no: why?)

Table 15: List of preset passwords

If passwords are used to restrict access to a method listed in Table 13 the DUT provides the following procedures for an authenticated end-user to change his password:

procedure	Description
A	
B	

Table 16: Password change procedures

If more than one access method to configure the DUT is available (e.g. web interface, ssh, telnet, mobile APP) the applicant MUST declare (or refer to documentation) if different configuration options are accessible by different access methods. For example: using the web interface all configuration options are accessible, using the mobile APP only a subset of options could be modified.

(answer) _____

_____

_____

The following sessions of an authenticated end-user could be established to/ from the DUT. This list should refer to all sessions of this kind the DUT offers, not only to the access methods listed in Section 3.6, Table 13, to configure the DUT. For example alternative sessions to change the password, to access information from the current or past state of the DUT and its services or alternative authentication mechanisms are also in focus. The applicant MUST address all mechanisms against session hijacking attacks (e.g. tokens).

Session	Description	protection against session hijacking attacks

Table 17: Sessions of an authenticated end-user

The applicant MUST list all identifiers of private cryptographic keys and secrets used in the *factory setting* and *initialized* state by any alternative authentication method. A statement is necessary how these key(s) or secrets are generated and whether these key(s) or secrets are shared by multiple DUTs.

state	identifier of private keys or sec	generated by/ unique per DUT	alternative authentication method
[*customized*]			
[*initialized*]			
[*factory*]			

Table 18: Cryptographic keys and secrets of alternative authentication methods

The applicant MUST list all types of security relevant events concerning the DUT itself which could be displayed to the end-user. Typical events of this type are detected attack on the secure operation or attempts to manipulate the DUT. Using the following Table 19 the applicant MUST describe in detailed the event, which mechanism results in the event and what data is logged and is presented to the end-user.

security relevant event	Description

Table 19: Security relevant events

3.7 Module E - Firmware Updates

The DUT provides the following firmware update mechanism(s). The applicant MUST list all mechanisms and MUST provide a short description as well as a reference to the corresponding technical documentation (see Table 3, Technical Documentation Reference).

Update mechanism	Description and documentation reference
manual update	firmware package download by the end-user, manually installation
automated update	
remote update	

Table 20: Firmware Update Mechanisms

Firmware package files MUST be authenticated by the DUT. The following mechanisms are implemented to provide this functionality. The applicant MUST list all mechanisms and MUST provide a short description as well as a reference to the corresponding technical documentation (see Table 3, Technical Documentation Reference).

Authentication mechanism	Description and documentation reference
digital signature	

Authentication mechanism	Description and documentation reference

Table 21: Firmware authentication mechanisms

The applicant MUST list all identifiers of private cryptographic keys and secrets used in the *factory setting* and *initialized* state by the firmware update mechanism(s) identified above. A statement is necessary how these key(s) or secrets are generated and whether these key(s) or secrets are shared by multiple DUTs.

state	identifier of private keys or secrets	generated by/ unique per DUT	Update mechanism
[*customized*]			
[*initialized*]			
[*factory*]			

Table 22: Cryptographic keys and secrets used by the firmware update mechanism(s)

The applicant MUST provide information about the processes and mechanisms to inform the end-user about firmware updates fixing common vulnerabilities and exposures that have a high severity.

(answer) _____

The applicant MUST provide information about the processes and mechanisms to inform the end-user if the DUT has reached the End of its Support (EoS).

(answer) _____

3.8 Module F - Firewall

The DUT MUST contain firewall functionalities. The applicant MUST provide information about the implementation details. Please refer to software used (e.g. open source, proprietary) and technical documentation.

(answer) _____

3.9 Module G - Domain Name System (DNS)

The DUT MUST contain DNS functionalities. The applicant MUST provide information about the implementation details. Please refer to software used (e.g. open source, proprietary) and technical documentation.

(answer) _____

The DUT SHOULD implement mechanisms to prevent so called rebind attacks. The applicant MUST provide information about the implementation details for this functionality.

(answer) _____

_____

_____

The DUT MUST support forwarding of DNSSEC packets according to [IETF RFC 6781 and the contained RFC in it]. The applicant MUST state that the DNS implementation of the DUT is according to [IETF RFC 6781 and the contained RFC in it].

(answer) _____

_____

_____

The DUT MUST support forwarding of DANE packets according to [IETF RFC 6698]. The applicant MUST state that the DNS implementation of the DUT is according to [IETF RFC 6698].

(answer) _____

_____

_____

3.10 Module H - Dynamic Host Configuration Protocol (DHCP)

The DUT MUST contain DHCP functionalities. The applicant MUST provide information about the implementation details. Please refer to software used (e.g. open source, proprietary) and technical documentation.

(answer) _____

_____

_____

3.11 Module I - Factory Reset

The DUT provides the following factory reset mechanism(s). The applicant MUST list all mechanisms and MUST provide a short description as well as a reference to the corresponding user guidance (see Table 2, User Guidance Reference).

Factory reset mechanism	Description and documentation reference
reset button (hardware)	
reset function provided by access method A	

Table 23: Factory Reset Mechanisms

3.12 Module J - Internet Protocol version 6 (IPv6)

No questions for the Implementation Conformance Statement.

3.13 Module K - Remote Configuration

The applicant MUST indicate if the DUT is pre-configured with end-user specific settings or belongs to the retail device class. In addition the applicant MUST indicate if the DUT supports remote configuration and if this is active before initialization.

(answer) _____

_____

_____

If remote configuration is supported by the DUT the applicant MUST provide information about the implementation details. Please refer to methods supported, software used (e.g. open source, proprietary) and technical documentation.

(answer) _____

_____

_____

Remote configuration MUST only be allowed with an encrypted and (server-) authenticated connection according to [TR-02102-2], Section 3, or other techniques fulfilling the same security requirements.

The applicant MUST provide information about the implementation details. If no strict conformance to [TR-02102-2] is claimed the "other technique fulfilling the same security requirements" MUST be described in detail. In this case the same level of detail according to [TR-02102-2] is required.

(answer) _____

_____

_____

The applicant MUST list all identifiers of private cryptographic keys and secrets used in the *factory setting* and *initialized* state by any remote configuration functionality. A statement is necessary how these key(s) or secrets are generated and whether these key(s) or secrets are shared by multiple DUTs.

state	identifier of private keys or secrets	generated by/ unique per DUT	remote configuration functionality
[*initialized*]			
[*factory*]			

Table 24: Remote configuration functionalities

3.14 Module L - Voice over IP (VoIP)

No questions for the Implementation Conformance Statement.

3.15 Module M - Virtual Private Network (VPN)

If the DUT supports VPN functionalities as client or server, the applicant MUST provide information about the implementation details. Please refer to software used (e.g. open source, proprietary) and technical documentation.

(answer) _____
_____
_____

The applicant MUST list all identifiers of private cryptographic keys and secrets used in the *factory setting* and *initialized* state by any VPN functionality of the DUT. A statement is necessary how these key(s) or secrets are generated and whether these key(s) or secrets are shared by multiple DUTs.

state	identifier of private keys or secrets	generated by/ unique per DUT	VPN functionality
[*customized*]			
[*initialized*]			
[*factory*]			

Table 25: VPN cryptographic keys and secrets

4 Test Cases

This Section defines test cases by referring to a Test Requirement defined in [BSI TR-03148] and defining a Test Procedure to verify conformance to the corresponding requirement. The requirements and procedures are labeled using the following scheme:

TR.[Module].[RequirementNumber] = Test **Requirement** [BSI TR-03148]

TP.[Module].[RequirementNumber].[TestNumber] = Test **Procedure**

Rating of Test Requirements and Test Procedures

PASS	Test evidence does support the assertions of the applicant and/ or manufacturer. The tests performed by the tester demonstrate that the respective Test Procedure is fulfilled. The tester considered all aspects of the Criteria to PASS.
FAIL	One single aspect of a Test Procedure fails or could not be verified. Therefore the complete Test Procedure and the respective Test Requirement is rated FAIL.
INCONCLUSIVE	This test verdict is given when the test result is such that neither a PASS nor a FAIL verdict can be given. For example: the tester needs further details of the implementation (e.g. documentation, source code, special test setup) to finalize his assessment but did not receive these details from the applicant or manufacturer.
NOT APPLICABLE	The tester is able to follow the argumentation of the applicant and/ or manufacturer that the respective Test Requirement is not relevant for the specific implementation of the DUT. In this case the tester MUST provide a detailed analysis and argumentation to support the rating. If the DUT does not support features which MAY be implemented the explanation might be short (e.g. DUT does not support community WLAN).

Functional Testing

Test Procedures (TP.[Module].[TestNumber]) that are described with formulations like “the tester performs functional testing” or “by functional testing” do not explicitly require specific test tools and test steps using these tools. It is up to the tester to use his/ her expertise and tools to validate conformance to the specific Test Procedures. The test report MUST detail the used tools and the specific functional tests the tester performed. The test evidence MUST be provided.

Remark concerning the DUTs state *initialized*

Several Test Procedures require testing in the *initialized* state. While performing several of those tests the DUT may more and more change to the *customized* state. It is important that the tester is convinced that the DUT is in the *initialized* state if required for testing. If previous tests could have an impact on further testing in the *initialized* state the tester MUST reset the DUT to *factory setting* and perform a new initialization to change to *initialized* again. The tester MUST verify that after resetting the DUT to *factory setting* the DUT is configured as by delivery by the applicant (e.g. firmware version, configuration).

Keywords

Both the Technical Guideline (BSI TR-03148) and this Test Specification make use of the following keywords as defined in [IETF RFC 2119]. The keywords “CONDITIONAL” and “IF” mean that the usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED.

Some notes provide further clarification for the testers.

MUST	*"This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification." [IETF RFC 2119]* Note: A "**MUST"** Test Requirement has to be assessed by the tester. If a single Test Procedure of this Requirement could not be verified with a PASS verdict the complete Test Requirement has to be rated as FAIL. In this case the DUT does not pass the complete test.
MUST NOT	*"This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification." [IETF RFC 2119]*
SHOULD	*"This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course." [IETF RFC 2119]* Note: Without further clarification by the applicant a "**SHOULD**" Test Requirement has to be assessed by the tester. If a single Test Procedure of this Requirement could not be verified with a PASS verdict the complete Test Requirement has to be rated as FAIL. In this case the DUT does not pass the complete test. In cases where the DUT obviously does not comply with a "SHOULD" Test Requirement, the applicant is free to submit a statement within the ICS (e.g. using Table 5) to provide further details of the DUTs implementation or behaviour. The tester has to verify the applicants statement in the context of the Test Requirement. A detailed assessment is necessary to verify solutions which (partly) do not comply with the Test Requirement. The tester has to provide detailed test evidence in the test report.
SHOULD NOT	*"This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label." [IETF RFC 2119]*
MAY	*"This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.* *An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)" [IETF RFC 2119]* Note: Only the "MAY" Requirements of the Technical Guideline (BSI TR-03148), which require specific implementations (e.g. additional "MUSTs", "SHOULDs" or "IFs") are part of this Test Specification (e.g. *"Personal Identification Number (PIN) based WPS* **MAY** *only be used,* **IF** *the feature is deactivated in the initialized state and a new PIN is generated for each newly registered device."*). A "**MAY"** Test Requirement is optional. The applicant is free to indicate this Test Requirement as Not Applicable (e.g. using Table 5). The tester has to verify the statement of the applicant and has to provide details in the test report (e.g. the applicant state "the DUT does not support PIN based WPS", the tester has to verify this statement). If a "MAY" Test Requirement is not indicated as Not Applicable, the tester has to assess this Requirement. If a single Test Procedure of this Requirement could not be verified with a PASS verdict the complete Test Requirement has to be rated as FAIL. In this case the DUT does not pass the complete test.

Table 26: Keywords

4.1 Module A - Private Network

TR.A.1 **A DUT MUST offer a Local Area Network (LAN) or WLAN interface to offer access to the Internet for the local user devices in the private network.**

TP.A.1.1 The tester verifies the assertions of the applicant given in Table 6, Private Network Interfaces and services of the DUT, to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 6, Private Network Interfaces and services of the DUT, is consistent with the user guidance.

TP.A.1.2 Following the user guidance the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*.

If more than one procedure is available to set the DUT into operation all procedures MUST be verified (e.g. web interface, mobile app, telnet, ssh).

If the procedure of setting the DUT into operation is not consistent with the procedure described in the user guidance this MUST be addressed in the test report.

Criteria to Pass

This Test Procedure is successfully passed, if the procedure of setting the DUT into operation is consistent with the procedure described in the user guidance.

TP.A.1.3 The tester verifies in *initialized* state for each identified interface of the private network offering access to the Internet the basic functionality.

The local user device (e.g. test system) in the private network segment MUST have full internet access.

Implementations, where the offered access to the Internet is limited in *initialized* state but full internet access could be permitted by a configuration option of the DUT are acceptable. In this case the test must be performed with enabled full internet access for the respective interface of the private network.

The tester verifies this Test Procedure by functional testing using typical internet protocols like IPv4, IPv6 or ICMP. In addition the internet access is verified by using typical application layer protocols like DNS, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), HTTPS, SMTP (Simple Mail Transfer Protocol), SSH (Secure Shell) and/ or Telnet.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not find any limitations of the internet access according to the tests specified above. Each identified interface of the private network offering access to the Internet must be assessed.

TR.A.2 **In *factory setting* the DUT SHOULD restrict access to a defined list of services provided to devices connected on the LAN and WLAN interface by the DUT.**

TP.A.2.1 Following TP.A.1.1 the tester summarizes for each identified interface of the **private network** all services provided by the DUT in *factory setting*. The tester verifies this to be consistent with the user guidance.

This Test Procedure depends on the DUTs state *factory setting*.

The services are provided on one or more dedicated TCP and/ or UDP ports or by the network stack itself.

Criteria to Pass

This Test Procedure is successfully passed, if the list of services provided by the DUT in factory setting to devices connected on the LAN and WLAN interface is a defined listing. This list MUST be consistent with the user guidance.

TP.A.2.2 In *factory setting* the tester performs service/ port scans for each identified interface of the **private network** to identify services offered by the DUT.

This Test Procedure depends on the DUTs state *factory setting*.

These scans MUST include techniques to detect protocols of the Internet layer, Transport layer and Application layer.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the service/ port scans are consistent with the results of TP.A.2.1 for the *factory setting* state.

TR.A.3 **Only a minimal selection of services SHOULD be available on the LAN and WLAN interface of the DUT.**

TP.A.3.1 Following TP.A.1.1 the tester summarizes for each identified interface of the private network all services provided by the DUT in all states. The tester verifies this to be consistent with the user guidance.

The services are provided on one or more dedicated TCP and/ or UDP ports or by the network stack itself.

An example of a list of minimal services may be found in [TR-03148], Table 3, Common services offered to the private network by the router. They are needed for the Internet gateway and network management functionality of the DUT. They allow the connected user devices to access the Internet through the DUT and to communicate with one another.

Services which SHOULD NOT be available on the DUTs interfaces of the private network in *factory setting* or *initialized* are for example the services for FTP, Mailserver, Mediaserver, NAS (network attached storage), Printserver, Remote Control, Smart Home or VPN.

Criteria to Pass

This Test Procedure is successfully passed, if the list of all services provided by the DUT in all states is minimal. This list MUST be consistent with the user guidance.

TP.A.3.2 In *initialized* the tester performs service/ port scans for each identified interface of the private network to identify services offered by the DUT.

These scans MUST include techniques to detect protocols of the Internet layer, Transport layer and Application layer.

To identify services for filesharing the tester has to connect an USB MSD (mass storage device) and an USB printer to the DUT before booting the device. Some implementations do not start filesharing services without detection of such devices during system start.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the service/ port scans are consistent with the results of TP.A.3.1 for the *initialized* state.

TR.A.4 All services provided by the DUT MUST be documented by the manufacturer including the port(s) or port ranges used.

TP.A.4.1 The tester verifies the assertions of the applicant for the services and client software of the DUT for the **private network** given in

- Table 6, Private Network Interfaces and services of the DUT and
- Table 7, Private Network Interfaces and client software of the DUT

to be consistent with the user guidance.

This Test Procedure does not depend on the DUTs state.

It is recommended to complete this Test Procedure at the end of the DUT's assessment. In doing so the tester is more familiar with the services provided by the DUT.

The documentation in the user guidance MUST include the port(s) or port ranges of the services. In addition the client services SHOULD be documented. All service and client software implementations are in focus.

Criteria to Pass

This Test Procedure is successfully passed, if the tester found no inconsistencies between the user guidance and the ICS (in detail Table 6 and 7).

TP.A.4.2 The tester verifies that the list of services and client software of the DUT for the **private network** is consistent with the documentation.

This Test Procedure does not depend on the DUTs state.

It is recommended to complete this Test Procedure at the end of the DUT's assessment. In doing so the tester is more familiar with the services provided by the DUT.

The assessment MUST include the port(s) or port ranges of the services. In addition the client services SHOULD be part of the test. All service and client software implementations are in focus.

When performing all the Test Procedures the tester creates a list of all services and client software including the port(s) or port ranges of the services. This list represents the implementation of the DUT verified by the tester. Services and client software identified during testing are noted in this list by the tester.

Criteria to Pass

This Test Procedure is successfully passed, if the tester found no inconsistencies between the implementation and the user guidance. The list of services and client software created by the tester MUST be consistent with the user guidance.

TR.A.5 **If one of the service offered by the DUT is deactivated during operation of the DUT the corresponding port(s) MUST be closed.**

TP.A.5.1 The tester verifies by functional testing for each service offered by the DUT for the **private network** that the corresponding port(s) is/ are closed as soon as the corresponding service is deactivated.

This Test Procedure does not depend on the DUTs state.

Open ports can be detected by port scanners (e.g. nmap, ICMP port unreachable message). To verify services based on connection-less protocols the tester could also use port scanners for well-known applications but could also use the application of the sender trying to re-connect to the DUT. If a re-connection is not possible the connection-less service of the DUT seems to be deactivated. This MUST always be verified by sniffing and analyzing the communication (e.g. tcpdump, wireshark) between sender and DUT during such a re-connection attempt.

Criteria to Pass

This Test Procedure is successfully passed, if no port(s) of a corresponding service offered by the DUT is detectable after this service is deactivated. All services offered by the DUT are in focus.

4.1.1 Local Area Network (LAN) Interfaces

No dedicated security requirements are defined for access to the cable connected (wired) LAN interface itself.

4.1.2 WLAN Interfaces

Security measures for the usage of WLAN MUST be implemented by the DUT to prevent attackers from gaining access to resources within the private network of the end-user, to the public network through the DUT and its gateway functionality and configuration of the DUT.

TR.A.6 **The WLAN interface MUST at least be implemented according to [IEEE 802.11i].**

According to [TR-03148] three different types of WLAN networks are in focus: private WLAN, guest WLAN and community WLAN. The following Test Procedures depend on these types.

TP.A.6.1 The tester verifies the assertions of the applicant given in Section 3.3.2. A statement of the DUT manufacturer MUST declare the compatibility of the WLAN interface(s) according to [IEEE 802.11i] at least.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

More up-to date encryption methods like WPA3 are also accepted.

The DUT MAY support WEP encryption. If WEP encryption is supported, WPA2 MUST be set as default encryption method for all preset WLAN profiles at least. The functional test is required by TR.A.9.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able verify the assertions of the applicant.

4.1.2.1 Private WLAN

In addition to the private WLAN, which MUST fulfill the requirements described in the following Sections the DUT MAY offer a user-configured guest WLAN, which SHOULD fulfill these requirements as well (refer to Section 4.1.2.2).

In addition to the private WLAN and the user-configured guest WLAN the DUT MAY offer a WLAN used by a larger user group (e.g. wireless community network/HotSpot, community WLAN). Requirements for community WLANs are specified in Section 4.1.2.3).

TR.A.7 **In *factory setting* the Extended Service Set Identifier (ESSID) SHOULD NOT contain any information that consists of or is derived from data or parts of data that depend on the DUT model itself.**

TP.A.7.1 In *factory setting* the tester verifies by functional testing that the ESSID does not contain information that consists of or is derived from data or parts of data that depend on the DUT model itself (e.g. model name).

This Test Procedure depends on the DUTs state *factory setting*.

After booting the DUT from *factory setting* the tester captures the ESSID. The information contained in this ESSID should not reveal the DUT model or DUT hardware family.

The tester should also verify public available resources (e.g. internet forum, vendor/ manufacturer support) that there exist no mappings between the ESSID and the DUT model or DUT hardware family. Some mappings might not be obviously, e.g. model or family codes.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information contained in the ESSID does not reveal the DUT model or DUT hardware family.

TR.A.8 **The DUT MUST allow an authenticated end-user to change the ESSID.**

TP.A.8.1 In *initialized* the tester uses one of the access methods listed in Section 3.6, Table 13, to configure the DUT. After successful authentication by the used access method the tester changes the configuration of the current used private WLAN access profile. The ESSID of this profile MUST be editable to a different value chosen by the tester.

This Test Procedure depends on the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to change the ESSID of the current private WLAN using one of the access methods listed in Section 3.6, Table 13, to configure the DUT.

TP.A.8.2 The tester verifies the change of the ESSID of the private WLAN by functional testing.

This Test Procedure depends on the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if functional testing shows the effectiveness of the ESSID change.

TR.A.9 The DUT MUST support encryption according to Wi-Fi Protected Access II (WPA2) based on [IEEE 802.11i] or more up to date versions for every private or guest WLAN.

TP.A.9.1 The tester performs a review of the user guidance. WPA2 MUST be addressed as configuration option for private and if supported for guest WLAN profiles.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to identify WPA2 as a configuration option for private and if supported for guest WLAN profiles in the user guidance.

TP.A.9.2 In *initialized* the tester verifies the configuration options for private and if supported for guest WLAN profiles using one of the access methods listed in Section 3.6, Table 13. These profiles MUST provide an option to choose WPA2 as a security standard.

This Test Procedure depends on the DUTs states *initialized* and *customized.*

The tester verifies that WPA2-Personal using PSK is a configuration option for user authentication.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to configure WPA2 as a security standard for private and if supported for guest WLAN.

TP.A.9.3 The tester verifies the WPA2 support for private and if supported for guest WLAN profiles by functional testing.

This Test Procedure depends on the DUTs states *initialized* and *customized.*

Criteria to Pass

This Test Procedure is successfully passed, if functional testing demonstrates that WPA2 can be used for private and if supported for guest WLAN. If supported by the DUT, all three WLAN frequencies (2.4 GHz, 5 GHz and 60 GHz) MUST be tested using a WLAN sniffer.

TP.A.9.4 If the DUT supports WEP encryption, the tester verifies by functional testing that WPA2 is the default encryption method for all preset private and if supported guest WLAN profiles.

This Test Procedure depends on the DUTs states *factory setting* and *initialized.*

More up-to date encryption methods like WPA3 are also accepted.

Criteria to Pass

This Test Procedure is successfully passed, if functional testing demonstrates that WPA2 is the default encryption method for all preset private and if supported guest WLAN profiles.

TR.A.10 If WLAN is activated in *factory setting* the supported encryption MUST be activated in *factory setting*.

TP.A.10.1 The tester performs a review of the user guidance. If WLAN is activated in *factory setting* WPA2 MUST be addressed as active encryption standard.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to identify WPA2 as active encryption standard in the user guidance.

TP.A.10.2 If WLAN is active in *factory setting* the tester verifies by functional testing that WPA2 is used.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could verify by functional testing that WPA2 is used for all WLANs of the DUT in *factory setting*. All three WLAN frequencies (2.4 GHz, 5 GHz and 60 GHz) MUST be tested using a WLAN sniffer.

TR.A.11 The passphrase (pre-shared key, PSK) configured in *factory setting* SHOULD have a length of at least 20 digits and MUST NOT contain information that consists of or is derived from data or parts of data that depend on the DUT itself.

TP.A.11.1 The tester verifies by functional testing in *factory setting* that the PSKs for all active WLAN networks have a length of at least 20 digits.

This Test Procedure depends on the DUTs states *factory setting.*

Criteria to Pass

This Test Procedure is successfully passed, if the tester could verify by functional testing that all pre-shared keys for all active WLAN networks have a length of at least 20 digits.

TP.A.11.2 The tester verifies by functional testing in *factory setting* that the PSKs for all active WLAN networks do not contain information that consists of or is derived from data or parts of data that depend on the DUT itself (e.g. manufacturer, model name, MAC address).

This Test Procedure depends on the DUTs states *factory setting.*

Criteria to Pass

This Test Procedure is successfully passed, if the tester could verify by functional testing that all pre-shared keys for all active WLAN networks do not contain information that consists of or is derived from data or parts of data that depend on the DUT itself.

TR.A.12 All private cryptographic keys and secrets MUST NOT be shared by multiple devices in the *factory setting* and *initialized* state.

TP.A.12.1 The tester verifies the assertions of the applicant given in Section 3.3.2, Table 9.

This Test Procedure depends on the DUTs states *factory setting* and *initialized.* It is not required for *customized*.

The applicant MUST state that no cryptographic key or secret is shared between multiple DUTs.

If the generation method for any private cryptographic key or secret is not disclosed by the applicant or manufacturer the tester MUST verify this Test Procedure using ten DUTs of the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any private cryptographic key or secret (e.g. PSK, PIN for WPS) demonstrates that the generated key value or secret is unique, except by chance.

TR.A.13 The DUT MUST allow an authenticated end-user to set the passphrase (PSK) to a different value.

TP.A.13.1 In *initialized* the tester uses one of the access methods listed in Section 3.6, Table 13, to configure the DUT. After successful authentication by the access method used the tester changes the configuration of the currently used WLAN profile.

This Test Procedure depends on the DUTs state *initialized.*

Criteria to Pass

This Test Procedure is successfully passed, if the PSK of the current WLAN profile is editable to a different value chosen by the tester.

TP.A.13.2 In *initialized* the tester performs functional testing to verify the change of the PSK for the current WLAN profile.

This Test Procedure depends on the DUTs state *initialized.*

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing the change of the PSK for the current WLAN profile.

TR.A.14 Changing the PSK SHOULD be supported by a mechanism showing the strength of the new desired PSK based on the number of digits and classes of digits with a mechanism comparable to the given example mechanism for passwords described in [TR-03148].

TP.A.14.1 The tester verifies the assertions of the applicant given in Section 3.3.2. A statement of the applicant MUST describe the mechanism showing the strength of a new desired PSK.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the implemented mechanism showing the strength of a new desired PSK is comparable to the given example mechanism for passwords described in [TR-03148].

TP.A.14.2 By changing the PSK following TP.A.13.1 the tester verifies the mechanism showing the strength of the new desired PSK by functional testing.

This Test Procedure depends on the DUTs state *initialized.*

Refer to TP.D.7.2 and TP.D.14.1 for a similar approach.

The rating of the strength SHOULD be based on a mechanism comparable to the given example mechanism for passwords described in Section 4.1.1, User Access to Configuration, of [TR-03148].

TR.A.11 requires at least 20 characters for the PSK configured in *factory setting*.

According to this given example an accepted PSK (= indication "good") MUST contain at least 20 characters, including at least two of the following kinds of characters: uppercase letters [A-Z], lowercase letters [a-z], special characters [e.g. ?, !, $, etc.] or numeric characters [0-9].

A "weak" PSK does not met the requirements above (e.g. PSK is too short, PSK only consists of numeric characters).

The mechanism can indicate a "high" PSK strength if the PSK fulfills more than at least one requirement (e.g. PSK is even longer, consists of more than 2 kinds of characters) while still fulfilling the other requirements.

All rules of the mechanism showing the strength of the new desired PSK MUST be verified by functional testing.

If one rule used to identify a "good" PSK requires that the PSK MUST be a combination of at least 2 of the following kinds of characters a) uppercase letters [A-Z], b) lowercase letters [a-z], c) special characters [e.g. ?, !, $, etc.] and d) numeric characters [0-9] the tester MUST verify all possible valid combinations ab, ac, ad, bc, bd, cd by functional testing.

Also input representing a "high" PSK or "weak" PSK MUST be tested.

In all cases the tester MUST detail the implementation and the tests performed in the test report.

Criteria to Pass

This Test Procedure is successfully passed, if the implemented mechanism showing the strength of the new desired PSK is verified by functional testing.

TR.A.15 The DUT MAY implement Wi-Fi Simple Configuration (WSC) according to [WSC]

TP.A.15.1 The tester verifies the assertions of the applicant given in Section 3.3.2. A statement of the DUT manufacturer MUST declare the implementation of WSC according to WSC2.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that WSC is implemented according to WSC2.

TP.A.15.2 If the DUT supports Wi-Fi Simple Configuration (WSC) according to [WSC2] the tester verifies the assertions of the applicant given in Table 8, WLAN features, to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 8, WLAN features, is consistent with the user guidance.

TP.A.15.3 The tester verifies by functional testing that after activation of the WPS push button functionality the device binding is only active for a limited time period.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing that for the WPS push button mode a timeout is implemented (e.g. 120 seconds). After activation of this WPS mode the functionality MUST only be active for this limited time period (timeout).

TP.A.15.4 The tester verifies by functional testing that after activation of the WPS PIN functionality (the DUT provides the PIN) the device binding is only active for a limited time period and only one device is able to connect successfully.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester verifies by functional testing that after activation of the WPS mode the functionality is only active for a limited time period (timeout, e.g. 120 seconds). In this time period only one device is able to perform a successful binding.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by

functional testing that for the WPS PIN mode where the DUT provides the PIN a timeout is implemented according to the test specified above.

TP.A.15.5 The tester verifies by functional testing that after activation of the WPS PIN functionality (the DUT provides the PIN) the device binding is protected against brute force connection attempts.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

WSC2 requires for PIN mode where the DUT provides the PIN: after 3 failed attempts within 60 seconds the PIN mode MUST be locked for 60 seconds.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing that the WPS PIN device binding mode is locked for 60 seconds if within 60 seconds three failed binding attempts occur (where the DUT provides the PIN).

TR.A.16 Personal Identification Number (PIN) based WPS MAY only be used, if the feature is deactivated in the *initialized* state and a new PIN is generated for each newly registered device.

TP.A.16.1 The tester verifies the WLAN configuration options of the DUT in *initialized* using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The current configuration shows that PIN based WPS is deactivated if supported.

This Test Procedure depends on the DUTs state *initialized*.

The tester uses one of the access methods listed in Section 3.6, Table 13, to verify the WLAN configuration options of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that PIN based WPS is deactivated.

TP.A.16.2 The tester performs functional testing to verify the configuration according to TP.A.16.1.

This Test Procedure depends on the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify using sniffing tools (e.g. WifiInfoView by Nir Sofer, WiFi Explorer by Adrian Granados, WiFi Analyzer app by farproc, wash – WiFi Protected Setup Scan Tool as part of the reaver package) that the WPS PIN mode is deactivated (status is NOT "configured", "not configured" or "locked").

TP.A.16.3 The tester performs functional testing for PIN based WPS to verify that the DUT generates a new PIN for each newly registered device.

This Test Procedure depends on the DUTs state *initialized*.

The tester uses five different devices to connect to the DUTs WLAN using PIN based WPS where the DUT provides the PIN.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify using functional testing that the DUT generates a new PIN for each newly registered device.

TP.A.16.4 TP.A.12.1 is applicable for the WPS PIN.

TR.A.17 Performing WPS based on Near Field Communication (NFC) SHOULD be deactivated in the *initialized* state.

TP.A.17.1 Following TP.A.15.2 the tester verifies the WLAN configuration options of the DUT in *initialized* using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The current configuration shows that WPS based on NFC is deactivated if supported.

This Test Procedure depends on the DUTs state *initialized*.

The tester uses one of the access methods listed in Section 3.6, Table 13, to verify the WLAN configuration options of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that WPS based NFC is deactivated.

TP.A.17.2 The tester performs functional testing to verify the configuration according to TP.A.17.1.

This Test Procedure depends on the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the DUTs WPS NFC mode is deactivated in *initialized*. The tester could use for example a mobile device supporting WLAN and WPS NFC mode to test the DUT.

4.1.2.2 Guest WLAN

TR.A.18 A user-configured guest WLAN SHOULD fulfill the requirements of a Private WLAN (refer to Section 4.1.2.1 above) as well.

TP.A.18.1 The tester verifies the assertions of the applicant given in Table 8, WLAN features, for guest WLAN to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 8, WLAN features, is consistent with the user guidance.

TP.A.18.2 The tester verifies that a user-configured guest WLAN fulfills all Test Procedures TP.A.7.1 up to TP.A.17.2 of a Private WLAN.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify the Test Procedures TP.A.7.1 up to TP.A.17.2 for the user-configured guest WLAN.

TR.A.19 The guest WLAN SHOULD be deactivated using *factory setting* and MUST NOT allow any communication with devices that are connected to the private WLAN or LAN interface.

TP.A.19.1 The tester verifies in factory setting by functional testing that the guest WLAN is deactivated.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any guest WLAN of the DUT in factory setting using a WLAN sniffer. All three WLAN frequencies (2.4 GHz, 5 GHz and 60 GHz) MUST be tested.

TP.A.19.2 The tester verifies the configuration options of the DUT by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The tester verifies that no configuration option can be used to allow communication between devices of the guest WLAN and devices of the private WLAN or LAN interface.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

If the DUT supports the functionality of a guest WLAN the configuration of this guest WLAN MUST NOT allow to activate communication between devices of the guest WLAN and devices of the private WLAN or LAN interface. The DUTs configuration features (e.g. Firewall) MUST handle the guest WLAN as a "special" WLAN segment and MUST not allow the same configuration details as for a private WLAN or LAN.

Note that all access methods listed in Section 3.6 MUST be considered. It could be that one access method has no access to all configuration details.

Criteria to Pass

This Test Procedure is successfully passed, if no configuration option could be identified by the tester to allow communication between devices of the guest WLAN and devices of the private WLAN or LAN interface.

TP.A.19.3 The tester verifies by functional testing that devices within the guest WLAN are not able to communicate with devices connected to the private WLAN or LAN interface.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

After *initialization* the tester activates the guest WLAN of the DUT. The tester verifies the intended functionality of this guest WLAN by testing the internet access of devices connected to this guest WLAN.

The IP network of the guest WLAN MUST be a different subnetwork compared to the community WLAN, private WLAN or LAN IP networks.

For all private network segments the tester verifies the following:

Test setup: One test system is used in the guest WLAN and in each active private network segment (private WLAN, private LAN) and if supported in the community WLAN. Each test system is capable to send IP Packets using a port scanner (e.g. nmap) and to sniff the local network segment using a network sniffer (e.g. tcpdump, wireshark). A network tap could be used to support testing.

Test procedure: The tester identifies possible IP network connections to be in focus for testing. These are the connections from the IP network segment of the guest WLAN to each IP network segment of a private network (private WLAN, private LAN) and if supported in the community WLAN. Focusing on these possible IP network connections, the tester

- SCANS: The tester performs port scans in both directions for each identified connection. These scans include all TCP, and SCTP ports as well as the ICMP/ ICMPv6 and ARP protocol. The destination IPs of the SCANS MUST include all IP addresses of the target network segment (e.g. 192.168.1.0/24 MUST be scanned for 254 hosts from 192.168.1.1 up to 192.168.1.254). The scan system must also send ARP packets to the destination network segment. It is expected that the DUT does not forward ARP packets between different network segment.
- The SCAN system MUST repeat all scans for three different source IP addresses, the first and last IP address of the segment and one IP address in the middle of the network segment (e.g. 192.168.1.1, 192.168.1.254 and 192.168.1.127 for the network segment 192.168.1.0/24).
- SNIFFS: While one test system is performing the SCANS all other test systems are sniffing the respective network segment. The tester verifies that no IP or ARP packets of the SCAN system are detectable in the other network segments.

Criteria to Pass

This Test Procedure is successfully passed, if no IP or ARP packet send by a SCAN system could be detected in the other network segments by following the Test Procedure defined above.

TR.A.20 The guest WLAN MUST NOT allow access to the configuration of the DUT.

TP.A.20.1 The tester verifies the configuration options of the DUT by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The tester verifies that no configuration options can be used to allow access to the configuration of the DUT from the guest WLAN interface.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

If the DUT supports the functionality of a guest WLAN the configuration of this guest WLAN MUST NOT allow to access any access method listed in Section 3.6, Table 13, to configure the DUT from any device within the guest WLAN.

Note that all access methods listed in Section 3.6 MUST be considered. It could be that one access method has no access to all configuration details.

Criteria to Pass

This Test Procedure is successfully passed, if no configuration option could be identified by the tester to allow access to the configuration of the DUT from any device within the guest WLAN.

TP.A.20.2 The tester verifies by functional testing that devices within the guest WLAN are not able to communicate with one of the access methods listed in Section 3.6, Table 13.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

After *initialization* the tester activates the guest WLAN of the DUT. The tester verifies the intended functionality of this guest WLAN by testing the internet access of devices connected to this guest WLAN.

Using a test system within the guest WLAN the tester tries to connect to/ scan each access method listed in Section 3.6, Table 13, to configure the DUT.

To detect if an access method of the DUT allows to configure the DUT from a device within the guest WLAN it is sufficient that the access method respond to

the IP communication of the test system. The port(s) of the access method MUST be closed on the DUTs IP interface of the guest WLAN.

The test system MUST repeat all connection attempts/ scans for three different source IP addresses, the first and last IP address of the segment and one IP address in the middle of the network segment (e.g. 192.168.1.1, 192.168.1.254 and 192.168.1.127 for the network segment 192.168.1.0/24).

Criteria to Pass

This Test Procedure is successfully passed, if the tester could verify that no access method listed in Section 3.6, Table 13, to configure the DUT is available from a device within the guest WLAN following the Test Procedure defined above.

4.1.2.3 Community WLAN

TR.A.21 A community WLAN MUST be restricted to allowing Internet Access to the devices connected to this WLAN. Connection to other devices connected to the LAN interface, private WLAN or guest WLAN MUST NOT be allowed by the DUT.

TP.A.21.1 The tester verifies the assertions of the applicant given in Table 8, WLAN features, for community WLAN to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 8, WLAN features, is consistent with the user guidance.

TP.A.21.2 The tester verifies the configuration options of the DUT by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The tester verifies that no configuration option can be used to allow communication between devices of the community WLAN and devices connected to the LAN interface, private WLAN or guest WLAN and between devices connected to the community WLAN.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

A device connected to the community WLAN is only allowed to use the DUTs Internet Access.

If the DUT supports the functionality of a community WLAN the configuration of this community WLAN MUST NOT allow to activate communication between devices of the community WLAN and devices of the private WLAN, LAN interface or guest WLAN and between the devices connected to the community WLAN. The DUTs configuration features (e.g. Firewall) MUST handle the community WLAN as a "special" WLAN segment and MUST not allow the same configuration details as for a private WLAN or LAN.

Note that all access methods listed in Section 3.6 MUST be considered. It could be that one access method has no access to all configuration details.

Criteria to Pass

This Test Procedure is successfully passed, if no configuration option could be identified by the tester to allow communication between devices of the community WLAN and devices of the private WLAN, LAN interface or guest WLAN and between the devices connected to the community WLAN.

TP.A.21.3 The tester verifies by functional testing that communication of devices within the community WLAN is restricted to allowing Internet Access.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

A device connected to the community WLAN is only allowed to use the DUTs Internet Access.

After *initialization* the tester activates the community WLAN and if supported the guest WLAN of the DUT. The tester verifies the intended functionality of this community WLAN and if supported of the guest WLAN by testing the internet access of devices connected to this community WLAN and if supported to the guest WLAN.

The IP network of the community WLAN MUST be a different subnetwork compared to the guest WLAN, private WLAN or LAN IP networks.

For all private network segments and if supported for the guest WLAN segment(s) the tester verifies the following:

Test setup: Two test systems are used in the community WLAN and one system in each active private network segment (private WLAN, private LAN) and if supported in the guest WLAN. Each test system is capable to send IP Packets using a port scanner (e.g. nmap) and to sniff the local network segment using a network sniffer (e.g. tcpdump, wireshark). A network tap could be used to support testing.

Test procedure: The tester identifies possible IP network connections to be in focus for testing. These are

- the connections from the IP network segment of the community WLAN to each IP network segment of a private network (private WLAN, private LAN) and if supported of a guest WLAN.
- direct communication between devices of the community WLAN.

Focusing on these possible IP network connections, the tester

- SCANS: The tester performs port scans in both directions for each identified connection. These scans include all TCP, UDP and SCTP ports as well as the ICMP/ ICMPv6 and ARP protocol. The destination IPs of the SCANS MUST include all IP addresses of the target network segment (e.g. 192.168.1.0/24 MUST be scanned for 254 hosts from 192.168.1.1 up to 192.168.1.254). The scan system must also send ARP packets to the destination network segment. It is expected that the DUT does not forward ARP packets between different network segment.
- The SCAN system MUST repeat all scans for three different source IP addresses, the first and last IP address of the segment and one IP address in the middle of the network segment (e.g. 192.168.1.1, 192.168.1.254 and 192.168.1.127 for the network segment 192.168.1.0/24).
- SNIFFS: While one test system is performing the SCANS all other test systems are sniffing the respective network segment. The tester verifies that no IP or ARP packets of the SCAN system are detectable in the other network segments.

The tester verifies that between devices of the community WLAN no communication is possible.

Criteria to Pass

This Test Procedure is successfully passed, if no IP or ARP packet send by a SCAN system could be detected in the other network segments by following the Test Procedure defined above.

TR.A.22 The community WLAN MUST NOT allow access to the configuration of the DUT.

TP.A.22.1 The tester verifies the configuration options of the DUT by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. The tester verifies that no configuration options can be used to allow access to the configuration of the DUT from the community WLAN interface.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

If the DUT supports the functionality of a community WLAN the configuration of this community WLAN MUST NOT allow to access any access method listed in Section 3.6, Table 13, to configure the DUT from any device within the community WLAN.

Note that all access methods listed in Section 3.6 MUST be considered. It could be that one access method has no access to all configuration details.

Criteria to Pass

This Test Procedure is successfully passed, if no configuration option could be identified by the tester to allow access to the configuration of the DUT from any device within the community WLAN.

TP.A.22.2 The tester verifies by functional testing that devices within the community WLAN are not able to communicate with one of the access methods listed in Section 3.6, Table 13.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

After *initialization* the tester activates the community WLAN of the DUT. The tester verifies the intended functionality of this community WLAN by testing the internet access of devices connected to this community WLAN.

Using a test system within the community WLAN the tester tries to connect to/ scan each access method listed in Section 3.6, Table 13, to configure the DUT.

To detect if an access method of the DUT allows to configure the DUT from a device within the community WLAN it is sufficient that the access method respond to the IP communication of the test system. The port(s) of the access method MUST be closed on the DUTs IP interface of the community WLAN.

The test system MUST repeat all connection attempts/ scans for three different source IP addresses, the first and last IP address of the segment and one IP address in the middle of the network segment (e.g. 192.168.1.1, 192.168.1.254 and 192.168.1.127 for the network segment 192.168.1.0/24).

Criteria to Pass

This Test Procedure is successfully passed, if the tester could verify that no access method listed in Section 3.6, Table 13, to configure the DUT is available from a device within the community WLAN following the Test Procedure defined above.

4.2 Module B - Public Network

TR.B.1 **The requirements to the corresponding WAN interface MUST be fulfilled by all instances of the interface in scenarios where the DUT is connected to more than one Internet Service.**

TP.B.1.1 If the DUT is connected to more than one Internet Service by different WAN interfaces the tester verifies that for all WAN interfaces the corresponding Test Requirements are fulfilled.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify for all WAN interfaces (e.g. Cable, xDSL, FTTH, LTE) all Test Requirements of this Module B - Public Network.

External WAN interfaces (e.g. USB LTE Sticks), which could be configured for alternative Internet access and which are not subject of the statements of the applicant in the ICS, are out of scope.

TR.B.2 **Only a minimal selection of services MUST be available to the public network.**

TP.B.2.1 The tester verifies the assertions of the applicant given in Table 10, Public Network Interfaces and services of the DUT, to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 10, Public Network Interfaces and services of the DUT, is consistent with the user guidance.

TP.B.2.2 Following TP.B.2.1 the tester summarizes for each identified interface of the public network all services provided by the DUT in all states. The tester verifies this to be a minimal selection of services.

This Test Procedure depends on all states of the DUT.

Services contained in the minimal selection may be found in [TR-03148], Table 4, Common services offered to the public network by the router.

For services listed and not included in [TR-03148], Table 4, Common services offered to the public network by the router, a strong justification by the applicant/ manufacturer is needed to clarify the necessity of the service.

In this case the tester MUST assess the justification and provide his own conclusion.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the list of services provided by the DUT contains only absolutely necessary services.

TP.B.2.3 In *factory setting* and *initialized* the tester performs service/ port scans for each identified interface of the public network. The results MUST be consistent with the results of TP.B.2.1.

This Test Procedure depends on all states of the DUT.

These scans MUST include techniques to detect protocols of the Internet layer, Transport layer and Application layer.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the service/ port scans are consistent with the results of TP.B.2.1.

TR.B.3 The services used for Voice over IP (V telephony MUST only be available if the DUT is already configured to use VoIP. If VoIP is deactivated on the DUT these services MUST not be available.

TP.B.3.1 Following the user guidance the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*. After this initialization the tester verifies the service status for VoIP by functional tests including port scans.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester performs port scans for all active private and public interfaces of the DUT. These scans include all ports of the VoIP services implemented in the DUT (e.g. 5060 UDP and TCP, 5061 TCP). Services and corresponding ports MUST be listed in the ICS, Table 6, "Private Network Interfaces and services of the DUT", and Table 10, "Public Network Interfaces and services of the DUT".

The tester verifies in addition the configuration options for VoIP by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the functional testing and the verification of the DUTs configuration demonstrate, that

- if during the initialization VoIP is configured for further use the corresponding services/ port(s) are present.
- if VoIP is not configured during this initialization step the services/ port(s) used for VoIP are not present.

TP.B.3.2 Using a DUT with activated and functional VoIP services the tester deactivates these VoIP services using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. After successful deactivation of these services the tester verifies by functional testing that no VoIP service is accessible and all corresponding TCP/ UDP ports are closed on all interfaces.

This Test Procedure depends on the DUTs state *initialized*.

By performing the tests required by TP.B.3.1 the tester is aware of the specific VoIP services of the DUT (e.g. open ports). Using this knowledge the tester can concentrate further testing (e.g. port scans) to these services.

Criteria to Pass

This Test Procedure is successfully passed, if the open ports of the DUTs VoIP services are closed on all private and public interfaces after deactivation of these services.

TR.B.4 The services used for remote configuration MUST only be available if the DUT is configured to use remote configuration. If remote configuration is deactivated on the DUT these services MUST not be available.

TP.B.4.1 Following the user guidance the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*. After this initialization the tester verifies the service status for remote configuration by functional tests including port scans.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester performs port scans for all active public interfaces of the DUT. These

scans include all ports of the remote configuration services implemented in the DUT (e.g. 80 TCP, 443 TCP, 7547 TCP/ UDP, 8080 TCP, 8089 TCP). Services and corresponding ports MUST be listed in the ICS, Table 10, "Public Network Interfaces and services of the DUT".

The tester verifies in addition the configuration options for remote configuration by using one of the access methods listed in Section 3.6, Table 13, to configure the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the functional testing and the verification of the DUTs configuration demonstrate, that

- if during the initialization remote configuration is configured for further use the corresponding services/ port(s) are present.
- if remote configuration is not configured during this initialization step the services/ port(s) used for remote configuration are not present.

TP.B.4.2 Using a DUT with activated and functional remote configuration services the tester deactivates these remote configuration services using one of the access methods listed in Section 3.6, Table 13, to configure the DUT. After successful deactivation of these services the tester verifies by functional testing that no remote configuration service is accessible and all corresponding TCP/ UDP ports are closed on all interfaces.

This Test Procedure depends on the DUTs state *initialized*.

By performing the tests required by TP.B.4.1 the tester is aware of the specific services for remote configuration of the DUT (e.g. open ports). Using this knowledge the tester can concentrate further testing (e.g. port scans) to these services.

Criteria to Pass

This Test Procedure is successfully passed, if the open ports of the DUTs remote configuration services are closed on all private and public interfaces after deactivation of these services.

TR.B.5 All services provided by the DUT MUST be documented by the manufacturer including the port(s) or port ranges used.

TP.B.5.1 The tester verifies the assertions of the applicant for the services and client software of the DUT for the **public network** given in

- Table 10, Public Network Interfaces and services of the DUT and
- Table 11, Public Network Interfaces and client software of the DUT

to be consistent with the user guidance.

This Test Procedure does not depend on the DUTs state.

It is recommended to complete this Test Procedure at the end of the DUT's assessment. In doing so the tester is more familiar with the services provided by the DUT.

The documentation in the user guidance MUST include the port(s) or port ranges of the services. In addition the client services SHOULD be documented. All service and client software implementations are in focus.

Criteria to Pass

This Test Procedure is successfully passed, if the tester found no inconsistencies between the user guidance and the ICS (in detail Table 10 and 11).

TP.B.5.2 The tester verifies that the list of services and client software of the DUT for the **public network** is consistent with the documentation.

This Test Procedure does not depend on the DUTs state.

It is recommended to complete this Test Procedure at the end of the DUT's assessment. In doing so the tester is more familiar with the services provided by the DUT.

The assessment MUST include the port(s) or port ranges of the services. In addition the client services SHOULD be part of the test. All service and client software implementations are in focus.

When performing all the Test Procedures the tester creates a list of all services and client software including the port(s) or port ranges of the services. This list represents the implementation of the DUT verified by the tester. Services and client software identified during testing are noted in this list by the tester.

Criteria to Pass

This Test Procedure is successfully passed, if the tester found no inconsistencies between the implementation and the user guidance. The list of services and client software created by the tester MUST be consistent with the user guidance.

TR.B.6 If one of the services offered by the DUT is deactivated during operation of the DUT the corresponding port(s) MUST be closed.

TP.B.6.1 The tester verifies by functional testing for each service offered by the DUT for the **public network** that the corresponding port(s) is/ are closed as soon as the corresponding service is deactivated.

This Test Procedure does not depend on the DUTs state.

Open ports can be detected by port scanners (e.g. nmap, ICMP port unreachable message). To verify services based on connection-less protocols the tester could also use port scanners for well-known applications but could also use the application of the sender trying to re-connect to the DUT. If a re-connection is not possible the connection-less service of the DUT seems to be deactivated. This MUST always be verified by sniffing and analyzing the communication (e.g. tcpdump, wireshark) between sender and DUT during such a re-connection attempt.

Criteria to Pass

This Test Procedure is successfully passed, if no port(s) of a corresponding service offered by the DUT is detectable after this service is deactivated. All services offered by the DUT are in focus.

4.2.1 Wide Area Network (WAN) Interfaces

TR.B.7 **After *initialization* the DUT MUST have access to an Internet Service provided by an Internet Access Provider (IAP) through a Wide Area Network (WAN) interface.**

TP.B.7.1 The tester verifies the assertions of the applicant given in Table 10, Public Network Interfaces and services of the DUT, to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 10, Public Network Interfaces and services of the DUT, is consistent with the user guidance.

TP.B.7.2 Following the user guidance the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*. The tester observes the mechanism of the DUT to gain access to the global Internet infrastructure.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

If more than one procedure is available to set the DUT into operation all procedures MUST be verified (e.g. web interface, mobile app, telnet, ssh).

The access methods listed in Section 3.6, Table 13, to configure the DUT MUST provide a status of the DUT's option to have access to the global Internet infrastructure (e.g. Internet online/ offline).

Criteria to Pass

This Test Procedure is successfully passed, if the mechanism of the DUT to gain access to the global Internet infrastructure is described in user guidance and this description is consistent with the observations of the tester.

TP.B.7.3 The tester verifies by functional testing in *initialized* that the DUT has access to an Internet Service provided by an Internet Access Provider (IAP) through a Wide Area Network (WAN) interface.

This Test Procedure depends on the DUTs state *initialized*.

By using one of the access methods listed in Section 3.6, Table 13, to configure the DUT, the tester verifies by functional testing that the DUT has access to the global Internet infrastructure. If implemented, the tester can use the DUT's test or diagnostic features (e.g. ping test).

The status of the DUT to indicate possible access to the global Internet infrastructure (e.g. Internet online/ offline) MUST be consistent with the observations by functional testing.

Note that this Test Procedure is applicable for the DUT itself, not for devices connected to any private network.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT has access to the global Internet infrastructure.

TR.B.8 **After *initialization* the DUT MUST restrict access on the WAN interface to a defined list of services provided by the DUT.**

TP.B.8.1 Following TP.B.2.1 the tester summarizes for each identified interface of the **public network** all services provided by the DUT. The tester verifies this to be consistent with the user guidance.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The services are provided on one or more dedicated TCP and/ or UDP ports or by the network stack itself.

An example of a list of minimal services may be found in [TR-03148], Table 4, Common services offered to the public network by the router. They are needed for the Internet access functionality of the DUT and additional services such as VoIP. They allow the DUT to connect to the IAPs infrastructure.

Criteria to Pass

This Test Procedure is successfully passed, if the list of services provided by the DUT on any WAN interface is limited to a defined list of services. This list MUST be consistent with the user guidance.

TP.B.8.2 In *initialized* the tester performs service/ port scans for each identified interface of the **public network** to identify services offered by the DUT.

These scans MUST include techniques to detect protocols of the Internet layer, Transport layer and Application layer.

Criteria to Pass

This Test Procedure is successfully passed, if the results of the service/ port scans are consistent with the results of TP.B.8.1 for the initialized state.

4.3 Module C - Functionalities

TR.C.1 **Functionalities, which are deactivated as a *factory setting* MUST be made transparent to the end-user IF they become activated during initialization.**

TP.C.1.1 The tester verifies the assertions of the applicant given in Table 12, Functionalities of the DUT, to be consistent with the user guidance.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the information given in Table 12, Functionalities of the DUT, is consistent with the user guidance.

TP.C.1.2 The tester verifies that each identified functionality is made transparent to the end-user in case of activation during initialization.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester creates a list of all functionalities of the DUT, which are deactivated in *factory setting* and become activated during initialization. Only those functionalities are in focus, which offer a service on an interface of the public or private network (e.g. open TCP/ UDP port).

The tester performs port-scans in *factory setting* for all public and private network interfaces. These scans are intended to identify functionalities which offer a service on an interface in the DUTs state *factory settings*.

Following the user guidance the tester then sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*. If more than one procedure is available to set the DUT into operation all procedures MUST be verified (e.g. web interface, mobile app, telnet, ssh).

During this initialization process the tester observes the behavior of the DUT. The tester verifies that during the initialization mechanism and/ or later in *initialized* the access method(s) provide(s) information about activation of functionalities to the end-user (e.g. overview of the DUTs status).

After this step the tester performs again port-scans in *initialized* for all public and private network interfaces. These scans are intended to identify functionalities which offer a service on an interface in the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that each functionality activated during initialization is made transparent to the end-user during the activation process or later in initialized using an access methods listed in Section 3.6, Table 13, to configure the DUT. Functional testing using port scanners support the tester to identify functionalities which are not made transparent to the end-user.

TR.C.2 Functionalities MUST NOT be hidden from the end-user.

TP.C.2.1 Using the information collected in TP.C.1.1 and TP.C.1.2, the tester verifies that all functionalities are described in the user guidance.

This Test Procedure depends on all states of the DUT.

It is recommended to complete this Test Procedure at the end of the DUT's assessment. In doing so the tester is more familiar with the functionalities provided by the DUT.

To identify functionalities the tester refers to TP.C.1.1, analyze the configuration options of the DUT and performs a search of public available resources (e.g. Internet forums like https://www.router-forum.de/, https://www.dsl-forum.de/ or https://www.ip-phone-forum.de/forums/).

In addition the tester performs port scans of all interfaces of the public and private network interfaces for initialized (re-use of TP.C.1.2) and customized to identify functionalities of the DUT.

The tester creates a list of all functionalities of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can't identify any functionality of the DUT, which is not described in the user guidance.

TP.C.2.2 The tester verifies that each identified functionality is made transparent to the end-user.

This Test Procedure depends on all states of the DUT.

Using one of the access methods listed in Section 3.6, Table 13, to configure the DUT, the tester verifies the information the DUT provides for every functionality. These information are for example configuration options, overview of the status (e.g. enabled, deactivated, not configured) and logging data.

The DUT could also provide other features to indicate the status of a functionality to the end-user (e.g. LED to indicate WLAN on/ off).

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any functionality which does not provide information or its status to the end-user.

4.4 Module D - Configuration and Information

The following Test Requirements differentiate between access methods to "configure the DUT and/ or access information" and access methods with the intention to simply "access information".

4.4.1 Access methods to configuration and information

TR.D.1 **All access methods allowing the end-user to configure the DUT and/ or access information from the current or past state of the DUT and its services in all three states (*factory setting*, *initialized* and *customized*) are in scope of the Module D Test Requirements.**

TP.D.1.1 Following the user guidance the tester configures the DUT for operation. The DUT will change from *factory setting* to *initialized*. The tester verifies the used access method is listed in Section 3.6, Table 13.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

If more than one procedure is available to set the DUT into operation all procedures MUST be verified (e.g. web interface, mobile app, telnet, ssh).

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any access method allowing the end-user to configure the DUT for operation which is not listed in the ICS, Section 3.6, Table 13.

TP.D.1.2 After initial configuration the tester verifies all access methods allowing the end-user to configure the DUT and/ or access information from the current or past state of the DUT and its services in the *initialized* and *customized* state. The tester verifies that these access methods are listed in Section 3.6, Table 13.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

To identify possible access methods the tester refers to the user guidance of the DUT and public available resources.

This Test Procedure is applicable for access methods allowing the end-user to configure the DUT as well for access methods allowing the end-user to access information from the current or past state of the DUT and its services. In most cases access to both, configuration and information, will be provided through a dedicated web server running on the DUT. Access to configuration and information MAY also be provided through other means (e.g. mobile app, telnet, ssh). In all cases the same requirements apply.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any access method allowing the end-user to configure the DUT and/ or access information from the current or past state of the DUT and its services which is not listed in the ICS, Section 3.6, Table 13.

4.4.2 Access methods to configuration

TR.D.2 **Access to the configuration of the DUT MUST at least be secured by a password in the *initialized* and *customized* state. The DUT MAY offer a higher level of security by providing alternative authentication mechanisms.**

TP.D.2.1 The tester verifies for each identified access method the provided authentication mechanism.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Using the results of TP.D.1.2 the tester creates a list of all access methods available to configure the DUT in *initialized* and *customized*. The tester specifies for each of those the authentication mechanism(s).

The tester verifies that each identified authentication mechanism of every access method listed is secured by a password at least. Alternative authentication mechanisms providing a higher level of security are accepted.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any access method allowing to configure the DUT without providing at least a password authentication mechanism.

TP.D.2.2 In *initialized* and *customized* the tester verifies by functional tests the authentication mechanism for each identified access method.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester verifies each authentication mechanism identified in TP.D.2.1 by functional testing. For passwords the Test Requirements listed in Section 4.4.3 apply. Alternative authentication mechanisms MUST meet the requirements listed in Section 4.4.4.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can demonstrate by functional testing that each authentication mechanism complies with the Test Requirements of Section 4.4.3 or alternative of Section 4.4.4.

TP.D.2.3 The tester verifies for each identified access method that the used authentication mechanism cannot be deactivated.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester verifies for each authentication mechanism identified in TP.D.2.1 the configuration options. By considering the user guidance, technical documentation and public available resources the tester examines possible configuration options to deactivate the authentication mechanism.

Criteria to Pass

This Test Procedure is successfully passed, if all identified authentication mechanisms of each access method provide no configuration option to deactivate the authentication mechanism.

TR.D.3 **If the DUT offers configuration through a web interface the complete communication to access the configuration SHOULD be secured using HTTP over Transport Layer Security (TLS) support according to [TR-02102-2] *Section 3: Recommendations*.**

TP.D.3.1 The tester verifies in *factory setting* and *initialized* the TCP communication to access the configuration via a web interface and confirms that the TLS support is implemented according to [TR-02102-2] *Section 3: Recommendations*.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

IF the DUT offers more than one configuration method through a web interface (e.g. mobile APP, different network interfaces) all methods MUST be analyzed. The tester MUST verify if these access methods use different TLS implementations or all access methods are linked to the same implementation.

The tester performs functional testing to verify the following aspects of the recommendations given in Section 3 of [TR-02102-2]. These tests can be performed using tools like wireshark or tcpdump.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

TLS Requirements:

- The TLS version MUST be TLS 1.2 or TLS 1.3.
- The requested minimum key lengths stated in Table 13 of [TR-02102-2] are implemented. The TLS implementation does not use any keys not fulfilling this requirement.

Requirements for TLS 1.2:

- Only cipher suites listed in Section 3.3.1 of [TR-02102-2] are supported.
- Cipher suites using Pre-shared Keys (TLS_PSK_*) are not supported.
- Only the signature procedures rsa, dsa and ecdsa according to Table 6 of [TR-02102-2] are implemented.
- SHA-1 is prohibited for all digital signatures. Only hash functions listed in Table 7 of [TR-02102-2] are acceptable.
- Only the Diffie-Hellman groups listed in Table 5 of [TR-02102-2] are supported.

Requirements for TLS 1.3:

- Cipher suites using Pre-shared Keys (psk_ke, psk_dhe_ke) are not supported.
- Only the Diffie-Hellman groups listed in Table 9 of [TR-02102-2] are supported.
- Only the signature procedures listed in Table 10 and Table 11 of [TR-02102-2] are implemented.
- Only cipher suites listed in Table 12 of [TR-02102-2] are supported.

In addition to the tests required above the tester MUST verify the TLS implementation to be robust against common attack vectors like heartbleed or POODLE vulnerability. One recommended tool is testssl.sh (https://testssl.sh/), which provides an output showing the found issues in red lines, which SHOULD be green, except it is a false positive. The tester MUST analyze the red lines.

Alternative tools can be used, but all tools MUST be mentioned in the test report

including log files and/ or screenshots.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the TLS support is implemented according to [TR-02102-2] *Section 3: Recommendations* as requested above. In addition the tester find no common vulnerabilities using test tools like testssl.sh.

TR.D.4 **In *factory setting* the DUT MUST allow end-user access to the configuration only using an interface of the private network.**

TP.D.4.1 The tester verifies in *factory setting* that the access methods identified in the ICS, Section 3.6, Table 13, to configure the DUT are only accessible by an interface of the private network.

This Test Procedure depends on the DUTs states *factory setting*.

The tester refers to TR.B.2 and verifies that all Test Procedures of this Requirement do not indicate an access method to allow an end-user to configure the DUT using an interface of the public network.

The tester verifies that TP.B.2.3 covers port scans in the DUTs state *factory setting* for all interfaces of the public network.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any access method allowing the end-user to configure the DUT using an interface of the public network.

TR.D.5 **If the DUT allows to access the configuration over an interface of the public network (Module B) as a *customization* feature this communication MUST be encrypted using TLS according to [TR-02102-2] Section 3: Recommendations. This access method MUST be deactivated in *factory setting*.**

TP.D.5.1 In *initialized* the tester uses one of the access methods listed in Section 3.6, Table 13, to configure the DUT, to allow configuration over an interface of the public network.

This Test Procedure depends on the DUTs state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the DUT allows the tester to activate and deactivate the remote configuration functionality. If more than one access method could be configured for a public network interface each method is in scope by this Test Requirement TR.D.5.

TP.D.5.2 For each access method identified by TP.D.5.1 the tester verifies by functional testing that this method is deactivated in *factory setting*.

This Test Procedure depends on the DUTs state *factory setting*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester has verified the Test Procedures of TR.D.4.

TP.D.5.3 For each access method identified by TP.D.5.1 the tester verifies by functional testing that the communication is encrypted using TLS according to [TR-02102-2] *Section 3: Recommendations*.

This Test Procedure depends on the DUTs state *customized*.

IF the DUT offers more than one access method to configure the DUT using an interface of the public network all methods MUST be analyzed. The tester MUST verify if these access methods use different TLS implementations or all access methods are linked to the same implementation.

The tester performs functional testing to verify the following aspects of the recommendations given in Section 3 of [TR-02102-2]. These tests can be performed using tools like wireshark or tcpdump.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

TLS Requirements:

- The TLS version MUST be TLS 1.2 or TLS 1.3.
- The requested minimum key lengths stated in Table 13 of [TR-02102-2] are implemented. The TLS implementation does not use any keys not fulfilling this requirement.

Requirements for TLS 1.2:

- Only cipher suites listed in Section 3.3.1 of [TR-02102-2] are supported.
- Cipher suites using Pre-shared Keys (TLS_PSK_*) are not supported.
- Only the signature procedures rsa, dsa and ecdsa according to Table 6 of [TR-02102-2] are implemented.
- SHA-1 is prohibited for all digital signatures. Only hash functions listed in Table 7 of [TR-02102-2] are acceptable.
- Only the Diffie-Hellman groups listed in Table 5 of [TR-02102-2] are supported.

Requirements for TLS 1.3:

- Cipher suites using Pre-shared Keys (psk_ke, psk_dhe_ke) are not supported.
- Only the Diffie-Hellman groups listed in Table 9 of [TR-02102-2] are supported.
- Only the signature procedures listed in Table 10 and Table 11 of [TR-02102-2] are implemented.
- Only cipher suites listed in Table 12 of [TR-02102-2] are supported.

In addition to the tests required above the tester MUST verify the TLS implementation to be robust against common attack vectors like heartbleed or POODLE vulnerability. One recommended tool is testssl.sh (https://testssl.sh/), which provides an output showing the found issues in red lines, which SHOULD be green, except it is a false positive. The tester MUST analyze the red lines.

Alternative tools can be used, but all tools MUST be mentioned in the test report including log files and/ or screenshots.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the TLS support is implemented according to [TR-02102-2] *Section 3: Recommendations* as requested above. In addition the tester find no common vulnerabilities using test tools like testssl.sh.

TR.D.6 **The end-user SHOULD be able to configure the port to be used for access to the configuration via the WAN interface.**

TP.D.6.1 For each access method identified by TP.D.5.1 the tester verifies that the port to be used for access to the configuration via an interface of the public network could be changed.

This Test Procedure depends on the DUTs state *customized*.

Using one of the access methods listed in Section 3.6, Table 13, to configure the DUT, the tester verifies the configuration options for each access method identified by TP.D.5.1. These configuration options SHOULD allow the end-user to change the port to be used for the respective access method.

If more than one interface of the public network allows the access to the configuration all interfaces MUST be assessed.

The tester verifies the port change for each access method by functional testing.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can demonstrate by functional testing that the end-user can change the port to be used for access to the configuration via the public network for each access method identified by TP.D.5.1.

TR.D.7 **If the DUT offers an option to save the current configuration to a file, this file SHOULD be encrypted and SHOULD be protected by a user selected password. The end-user SHOULD be assisted upon setting the password by a mechanism indicating the strength of the password by a mechanism similar to the one described for access to the configuration (refer to Section 4.4.3, Passwords).**

TP.D.7.1 The tester verifies by functional testing the DUT functionality to save the current configuration to an encrypted and password protected file.

This Test Procedure depends on the DUTs state *initialized*.

In initialized the tester follows the user guidance to save the current configuration of the DUT to an encrypted and password protected file.

The tester details in the test report the encryption method(s) offered by the DUT. If the DUT offers more than one encryption method or mechanism to save the current configuration all methods and mechanisms have to be assessed by the tester.

For all methods and mechanisms the tester analyses the password protected file. Using tools like a hex editor the tester tries to identify weaknesses like clear text password stored in the file or unencrypted parts of the file. Also tools like the RouterPassView by NirSoft (https://www.nirsoft.net/utils/router_password_recovery.html) can be used to analyze the configuration file.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the configuration file of the DUT is encrypted and password protected and functional testing does not indicate any issues.

TP.D.7.2 The tester verifies by functional testing the mechanism indicating the strength of the password used to protect the encrypted file. This mechanism SHOULD be similar to the one described for access to the configuration (refer to Section 4.4.2, Passwords).

This Test Procedure depends on the DUTs state *initialized*.

Refer to TP.A.14.2 and TP.D.14.1 for a similar approach.

In initialized the tester follows the user guidance to save the current configuration of the DUT to an encrypted and password protected file.

During entering the password for the file to be encrypted and exported the tester observes the mechanism indicating the strength of the password entered. If the DUT offers more than one mechanism to save the current configuration all mechanisms have to be assessed by the tester.

According to [TR-03148], Section 4.1.1, *User Access to Configuration*, an accepted password (= indication "good") MUST contain at least 8 characters, including at least two of the following kinds of characters: uppercase letters [A-Z], lowercase letters [a-z], special characters [e.g. ?, !, $, etc.] or numeric characters [0-9].

A "weak" password does not met the requirements above (e.g. password is too short, password only consists of numeric characters).

The mechanism can indicate a "high" password strength if the password fulfills more than at least one requirement (e.g. password is even longer, consists of more than 2 kinds of characters) while still fulfilling the other requirements.

If one rule used to identify a "good" password requires that the password MUST be a combination of at least 2 of the following kinds of characters a) uppercase letters [A-Z], b) lowercase letters [a-z], c) special characters [e.g. ?, !, $, etc.] and d) numeric characters [0-9] the tester MUST verify all possible valid combinations ab, ac, ad, bc, bd, cd by functional testing.

Also input representing a "high" password or "weak" password MUST be tested.

Other implementations are acceptable if they are similar. In all cases the tester MUST detail the implementation and the tests performed in the test report.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify by functional testing that the mechanism indicating the strength of the password is conform to the requirements stated above.

TR.D.8 To export and/ or import the DUT settings the end-user MUST be successfully authenticated at the device.

TP.D.8.1 The tester verifies by functional testing that the DUT requires successful end-user authentication before export and/ or import of settings.

This Test Procedure depends on the DUTs state *initialized*.

In initialized the tester follows the user guidance to save the current configuration of the DUT to an encrypted and password protected file.

The tester verifies by functional testing that this export mechanism is only be accessible after successful user authentication at the DUT.

After export of the current configuration of the DUT to an encrypted and password protected file the tester follows the user guidance to import the file of the previously exported configuration.

The tester verifies by functional testing that this import mechanism is only be accessible after successful user authentication at the DUT.

If the DUT offers more than one mechanism to save and/ or import the configuration all mechanisms have to be assessed by the tester.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot identify any functionality of the DUT to export and/ or import of settings without requiring successful end-user authentication.

4.4.3 Passwords

For each access method identified by TP.D.1.2 requiring a password as the designated factor for user authentication the password method MUST fulfill the following requirements.

TR.D.9 **The preset password used for user authentication MUST contain at least 8 characters, including at least two of the following kinds of characters: uppercase letters [A-Z], lowercase letters [a-z], special characters [e.g. ?, !, $, etc.] or numeric characters [0-9].**

TP.D.9.1 The tester verifies the password policy defined by TR.D.9 for each preset password.

This Test Procedure depends on all states of the DUT.

The tester verifies the preset password contains at least 8 characters, including a combination of at least 2 of the following kinds of characters

a) uppercase letters [A-Z],

b) lowercase letters [a-z],

c) special characters [e.g. ?, !, $, etc.] and

d) numeric characters [0-9].

The tester MUST verify all preset passwords of the DUT associated to any access method requiring a password as the designated factor for user authentication. Also access methods which are not available in *factory setting* or *initialized* are in focus (e.g. ssh access enabled in *initialized* and configured using a preset password).

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot identify any preset password of an access method not fulfilling this requirement.

TR.D.10 **The DUT MUST allow an authenticated end-user to change the password after entering the previous password.**

TP.D.10.1 The tester verifies that an authenticated end-user is able to change his password after entering the previous password.

This Test Procedure depends on all states of the DUT.

The tester verifies the list of procedures offered by the DUT for an authenticated end-user to change his password as stated by the applicant in Section 3.6, Table 16: Password change procedures. This list of procedures must be consistent with the user guidance.

The tester verifies by functional testing each procedure of this list. To verify the implementation the tester uses the password of the end-user to authenticate himself at the DUT. After authentication the tester performs the process to change the previous used password. This process MUST require to enter first the previous

(old) password again and than entering the new password. Alternatively the old and new password can be entered in the same dialog/ command.

The tester performs a logout (if necessary) and test the new credentials using an access method listed in Section 3.6, Table 13, to configure the DUT.

The tester SHOULD also verify that the previous (old) credentials are never accepted by the associated access method.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can perform a password change according to the requirements of this Test Procedure.

TR.D.11 The password authentication mechanism MUST be protected against brute force attacks.

TP.D.11.1 The tester verifies by functional testing that each password authentication mechanism provides an error counter for consecutively failed login attempts.

This Test Procedure depends on all states of the DUT.

The password authentication mechanism could be an element of an access method listed in Section 3.6, Table 13, to configure the DUT. Alternative methods are acceptable.

The tester creates a list of all password authentication mechanisms of the DUT.

Using this list of password authentication mechanisms the tester verifies for each mechanism by functional testing that an error counter for consecutively failed login attempts exists. It is expected, that the DUT reacts for example on 10 consecutively failed login attempts.

The tester tries to perform multiple login attempts to each password authentication mechanism from different client devices using different invalid credentials.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot identify any password authentication mechanism not providing an error counter for consecutively failed login attempts.

TP.D.11.2 The tester verifies by functional testing that after an overrun of the error counter the following login attempt is delayed. Alternative login protections like two-factor-authentication are acceptable.

This Test Procedure depends on all states of the DUT.

Using the list of password authentication mechanisms created in TP.D.11.1 the tester verifies for each mechanism by functional testing that after an overrun of the error counter the following login attempt is delayed (e.g. for 60 seconds).

Alternative protection mechanisms like two-factor-authentication (2FA) are acceptable and should also be assessed by the tester.

The tester tries to perform multiple login attempts to each password authentication mechanism from different client devices using different invalid credentials. By performing these multiple login attempts using invalid credentials the error counter MUST overrun the boundary (e.g. 10). The tester tries to perform the next login attempts (e.g. the 11th), which MUST be delayed for example 60 seconds. Also the following login attempts (e.g. the 12th, 13th, 14th ...) MUST be delayed.

After a successful login using valid credentials the error counter SHOULD be reset.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot identify any password authentication mechanism not providing a delayed login mechanism after reaching the error counter for consecutively failed login attempts. Alternative protection mechanisms like two-factor-authentication (2FA) are acceptable.

TR.D.12 The session of an authenticated end-user MUST be protected against session hijacking attacks. At minimum session time outs and Cross-Site-Request-Forgery (CSRF) tokens must be implemented.

TP.D.12.1 The tester verifies by functional testing that the DUT enforces a session time out for all sessions of an authenticated end-user.

This Test Procedure depends on all states of the DUT.

Refer to TP.D.18.1 for a similar approach for all access methods based on alternative authentication methods.

The term “the session of an authenticated end-user” refers to all sessions of this kind the DUT offers, not only to the access methods listed in Section 3.6, Table 13, to configure the DUT. For example alternative sessions to change the password or to access information from the current or past state of the DUT and its services are also in focus.

The tester verifies the list of sessions of an authenticated end-user the DUT offers in *initialized* and *customized* as stated by the applicant in Section 3.6, Table 17: Sessions of an authenticated end-user. The addressed mechanisms to protect the sessions against session hijacking attacks must be consistent with the technical documentation.

For all sessions of this list the tester verifies by functional testing that the DUT enforces a session time out of maximum 10 minutes. This session time out MUST be enforced by the server side (by the DUT), not by the client side (e.g. JavaScript, cookie).

Criteria to Pass

This Test Procedure is successfully passed, if functional testing for all sessions of an authenticated end-user demonstrates an existing session time out according to the requirements of this Test Procedure.

TP.D.12.2 The tester verifies by functional testing that the DUT enforces for each session of an authenticated end-user CSRF tokens.

This Test Procedure depends on all states of the DUT.

Refer to TP.D.18.2 for a similar approach for all access methods based on alternative authentication methods.

For all sessions identified in TP.D.12.1 the tester verifies by functional testing that the DUT enforces CSRF tokens. The token generation method MUST demonstrate that the generated token secret is unique, except by chance. For each end-user authenticated session a new token MUST be created.

Criteria to Pass

This Test Procedure is successfully passed, if functional testing for all sessions of an authenticated end-user demonstrates existing CSRF tokens according to the requirements of this Test Procedure.

TR.D.13 The DUT MUST NOT be initialized with accounts undocumented to the end-user.

TP.D.13.1 The tester verifies that all existing accounts to initialize the DUT are documented to the end-user.

This Test Procedure depends on the DUTs state *factory setting*.

Refer to TP.D.19.1 for a similar approach for all access methods based on alternative authentication methods.

Following TP.A.1.2 the tester creates a list of all accounts which can be used to initialize the DUT. This list MUST refer to all procedures identified in TP.A.1.2.

Criteria to Pass

This Test Procedure is successfully passed, if all accounts of this list are documented to the end-user in the user guidance.

TP.D.13.2 The tester verifies that the DUT could not be initialized with accounts undocumented to the end-user.

This Test Procedure depends on the DUTs state *factory setting*.

Refer to TP.D.19.2 for a similar approach for all access methods based on alternative authentication methods.

By considering the DUTs user documentation, the configuration options and by searching using public available resources the tester performs a search for accounts to initialize the DUT which are not listed in TP.D.13.1.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot find any account to initialize the DUT which is undocumented to the end-user.

If the password change mechanism is supported by a mechanism indicating the password strength the following requirements apply.

TR.D.14 The mechanism indicating the password strength is based on the entropy of the password entered by the user. The entropy MAY be estimated by considering the password length and combination of different kind of characters used.

TP.D.14.1 The tester verifies by functional testing the mechanism(s) indicating the password strength.

This Test Procedure depends on all states of the DUT.

Refer to TP.A.14.2 and TP.D.7.2 for a similar approach.

Following the list of password change mechanisms created in TP.D.10.1 the tester verifies the mechanism indicating the password strength for each mechanism of the list.

Each mechanism indicating the password strength MUST use the entropy of the password entered by the user. One example of a mechanism that fulfills this requirement is given below.

Example

> According to [TR-03148], Section 4.1.1, User Access to Configuration, an accepted password (= indication "good") MUST contain at least 8 characters,

including at least two of the following kinds of characters: uppercase letters [A-Z], lowercase letters [a-z], special characters [e.g. ?, !, $, etc.] or numeric characters [0-9].

A "weak" password does not met the requirements above (e.g. password is too short, password only consists of numeric characters).

The mechanism can indicate a "high" password strength if the password fulfills more than at least one requirement (e.g. password is even longer, consists of more than 2 kinds of characters) while still fulfilling the other requirements.

The tester performs functional testing to verify the implementation for each password change mechanism and the associated mechanism indicating the password strength.

If one rule used to identify a "good" password requires that the password MUST be a combination of at least 2 of the following kinds of characters a) uppercase letters [A-Z], b) lowercase letters [a-z], c) special characters [e.g. ?, !, $, etc.] and d) numeric characters [0-9] the tester MUST verify all possible valid combinations ab, ac, ad, bc, bd, cd by functional testing.

Also input representing a "high" password or "weak" password MUST be tested.

Other implementations are acceptable if they are similar. In all cases the tester MUST detail the implementation and the tests performed in the test report.

Criteria to Pass

This Test Procedure is successfully passed, if the evaluator can verify that the mechanism indicating the password strength is based on the entropy of the password entered by the user following the requirements of this Test Procedure.

TR.D.15 This mechanism MUST prevent the user from selecting a weak password without being warned about doing so.

TP.D.15.1 The tester verifies by functional testing that the user is warned from selecting a weak password.

This Test Procedure depends on the DUTs state *initialized* and *customized*.

Following the list of password change mechanisms created in TP.D.10.1 the tester verifies by functional testing for each mechanism that the user is warned if he is trying to select a weak password according to the mechanism indicating the password strength.

For each password change mechanism the tester tries to set a weak password according to the rules of the mechanism indicating the password strength. It is expected that the warning dialog contains a resolute warning message like "This is an insecure password! Please use a strong password for authentication.".

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that each password change mechanism provides a warning dialog for the user in case that the user tries to select a weak password.

If a preset password is used with *factory setting* the following requirements apply in addition.

TR.D.16 The preset password used with *factory setting* MUST NOT contain information that consists of or is derived from data or parts of data that depend on the DUT itself.

TP.D.16.1 The tester verifies the password generation method(s) for all preset passwords of the DUT.

This Test Procedure depends on all states of the DUT.

The tester verifies the list of preset passwords including their generation method as stated by the applicant in the ICS, Table 15: List of preset passwords.

For all passwords of this list the tester performs a review of the password generation method(s) by using the vendor/ manufacturer documentation.

If this documentation is not disclosed by the applicant or manufacturer the tester MUST verify this Test Procedure using 10 samples of the DUT from the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

The tester verifies that these passwords do not contain information that consists of or is derived from data or parts of data that depend on the DUT itself. Data that depend on the DUT is for example the product or vendor/ manufacturer name, serial number, Media Access Control (MAC) address or the preset SSID.

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any preset password demonstrates that the generated password value does not contain information that consists of or is derived from data or parts of data that depend on the DUT itself.

TR.D.17 The preset password used with *factory setting* MUST NOT be shared by multiple devices of the same manufacturer.

TP.D.17.1 The tester verifies the assertions of the applicant given in Section 3.3.2, Table 15.

This Test Procedure depends on the DUTs state *factory setting*.

The applicant MUST state that no preset password is shared between multiple DUTs of the same manufacturer.

For all passwords of the list created in TP.D.16.1 the tester performs a review of the password generation method(s) by using the vendor/ manufacture documentation.

If the generation method for any preset password is not disclosed by the applicant or manufacturer the tester MUST verify this Test Procedure using ten DUTs of the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

The tester verifies that no preset password is shared by multiple devices of the same manufacturer.

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any preset password demonstrates that the generated password value is individual per DUT and will not be shared by multiple devices of the same manufacturer.

4.4.4 Alternative Authentication Methods

For each access method identified by TP.D.1.1 requiring alternative authentication methods as the designated factor for user authentication the method MUST fulfill the following requirements (TR.D.18 up to TR.D.20). Alternative authentication methods offer a higher level of security like One Time Pads (OTP), hardware tokens or similar techniques to realize 2-Factor-Authentication.

TR.D.18 **The session of an authenticated end-user MUST be protected against session hijacking attacks. At minimum session time outs and CSRF tokens MUST be implemented.**

TP.D.18.1 The tester verifies by functional testing that the DUT enforces a session time out for all sessions of an authenticated end-user.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Refer to TP.D.12.1 for a similar approach for all password based access methods.

The term “the session of an authenticated end-user” refers to all sessions of this kind the DUT offers, not only to the access methods listed in Section 3.6, Table 13, to configure the DUT. For example alternative sessions to change the password or to access information from the current or past state of the DUT and its services are also in focus.

The tester verifies the list of sessions of an authenticated end-user the DUT offers in initialized and customized as stated by the applicant in Section 3.6, Table 17: Sessions of an authenticated end-user. The addressed mechanisms to protect the sessions against session hijacking attacks must be consistent with the technical documentation.

For all sessions of this list the tester verifies by functional testing that the DUT enforces a session time out of maximum 10 minutes. This session time out MUST be enforced by the server side (by the DUT), not by the client side (e.g. javascript, cookie).

Criteria to Pass

This Test Procedure is successfully passed, if functional testing for all sessions of an authenticated end-user demonstrates an existing session time out according to the requirements of this Test Procedure.

TP.D.18.2 The tester verifies by functional testing that the DUT enforces for each session of an authenticated end-user CSRF tokens.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Refer to TP.D.12.2 for a similar approach for all password based access methods.

For all sessions identified in TP.D.18.1 the tester verifies by functional testing that the DUT enforces CSRF tokens. The token generation method MUST demonstrate that the generated token secret is unique, except by chance. For each end-user authenticated session a new token MUST be created.

Criteria to Pass

This Test Procedure is successfully passed, if functional testing for all sessions of an authenticated end-user demonstrates existing CSRF tokens according to the requirements of this Test Procedure.

TR.D.19 The DUT MUST NOT be initialized with accounts undocumented to the end-user.

TP.D.19.1 The tester verifies that all existing accounts to initialize the DUT are documented to the end-user.

This Test Procedure depends on the DUTs state *factory setting*.

Refer to TP.D.13.1 for a similar approach for all password based access methods.

Following TP.A.1.2 the tester creates a list of all accounts which can be used to initialize the DUT. This list MUST refer to all procedures identified in TP.A.1.2.

Criteria to Pass

This Test Procedure is successfully passed, if all accounts of this list are documented to the end-user in the user guidance.

TP.D.19.2 The tester verifies that the DUT could not be initialized with accounts undocumented to the end-user.

This Test Procedure depends on the DUTs state *factory setting*.

Refer to TP.D.13.2 for a similar approach for all password based access methods.

By considering the DUTs user documentation, the configuration options and by searching using public available resources the tester performs a search for accounts to initialize the DUT which are not listed in TP.D.18.1.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot find any account to initialize the DUT which is undocumented to the end-user.

TR.D.20 All private cryptographic keys and secrets used for alternative authentication mechanisms MUST NOT be shared by multiple devices in the *factory setting* and *initialized* state.

TP.D.20.1 The tester verifies the assertions of the applicant given in Section 3.6, Table 18.

This Test Procedure depends on the DUTs states *factory setting* and *initialized.*

The applicant MUST state that no cryptographic key or secret is shared between multiple DUTs.

If the generation method for any private cryptographic key or secret is not disclosed by the applicant or manufacturer the tester MUST verify this Test Procedure using ten DUTs of the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

The tester verifies that no private cryptographic key or secret used for alternative authentication mechanism(s) is shared by multiple devices of the same manufacturer.

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any private cryptographic key or secret demonstrates that the generated key value or secret is individual per DUT and will not be shared by multiple devices of the same manufacturer.

4.4.5 Providing Information

TR.D.21 **The DUT MUST provide security relevant information to the authenticated end-user. This information SHOULD be made available at a central source of information (e.g. on a specific site on the configuration interface).**

TP.D.21.1 The tester verifies that the DUT provides security relevant information to the authenticated end-user.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The types of security relevant information to be provided to the authenticated end-user are given in [TR-03148], Table 6, *Information provided to the end-user*.

The tester identifies all access methods of the DUT to provide security relevant information according to [TR-03148], Table 6. This identification MUST be supported by functional verification by the tester.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT provides at least one access methods allowing the authenticated end-user to access security relevant information. All identified access methods MUST be part of the listing in the ICS, Section 3.6, Table 13.

TP.D.21.2 The tester verifies that the DUT provides the security relevant information at a central source of information.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify for all access methods identified in TP.D.21.1 that the security relevant information is provided at a central source of information (e.g. on a specific site on the configuration interface).

TR.D.22 **The DUT SHOULD provide a functionality to send (push) notifications of security relevant events to the end-user. This communication MUST always be encrypted, if the distant communication endpoint supports encryption. If the distant communication endpoint supports TLS this encryption method MUST be used. For TLS the requirements of [TR-02102-2], Section 3: Recommendations, are mandatory. The DUT MUST restrict the supported cipher suites for alternative encryption methods to the suites listed in [TR-02102-2] Section 3. The functionality to send (push) notifications MUST only be activated upon the end-users request.**

TP.D.22.1 The tester verifies that the DUT provides a functionality to send (push) notifications of security relevant events to the end-user.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Security relevant events are for example changes to the configuration, protocols of observed attacks on the firewall or firmware updates. This functionality MAY be provided through eMail, an App or with similar techniques.

The tester creates a list of all functionalities of the DUT to send (push) notifications of security relevant events to the end-user. To identify these functionalities the tester refers to the user documentation and the configuration options of the access methods to configure the DUT (ICS, Section 3.6, Table 13).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to identify at least one functionality of the DUT to send (push) notifications of security relevant events to the end-user.

TP.D.22.2 The tester performs functional testing for all functionalities to send (push) notifications of security relevant events to the end-user. The tester verifies that the functionality to send (push) notifications MUST be activated by the end-user and is disabled by default in *factory setting* and *initialized*.

This Test Procedure depends on all states of the DUT.

For each functionality identified in TP.D.22.1 the tester performs functional testing including

- verification of the functionality before activation. The tester verifies in *factory setting* and *initialized* that the functionality to send (push) notifications is deactivated by default.
- the configuration of the functionality according to the user guidance. The configuration must only be accessible using an access method listed in Section 3.6, Table 13, to configure the DUT. The tester configures the functionality to send (push) notifications.
- tests of the send (push) mechanism at the DUT. The tester triggers different events which should release push notifications of security relevant events to the end-user. If the distant communication endpoint supports encryption the DUT MUST always encrypt the notifications. The tester verifies the sending of notifications using sniffing tools like wireshark or tcpdump. By triggering several events the tester verifies that all events which should release a push notification are sent by the DUT.
- tests of the receive mechanism at the client. Following the notifications sent above the tester verifies the receiver side. Here also tools like wireshark or tcpdump can be used by the tester to verify the communication. The tester verifies that the push notifications of security relevant events can be read and if necessary encrypted at the client site.
- test of the deactivation of the functionality to send (push) notifications of security relevant events. The tester deactivates this functionality using one of the access method listed in Section 3.6, Table 13, to configure the DUT. After deactivation the tester verifies that the DUT does not send (push) these notifications any more. This verification must be supported by functional tests using sniffing tools like wireshark or tcpdump.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify the DUTs capabilities to send (push) notifications of security relevant events based on the Requirements above. This functionality is deactivated by default in *factory setting* and *initialized*.

TP.D.22.3 The tester verifies by functional testing that the communication to send (push) notifications is encrypted using TLS according to [TR-02102-2], *Section 3: Recommendations*, if the distant communication endpoint supports TLS.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

For each functionality identified in TP.D.22.1 the tester verifies if this method uses different TLS implementations or all methods are linked to the same implementation.

The tester performs functional testing to verify the following aspects of the recommendations given in Section 3 of [TR-02102-2]. These tests can be performed using tools like wireshark or tcpdump.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

The communication to send (push) notifications is typically a client software implementation. For both client or server implementations the following requirements MUST be fulfilled by the DUT.

TLS Requirements:

- The TLS version MUST be TLS 1.2 or TLS 1.3.
- The requested minimum key lengths stated in Table 13 of [TR-02102-2] are implemented. The TLS implementation does not use any keys not fulfilling this requirement.

Requirements for TLS 1.2:

- Only cipher suites listed in Section 3.3.1 of [TR-02102-2] are supported.
- Cipher suites using Pre-shared Keys (TLS_PSK_*) are not supported.
- Only the signature procedures rsa, dsa and ecdsa according to Table 6 of [TR-02102-2] are implemented.
- SHA-1 is prohibited for all digital signatures. Only hash functions listed in Table 7 of [TR-02102-2] are acceptable.
- Only the Diffie-Hellman groups listed in Table 5 of [TR-02102-2] are supported.

Requirements for TLS 1.3:

- Cipher suites using Pre-shared Keys (psk_ke, psk_dhe_ke) are not supported.
- Only the Diffie-Hellman groups listed in Table 9 of [TR-02102-2] are supported.
- Only the signature procedures listed in Table 10 and Table 11 of [TR-02102-2] are implemented.
- Only cipher suites listed in Table 12 of [TR-02102-2] are supported.

If the communication to send (push) notifications is based on a server implementation on the DUT the following aspect MUST be considered by the tester:

> In addition to the tests required above the tester MUST verify the TLS implementation to be robust against common attack vectors like heartbleed or POODLE vulnerability. One recommended tool is testssl.sh (https://testssl.sh/), which provides an output showing the found issues in

red lines, which SHOULD be green, except it is a false positive. The tester MUST analyze the red lines.

Alternative tools can be used, but all tools MUST be mentioned in the test report including log files and/ or screenshots.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the TLS support is implemented according to [TR-02102-2] *Section 3: Recommendations* as requested above. In addition the tester find no common vulnerabilities in server implementations using test tools like testssl.sh.

TP.D.22.4 If the distant communication endpoint supports alternative encryption methods (not TLS) the tester verifies by functional testing that the communication to send (push) notifications is encrypted using cipher suites according to [TR-02102-2] *Section 3: Recommendations*.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

For each functionality identified in TP.D.22.1 the tester verifies if this method supports alternative encryption methods (not TLS).

The tester performs functional testing to verify the following details of the implementation(s) for alternative encryption methods. These tests can be performed using tools like wireshark or tcpdump.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

The communication to send (push) notifications is typically a client software implementation. For both client or server implementations only cipher suites listed in Section 3.3.1 or Table 12 of [TR-02102-2] are supported.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the alternative encryption method restricts the implemented cipher suites to the suites listed in [TR-02102-2] *Section 3: Recommendations*.

TR.D.23 The DUT MUST allow the end-user to display the version number of the firmware currently installed on the DUT. The DUT MAY additionally show an estimate date of the firmware.

TP.D.23.1 The tester verifies that the DUT indicates the version number of the firmware currently installed.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT allow the end-user to display the version number of the firmware currently installed.

The tester performs an update of the DUTs firmware and verifies the new version number of the updated firmware is consistent with the firmware identifier of the new version.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT indicates the version number of the firmware currently installed.

TP.D.23.2 The tester verifies that the DUT indicates the estimate date of the firmware currently installed.

This Test Procedure depends on all states of the DUT.

If supported the tester verifies the additionally shown estimate date of the firmware currently installed.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies this estimate date, which can be information about the release date, compilation date or the date of the installation of the firmware on the DUT.

The tester performs an update of the DUTs firmware and verifies the new estimate date of the updated firmware is consistent.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT indicates the estimate date of the firmware currently installed.

TR.D.24 If the DUT has obtained knowledge that the firmware installed on it is currently out-of-date the DUT MUST inform the end-user about this with a meaningful message.

TP.D.24.1 The tester verifies that the DUT informs the end-user about an outdated version of the currently installed firmware.

This Test Procedure depends on all states of the DUT.

Using a DUT with an old firmware version installed on it the tester verifies in all three states that after booting the DUT and connecting to the IAP the DUT automatically verifies its firmware status. After this firmware verification task the tester verifies that the DUT informs the end-user about the firmware status with a meaningful message (e.g. display Pop-Up after Log-In).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT informs in all three states the end-user about an outdated version of the currently installed firmware.

TR.D.25 As soon as a decision is made by the manufacturer to not support for the DUT anymore the same mechanism MUST be used by the manufacturer to inform the end-user about the End of Service (EoS) of the DUT as required by TR.E.10.

TP.D.25.1 The tester confirms that the Test Procedures of TR.E.10 are verified.

“The same mechanism” refers to the mechanism verified under TR.E.10 (e.g. notification on the web interface to configure the DUT).

Criteria to Pass

This Test Procedure is successfully passed, if all Test Procedures of TR.E.10 can be verified by the tester with a PASS verdict.

TR.D.26 The DUT MUST allow the end-user to display the current state (active/ inactive) of the firewall as well as it MUST display the rule set currently set up by the end-user.

TP.D.26.1 The tester verifies that the DUT informs the end-user about the current state of the firewall.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access

information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT allows the end-user to display the current state of the firewall (e.g. active/ inactive). The tester activates and deactivates the DUTs firewall several times and observes the correct indication of the corresponding firewall state.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT correctly indicates the current state of the firewall to the end-user.

TP.D.26.2 The tester verifies that the DUT informs the end-user about the firewall rule set currently set up by the end-user.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT allow the end-user to display the firewall rule set currently set up by the end-user (e.g. port forwarding configuration). The tester changes the firewall rule set several times and observes the correct indication of the corresponding rule set.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT correctly indicates the current firewall rule set to the end-user.

TR.D.27 If the DUT offers remote configuration the status of this functionality (active/ inactive) MUST be made available to the end-user.

TP.D.27.1 The tester verifies that the DUT informs the end-user about the status (active/ inactive) of the remote configuration functionality.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT allows the end-user to display the current status of the remote configuration functionality (e.g. active/ inactive). The tester activates and deactivates the DUTs remote configuration functionality several times and observes the correct indication of the corresponding status.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT correctly indicates the current status of the remote configuration functionality to the end-user.

TR.D.28 The DUT MUST allow the end-user to retrieve information about the last or more login attempt(s). If the login attempt was made after *initialization*, the information about the last login attempt(s) MUST consist of the time and date of the login attempt, the IP address and the MAC address of the device from which the login attempt was made from.

TP.D.28.1 The tester verifies that the DUT informs the end-user about the last or more login attempt(s) include successful and unsuccessful login attempt(s).

This Test Procedure depends on all states of the DUT.

For all access methods listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT allows the end-user to retrieve information about the last or

more login attempt(s).

The tester performs several login attempts using correct and incorrect credentials and verifies that these events are consistent with the DUTs log entries.

If the DUT supports more than one access method to configure the DUT the tester MUST verify that the information about the login attempt(s) are consolidated. It is not sufficient if the log information is created for each access method separately and the end-user must verify each access method to collect all information about login attempt(s).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT correctly indicates consolidated information about the last or more login attempt(s) for all access methods supported to the end-user.

TP.D.28.2 The tester verifies that after *initialization* the log information includes the time and date of the login attempt, the IP address and the MAC address of the device from which the login attempt was made from.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

For all access methods listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies that the consolidated log information includes the time and date of the login attempt, the IP address and the MAC address of the device from which the login attempt was made from.

Monitoring (log) of devices in the public network (Internet) is only based on the IP address due to the fact that the MAC address of the device (from which the login attempt was made from) is changed by the public router(s) involved.

The tester performs several login attempts from different devices using correct and incorrect credentials and verifies that these events are consistent with the DUTs log entries.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that after *initialization* the DUT provides consolidated log information including the data as required above.

TR.D.29 The DUT MUST display a summary page for the currently active services on all interfaces. This especially refers to those services optionally provided by the DUT. The DUT SHOULD display exact details on the services running.

TP.D.29.1 The tester verifies that the DUT provides a summary page for all currently active services on all interfaces.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT provides a summary page for all currently active services on all private and public network interfaces.

The list of services for the private and public network interfaces identified by this Test Procedure MUST be consistent with the test activities for TP.A.4.1 and TP.B.5.1.

The tester activates and deactivates several services and verifies that the status

(active/ inactive) is consistent with the summary page of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT provides a summary page for all active services on all interfaces and lists also optional services on this page.

TP.D.29.2 The tester verifies that the DUT provides exact details on the services running.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT provides exact details on the services running (e.g. service and port(s) being used). A rough estimate on the level of detail to be used for this list of running services are services listed in [TR-03148], Table 3 and Table 4.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT provides a summary page for all active services on all interfaces including exact details on the services running.

TR.D.30 The DUT SHOULD display information of the devices that are currently connected to the DUT and the interface being used for this connection. This information MUST include the devices IP address, MAC address and SHOULD contain information on the duration of the connection.

TP.D.30.1 The tester verifies that the DUT provides information on the devices that are currently connected to the DUT.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester verifies in all three states that the DUT provides information of the devices that are currently connected to the DUT. The tester verifies that this information includes the interface being used for this connection as well as the devices IP and MAC address and the duration of the connection. To verify this the tester connects and disconnects several devices using different interfaces of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT provides information on the devices that are currently connected to the DUT including all details required by this Test Procedure.

TR.D.31 The DUT SHOULD allow the end-user to display general information of security relevant events concerning the DUT itself including detected attacks on the secure operation or attempts to manipulate the DUT. If a login attempt was made after *initialization* the DUT SHOULD display the time and date of the login attempt and the IP address and the MAC address of the device the login attempt was made from.

TP.D.31.1 The tester verifies that the DUT provides general information of security relevant events concerning the DUT itself.

This Test Procedure depends on all states of the DUT.

Using one of the access method listed in Section 3.6, Table 13, to access information from the current or past state of the DUT and its services, the tester

verifies in all three states that the DUT provides general information of security relevant events concerning the DUT itself. This information MUST include detected attacks on the secure operation or attempts to manipulate the DUT.

The tester verifies the list of security relevant events concerning the DUT itself as stated by the applicant in Section 3.6, Table 19, by triggering these events. If an event is triggered the tester verifies that the information about this event is indicated to end-user.

The tester verifies in TP.D.28.2 that after *initialization* the log information includes the time and date of the login attempt, the IP address and the MAC address of the device from which the login attempt was made from.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to trigger security relevant events and the DUT provides the information about the respective event to the end-user. In addition TP.D.28.2 is verified with a PASS verdict.

4.5 Module E - Firmware Updates

TR.E.1 The DUT MUST have a functionality to update the firmware using a firmware package.

TP.E.1.1 The tester verifies that the DUT provides a functionality to update its firmware.

This Test Procedure depends on all states of the DUT.

The tester performs a review of the user guidance to identify functionalities of the DUT to update its firmware. In addition the tester verifies the configuration options of the DUT to identify further update functionalities using all access methods listed in Section 3.6, Table 13, to configure the DUT.

The tester verifies that all methods to update the DUTs firmware are listed in the statement of the applicant given in the ICS, Section 3.7, Table 20, *Firmware Update Mechanisms*.

Criteria to Pass

This Test Procedure is successfully passed, if at least one method to update the firmware of the DUT is addressed in the user guidance.

TR.E.2 The DUT MUST allow the end-user to fully control such a firmware update and determine to initiate an online update and/ or manually update the firmware through the configuration interface.

TP.E.2.1 The tester verifies by functional testing that the DUT allows the end-user to fully control the firmware update functionality.

This Test Procedure depends on all states of the DUT.

The tester verifies for all firmware update mechanisms listed in Section 3.7, Table 20, that these mechanisms allow the end-user to fully control the update process.

This includes functional tests of automated online updates (router retrieves firmware package from the Internet (public interface)) and/ or the manually update process (user provides firmware package). It is not required that the DUT supports both automated online and manually update mechanisms.

The tester verifies that the end-user is able to control at least the following configuration settings regarding the automated online update functionality of the DUT:

- activation/ deactivation of the online update feature and
- basic time scheduling for installation of updates (e.g. postponement, specific installation time(s)).

The manual update functionality is inherently under fully control of the end-user.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing for all automated online and manual update mechanisms of the DUT that these mechanism(s) can be controlled by the end-user.

TR.E.3 The DUT SHOULD offer an option to automatically retrieve security relevant firmware updates from a trustworthy source over the Internet (WAN interface).

TP.E.3.1 The tester verifies that the DUT offers an automated firmware download mechanism for updates using a trustworthy source over the Internet.

This Test Procedure depends on all states of the DUT.

The tester performs a review of the user guidance to identify functionalities of the DUT to download firmware update packages. In addition the tester verifies the configuration options of the DUT to identify further download functionalities using all access methods listed in Section 3.6, Table 13, to configure the DUT.

Based on these findings the tester creates a list of all functionalities of the DUT to download firmware update packages for both automated online and/ or manual update mechanisms.

For all methods of this list the tester verifies the download source (e.g. web server, sftp server) and the DUTs functionalities to identify the source (e.g. the server certificate for TLS, reverse DNS lookup (rDNS)).

Criteria to Pass

This Test Procedure is successfully passed, if the tester can identify a functionality of the DUT to automatically download firmware update packages over the Internet. In addition the tester was able to verify that these functionalities verify the download source.

TR.E.4 If the DUT offers an option to automatically retrieve firmware updates this functionality SHOULD be activated by default, but MUST be possible for the end-user to deactivate it when using *customized* settings.

TP.E.4.1 The tester verifies that the DUTs functionality to automatically retrieve firmware updates is activated by default.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester verifies in *factory setting* and *initialized* for the functionalities identified in TP.E.3.1 that the mechanism to retrieve firmware updates is activated by default.

Using a DUT with an outdated firmware installed on it the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*. The tester verifies that the DUT automatically triggers the firmware download mechanism to retrieve a new firmware package during this initialization process or latest immediately after initialization in the state *initialized*.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing that the DUT automatically retrieves firmware update packages

for its outdated firmware status.

TP.E.4.2 The tester verifies that the DUTs functionality to automatically retrieve firmware updates can be deactivated when using *customized* settings.

This Test Procedure depends on the DUTs state *customized*.

The tester verifies in *customized* using an access methods listed in Section 3.6, Table 13, to configure the DUT, that the functionality of the DUT to automatically retrieve firmware updates can be deactivated.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can deactivate in *customized* the DUTs functionality to automatically retrieve firmware updates.

TR.E.5 The firmware update function of the DUT MUST check the authenticity of the firmware package before it is installed on the DUT.

TP.E.5.1 The tester verifies that the DUT checks the authenticity of the firmware package before it is installed.

This Test Procedure depends on all states of the DUT.

The tester verifies for all firmware update mechanisms listed in Section 3.7, Table 20, that these mechanisms require that the DUT performs a check of the authenticity of the firmware package before it is installed. Both online and manual firmware update mechanisms are in scope.

The tester performs a review of the user guidance to identify the DUTs mechanisms to authenticate firmware packages. In addition the tester verifies the configuration options of the DUT to identify further authentication mechanisms using all access methods listed in Section 3.6, Table 13, to configure the DUT.

The tester verifies that the list of identified authentication mechanisms for firmware packages is consistent with the statement of the applicant given in the ICS, Section 3.7, Table 21, Firmware authentication mechanisms.

The tester performs functional testing of each authentication mechanism for firmware packages. These tests include verification of the mechanism(s) itself by using firmware packages containing

- incorrect signatures (e.g. one bit of the signature is changed),
- incorrect payload (e.g. one bit of the firmware data is changed),
- valid signature tested with misconfigured DUT (system date set to a value outside of the validity of the public key, only applicable if the DUT allows this manual configuration).

The tester can use the DUTs log capabilities to support the test evidence and verifies the installation of the new firmware package.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify for each firmware update mechanism of the DUT that each mechanism verifies the authenticity of the firmware package before it is installed.

TR.E.6 The authenticity of a firmware package SHOULD be based on a digital signature that is applied to the firmware package by the manufacturer and checked by the DUT itself. For this purpose only signature schemes in accordance to [SOG-IS] *Section 5.2* MUST be used.

TP.E.6.1 The tester verifies that the authenticity of a firmware package of the DUT is based on digital signatures.

This Test Procedure depends on all states of the DUT.

The tester verifies that all firmware authentication mechanisms of the DUT as stated in the ICS, Section 3.7, Table 21, are based on digital signatures. Functional tests of these mechanism are part of TP.E.5.1 above.

Criteria to Pass

This Test Procedure is successfully passed, if the tester cannot identify any firmware authentication mechanism of the DUT which is not based on digital signatures.

TP.E.6.2 The tester verifies that only signature schemes according to [SOG-IS] *Section 5.2* are used.

This Test Procedure depends on all states of the DUT.

The tester verifies that only the following signature schemes are used to verify the authenticity of firmware packages based on digital signatures (for more notes refer to [SOG-IS] Section 5.2):

Primitive	**Scheme**
RSA	PSS (PKCS#1v2.1) [RFC3447, PKCS1, ISO9796-2]
FF-DLOG	KCDSA [ISO14888-3]
	Schnorr [ISO14888-3/am1]
	DSA [FIPS186-4, ISO14888-3]
EC-DLOG	EC-KCDSA [ISO14888-3]
	EC-DSA [FIPS186-4, ISO14888-3]
	EC-GDSA [TR-03111]
	EC-Schnorr [ISO14888-3/am1]
RSA	PKCS#1v1.5 [RFC3447, PKCS1, ISO9796-2]

Table 27: Agreed Digital Signature schemes

To verify the supported signature scheme the tester refers to the technical documentation as referenced by the applicant in the ICS, Section 3.7, Table 21. In addition the tester verifies the implementation by analyzing the firmware update package for each authentication mechanism. The applicant/ manufacturer MUST provide the public key(s) of the DUT for firmware authentication. Using these public key(s) the tester verifies with his own tools the firmware package according to the supported signature scheme including the conformance tests to the specification of the scheme.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can reproduce the authentication mechanism of the DUT using his own tools to verify the digital signature according to the required standard as stated above.

TR.E.7 The DUT MUST NOT automatically install any unsigned firmware.

TP.E.7.1 The tester verifies that the DUTs firmware update mechanism(s) do not automatically install unsigned firmware packages.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

Using a DUT with an outdated firmware installed on it the tester verifies for all

manual firmware update mechanisms listed in Section 3.7, Table 20, that the update mechanism does not automatically install unsigned firmware. For testing the manufacturer MUST provide an unsigned firmware package for testing.

For all automated online firmware update mechanisms listed in Section 3.7, Table 20, this verification of the tester is based on a documentation review. The manufacturer MUST provide evidence on paper basis that the automated update mechanism(s) do not automatically install unsigned firmware packages (refer to documentation references given in the ICS, Table 21).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing and review of documentation that the DUT does not install unsigned firmware packages automatically.

TR.E.8 The DUT MAY allow the installation of unsigned firmware IF a meaningful warning message has been shown to the authenticated end-user and the end-user accepts the installation of the unsigned firmware.

TP.E.8.1 The tester verifies that the DUT shows a meaningful warning message to the authenticated end-user if an unsigned firmware package should be installed.

This Test Procedure depends on the DUTs states *factory setting* and *initialized.*

Using a DUT with an outdated firmware installed on it the tester verifies for all manual firmware update mechanisms listed in Section 3.7, Table 20, that the update mechanism shows a meaningful warning message to the authenticated end-user if an unsigned firmware package should be installed. The authenticated end-user is required to accept the installation of the unsigned firmware before the installation process starts.

The tester uses an unsigned firmware package of the manufacturer to verify this by functional testing using the manual update process. During these tests the tester verifies that the installation of the unsigned firmware package does not start before the warning message is shown and the authenticated end-user is required to accept the installation explicitly (e.g. warning dialog using a pop-up combined with an accept/ decline prompt).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is not able to install an unsigned firmware package without receiving a meaningful warning message and accepting the installation explicitly.

TR.E.9 The manufacturer of the DUT MUST provide information on how long firmware updates fixing common vulnerabilities and exposures that have a high severity will be made available. This information SHOULD be available on the manufacturer website. Additionally it MAY be made available on the DUT configuration interface.

TP.E.9.1 The tester verifies that the manufacturer provides information on how long firmware updates will be made available.

This Test Procedure depends on all states of the DUT.

The tester performs a review of the applicants assertions as stated in the ICS, Section 3.7. The applicant MUST provide information about the processes and mechanisms to inform the end-user about firmware updates fixing common vulnerabilities and exposures that have a high severity.

The tester verifies that the processes and mechanisms to provide information

about firmware updates are in place. This information MUST contain statements about how long firmware updates fixing common vulnerabilities and exposures that have a high severity (i.e. a CVSS combined score higher than 6.0 according to the Common Vulnerability Scoring System assigned to the specific device or a component used by the device) will be made available.

The tester verifies that this information is available at least on the manufacturer website.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the manufacturer provides information about firmware updates fixing common vulnerabilities and exposures on his website.

TR.E.10 The manufacturer MUST provide information if the DUT has reached the End of its Support (EoS) and will not receive firmware updates by the manufacturer anymore. This information (EoS) MUST be made available on the DUT configuration.

TP.E.10.1 The tester verifies that the manufacturer provides information if the DUT has reached the End of its Support (EoS).

This Test Procedure depends on all states of the DUT.

The tester performs a review of the applicants assertions as stated in the ICS, Section 3.7. The applicant MUST provide information about the processes and mechanisms to inform the end-user if the DUT has reached the EoS.

The tester verifies that the manufacturer provides information on the DUTs configuration if the DUT has reached the EoS and will not receive firmware updates by the manufacturer anymore. The term "on the DUTs configuration" refers to the access methods listed in Section 3.6, Table 13, to configure the DUT. Using these methods the end-user MUST be notified about the EoS (e.g. notification on the web interface to configure the DUT).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify based on documentation that the manufacturer provides information if the DUT has reached the End of its Support (EoS).

TR.E.11 The manufacturer MUST provide firmware updates to fix common vulnerabilities and exposures of a high severity without culpable delay (without undue delay) after the manufacturer obtains knowledge.

TP.E.11.1 The tester verifies that the manufacturer provides firmware updates to fix common vulnerabilities and exposures of a high severity.

This Test Procedure depends on all states of the DUT.

The tester performs a review of the applicants assertions as stated in the ICS, Section 3.7. The applicant MUST provide information about the processes and mechanisms to inform the end-user about firmware updates fixing common vulnerabilities and exposures that have a high severity. The tester verifies if the referenced technical documentation contains information about the update policy of the manufacturer regarding common vulnerabilities and exposures of a high severity.

In addition the tester verifies the change logs for all firmware updates relevant for the DUT for the past 5 years. Shorter periods under review are acceptable if the DUT is new to the market or the manufacturer has changed his firmware update

processes in this period.

By considering public available resources the tester performs a search for known vulnerabilities applicable for the DUT (e.g. https://www.cvedetails.com, https://routersecurity.org/bugs.php, https://vuldb.com/, https://www.exploit-db.com/, https://cve.mitre.org/index.html).

Using this knowledge the tester verifies if

- All vulnerabilities and exposures that have a high severity (e.g. CVE > 6.0) are addressed by the manufacturer in his firmware update process.
- The release of a firmware fix after the manufacturer is informed about the issue is not culpable delayed by the manufacturer. Typically 90 days are acceptable if the vulnerability is not public.
- The release of a firmware fix after the vulnerability is public is not culpable delayed by the manufacturer (e.g. less than 10 days).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the manufacturer provides firmware updates to fix common vulnerabilities and exposures of a high severity according to the requirements stated above.

4.6 Module F - Firewall

All Test Requirements for this Module F - Firewall - are applicable for IPv4 and if supported for IPv6. Therefore the tester MUST verify each Test Procedure twice using a DUT and test clients configured for IPv4 and additionally using a DUT and test clients configured for IPv6. If the DUT supports IPv6 the test report for Module F – Firewall – MUST indicate each Test Procedure (e.g. TP.F.1.1, TP.F.1.2) twice.

TR.F.1 **The DUT MUST contain firewall functionalities that include the basic monitoring and controlling of how IP packets between the private network and the end-user (WLAN and LAN interface) on the one side and the public network i.e. Internet (WAN interface) on the other side are exchanged. The firewall MUST enforce rules for this kind of network traffic by implementing a packet filter.**

TP.F.1.1 The tester verifies that the DUT contains firewall functionalities including basic monitoring and controlling features for IP packets.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester performs a review of the applicants assertions and the referenced user guidance and technical documentation as stated in the ICS, Section 3.1.1 (Table 2 and Table 3) and Section 3.8. In addition the tester identifies the implemented firewall functionality using the access methods listed in Section 3.6, Table 13, to configure the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can identify the DUTs firewall functionality and can confirm that the firewall functionality can be used for basic monitoring and controlling of IP packets between the network segments of the DUT.

TP.F.1.2 The tester verifies by functional testing that the DUTs firewall functionality contain a packet filter (i.e. stateful packet inspection).

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester performs functional testing of the implemented firewall functionality in *initialized*. To monitor and configure the DUTs firewall functionality the tester uses the access methods listed in Section 3.6, Table 13, to configure the DUT.

Test setup: One test system is used in each private network segment (private WLAN, private LAN) and one test system in the public network (Internet, e.g. test system with public IP address). Each test system is capable to send IP Packets (e.g. telnet client, web browser, port scanner like nmap) and to sniff the local network segment using a network sniffer (e.g. tcpdump, wireshark). A network tap could be used to support testing. If the DUT provides several private network segments the tests could be performed in series using two test systems.

Using this test setup the tester verifies for the IP protocols ICMP, TCP (e.g. http) and UDP (e.g. DNS) sent between the test systems in the private network segments and the test system in the Internet that the DUTs firewall is able to monitor (log) and control (filter) these connections. The tester verifies that the DUTs firewall contains a packet filter based on stateful packet inspection.

The monitor (log) feature MUST include details like source IP address/ MAC, destination IP address/ MAC, source port, destination port, a timestamp and a reference to the firewall rule responsible for this specific log event.

The control (filter) feature MUST include the options to allow (accept, enable) or to

forbid (decline, disable) single connections based on the source IP address/ MAC, destination IP address/ MAC, source port, destination port and the connection type (new, established, related).

Monitoring (log) and controlling (filter) of the test system in the public network (Internet) is only based on the test systems IP address due to the fact that the MAC address of this test system is changed by the public router(s) involved.

To verify that the implemented packet filter is based on a stateful packet inspection the tester analyses the necessary firewall rules for IP connections. In case of a stateful packet inspection the necessary rules can analyze the connection type (new, established, related) and typically an IP connection between two network segments requires two rules: one outgoing rule for new connections and one rule accepting all established and related connections.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able monitor (log) and control (filter) different IP connections between the test systems in the private network segment(s) and the Internet using the DUTs firewall functionality based on a packet filter containing a stateful packet inspection.

TR.F.2 The end-user MUST be able to configure the set of rules being used.

TP.F.2.1 The tester verifies that the end-user is able to configure the firewall rule set being used.

This Test Procedure depends on all states of the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to configure the DUTs firewall rule set being used by using the access methods listed in Section 3.6, Table 13, to configure the DUT.

TR.F.3 The firewall MUST NOT contain any port forwarding rules configured *initially*.

TP.F.3.1 The tester verifies that the initial (preset) firewall rules of the DUT do not contain any port forwarding rules.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester verifies in *factory setting* and *initialized* using the access methods listed in Section 3.6, Table 13, to configure the DUT, that the initial (preset) firewall rules do not contain any port forwarding rules.

Criteria to Pass

This Test Procedure is successfully passed, if the tester could not identify any port forwarding rules for the DUTs initial (preset) firewall rules.

TR.F.4 The DUT MUST allow the end-user to define rules for incoming and outgoing network traffic.

TP.F.4.1 The tester verifies that the access methods to configure the DUT allows the end-user do define incoming and outgoing filter rules for the DUTs firewall.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester verifies using the access methods listed in Section 3.6, Table 13, to configure the DUT, that the authenticated end-user is able to define incoming and outgoing filter rules for the DUTs firewall functionality.

The tester verifies by functional testing that filter rules for incoming and outgoing

network traffic between private and public network interfaces based on the IP protocols ICMP, TCP (e.g. http) and UDP (e.g. DNS) can be edited and new rules can be created. In addition the tester verifies the functionality of the DUTs firewall rule set by editing and/ or creating 10 different filter rules and verify the effectiveness of these changed/ new rules.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUTs firewall rule set allows the authenticated end-user to define rules for incoming and outgoing network traffic. Functional tests have confirmed the effectiveness of the changes to the rule set.

TR.F.5 The firewall functionalities of the DUT MUST be enabled after *initialization*. After *initialization* the firewall SHOULD allow all outgoing communication from the private network and deny all not requested incoming communication from the public network.

TP.F.5.1 The tester verifies that the DUTs firewall functionality is enabled after *initialization*.

This Test Procedure depends on the DUTs state *initialized*.

Following the user guidance the tester sets the DUT into operation by changing the DUTs state from *factory setting* to *initialized*.

First after *initialization* the tester verifies using the access methods listed in Section 3.6, Table 13, to configure the DUT, that the DUTs firewall functionality is active and the initial (preset) firewall filter rules are loaded (active).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able verify that after initialization of the DUT the firewall filter rules are active and functional.

TP.F.5.2 The tester verifies by functional testing that these initial (preset) firewall filter rules allow all outgoing network traffic (from the private network segments to the Internet) and rejects all new incoming network traffic (from the public network, i.e. Internet).

This Test Procedure depends on the DUTs state *initialized*.

The tester performs a review of the DUTs firewall filter rules using an access method listed in Section 3.6, Table 13, to configure the DUT. Alternatively the review can be performed on the technical documentation provided by the applicant/ manufacturer as referenced in the ICS, Section 3.1.1, Table 3.

The tester verifies by functional testing that these initial (preset) firewall filter rules are functional and enforce the following rules:

- ACCEPT all outgoing network traffic from the private network segments to the Internet (public network).
- ACCEPT all outgoing network traffic from the DUT itself to the Internet.
- REJECT all incoming (new) network traffic from the Internet to the DUT itself. ACCEPT all established/ related network traffic in this direction.
- REJECT all incoming (new) network traffic from the Internet to any private network segment. ACCEPT all established/ related network traffic in this directions.

The above described rule set is typically implemented by a DUT performing Network Address Translation (NAT).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify the DUTs initial firewall filter rules by functional testing according to the rules given above.

4.7 Module G - Domain Name System (DNS)

TR.G.1 The DUT SHOULD allow the end-user to configure a different DNS server.

TP.G.1.1 The tester verifies that the DUT provides configuration options to use a different DNS server.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

The tester performs a review of the applicants assertions and the referenced user guidance and technical documentation as stated in the ICS, Section 3.1.1 (Table 2 and Table 3) and Section 3.9 to identify the implemented DNS functionality.

The tester verifies using an access method listed in Section 3.6, Table 13, to configure the DUT, that the authenticated end-user is able to configures a different DNS server. Functional testing supports the testers evidence that this configuration is effective.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to configures and tests a different DNS server using a known access method (Table 13).

TR.G.2 The DUT SHOULD implement mechanisms to prevent so called rebind attacks.

TP.G.2.1 The tester verifies by functional testing that the DUT provides mechanisms to prevent rebind attacks.

This Test Procedure depends on all states of the DUT.

The tester performs a review of the applicants assertions and the referenced user guidance and technical documentation as stated in the ICS, Section 3.1.1 (Table 2 and Table 3) and Section 3.9 to identify the implemented functionality to prevent rebind attacks.

The tester performs functional testing to verify that the DUT provides mechanisms to prevent rebind attacks. The test setup includes a malicious DNS server setup configured to provide IP addresses of a private address range for public DNS host queries (e.g. https://tools.kali.org/sniffingspoofing/rebind). The tester configures the DUT using an access method listed in Section 3.6, Table 13, to use this malicious DNS server.

Criteria to Pass

This Test Procedure is successfully passed, if the DUT does not forward/ accept DNS response packets from a public DNS server containing a private IP address for a public domain name (request).

TR.G.3 Source ports and transaction-IDs of the DNS protocol MUST be selected randomly by the DUT.

TP.G.3.1 The tester verifies by functional testing that the DUT selects randomly the source ports and transaction-IDs of the DNS protocol.

This Test Procedure depends on all states of the DUT.

The tester performs functional testing to verify that the DUT selects randomly the source ports and transaction IDs of the DNS protocol to prevent DNS spoofing. The tester configures the DUT to use a different (test-) DNS server addressable by the public network. The network traffic between the DUT and this (test-) DNS server is monitored and analyzed using tools like wireshark or tcpdump and a network tap device at the network interface of the (test-) DNS server.

The tester performs at least 100 different DNS queries to this (test-) DNS server. The captured traffic is analyzed and the source ports of the DUTs packets and the transaction-IDs are extracted and collected in a list.

For these 100 source port values and 100 transaction-IDs the tester performs statistical analysis to verify that these values are randomly generated. The tester is free to use tools like the DNS port test from the Domain Name System Operations Analysis and Research Center (https://www.dns-oarc.net).

If the DUT does not allow to configure a different DNS server the applicant/ manufacturer MUST provide details about the DNS implementation. The tester MUST be able to verify the DUTs functionality for this specific topic by documentation review.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT selects randomly the source ports and transaction-IDs of the DNS protocol to prevent DNS spoofing.

TR.G.4 The DUT MUST support forwarding of DNSSEC packets according to [IETF RFC 6781].

TP.G.4.1 The tester verifies by functional testing that the DUT forwards DNSSEC packets according to [IETF RFC 6781 and the contained RFC in it].

This Test Procedure depends on all states of the DUT.

The tester performs functional testing to verify that the DUT forwards DNSSEC packets. Using a test system in the private network segment (LAN or WLAN) the tester can use tools like DNSSEC-TRIGGER (https://nlnetlabs.nl/projects/dnssec-trigger/about/) to force the client to use a DNS server with DNSSEC support (e.g. server of the https://securedns.eu/ or https://digitalcourage.de/ projects). The network traffic between the test client and the DUT can be monitored and analyzed to verify this Test Procedure. The tool "dig" using the query option "+dnssec" indicates with the flag "ad" DNSSEC support.

The tester verifies the assertions of the applicant/ manufacturer in Section 3.9 to verify that the implementation was done according to the recommendations given in [IETF RFC 6781 and the contained RFC in it].

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT forwards DNSSEC packets send from a client within a private network segment.

TR.G.5 **The DUT MUST support forwarding of DANE packets according to [IETF RFC 6698].**

TP.G.5.1 The tester verifies by functional testing that the DUT forwards DNS DANE packets according to [IETF RFC 6698].

This Test Procedure depends on all states of the DUT.

The tester performs functional testing to verify that the DUT forwards DNS DANE TLSA records (TLSA queries). Using a test system in the private network segment (LAN or WLAN) the tester can use a domain with DANE support (e.g. bund.de) to perform dns queries and verify the TLSA record.

The tester verifies the assertions of the applicant/ manufacturer in Section 3.9 to verify that the implementation was done according to the recommendations given in [IETF RFC 6698].

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT forwards DNS DANE packets according to [IETF RFC 6698].

4.8 Module H - Dynamic Host Configuration Protocol (DHCP)

TR.H.1 **The DUT MUST support using Dynamic Host Configuration Protocol (DHCP) for devices connected on the LAN and WLAN interface.**

TP.H.1.1 The tester verifies by functional testing that the DUT provides DHCP support for devices connected to any LAN or WLAN interface of the DUT.

This Test Procedure depends on all states of the DUT.

The tester verifies the assertions of the applicant in Section 3.3, Table 6. For each private interface (LAN or WLAN) DHCP as a mandatory service MUST be addressed.

The tester performs functional testing to verify for each LAN or WLAN interface listed in Table 6 that the DHCP service of the corresponding interface is functional and provides IPv4 or IPv6 addresses. If necessary the tester uses an access method listed in Section 3.6, Table 13, to enable DHCP for the interface to be tested.

Criteria to Pass

This Test Procedure is successfully passed, if functional testing provides evidence, that the DUT provides DHCP support for IPv4 and if supported IPv6 devices connected to any private interface.

TR.H.2 **The DUT SHOULD provide an option to manually set the DNS server being used by all devices connected to the DUT via DHCP. The DNS server configured in DHCP-Option 6 SHOULD be the DNS server manually configured or the DNS server provided by the IAP.**

TP.H.2.1 The tester verifies that the DUT provides a configuration option for its DHCP service(s) to distribute a manual configured IPv4 and/ or if supported IPv6 DNS server IP for all devices connected to the DUT via DHCP.

This Test Procedure depends on all states of the DUT.

Using an access method listed in Section 3.6, Table 13, the tester configures the DUTs DHCP service(s) for its private network interface(s) to distribute a manual configured DNS server IP for all devices connected to the DUT via DHCP.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT provides an option to manually set the IPv4 and/ or if supported IPv6 DNS server being used by all devices connected to the DUT via DHCP.

TP.H.2.2 The tester verifies by functional testing that the DUTs DHCP service(s) for the private network interface(s) distribute(s) the manually configured DNS server IP or the DNS server IP provided by the IAP in the DHCP-Option 6 (only IPv4).

This Test Procedure depends on all states of the DUT.

The tester performs functional testing for each LAN or WLAN interface listed in Table 6. Using a test system configured to use DHCP service to retrieve an IP address the tester monitors in each network segment the network traffic between this test system and the DUT using tools like tcpdump or wireshark. The tester verifies that the DHCP service of the corresponding interface provides the manual configured DNS server IP address or the DNS server IP provided by the IAP in the DHCP-Option 6. This is only applicable for IPv4.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify for each private network segment that the DUT provides the manual configured DNS server IP address or the DNS server IP provided by the IAP in the DHCP-Option 6.

4.9 Module I - Factory Reset

TR.I.1 The DUT MUST allow an authenticated end-user to reset the DUT back to *factory setting* from an *initialized* or end-user *customized* state by deleting the personal data and settings of the end-user from the DUT.

TP.I.1.1 The tester verifies that the DUT provides a factory reset functionality for an authenticated end-user.

This Test Procedure depends on the DUTs states *initialized* and *customized*.

Using an access method listed in Section 3.6, Table 13, to configure the DUT, the tester verifies that the DUT provides a factory reset functionality for an authenticated end-user.

Hardware functionalities to perform a factory reset (e.g. reset button, telephone code using an analog telephone) without authentication of the end-user are accepted.

The tester verifies that all identified functionalities to perform a factory reset are described in the user-guidance and addressed in the ICS, Section 3.11, Table 23.

The tester performs a factory reset from the *initialized* and from the end-user *customized* state using all identified factory reset functionalities (software and hardware) and verifies that after the reset the DUT is back in *factory setting* and all personal data and settings of the end-user are deleted from the DUT.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to use the DUTs factory reset functionalities according to the user-guidance. The tester is able to verify that after factory reset all personal data and settings of the end-user are deleted from the DUT.

4.10 Module J - Internet Protocol version 6 (IPv6)

TR.J.1 The DUT SHOULD implement Internet Protocol version 6 (IPv6) and offer its services accordingly.

TP.J.1.1 The tester verifies that the DUT provides IPv6 support.

This Test Procedure depends on all states of the DUT.

The tester verifies that the DUT provides IPv6 support for all public and private network interfaces listed in Table 6 and Table 10. Using an access method listed in Section 3.6, Table 13, to configure the DUT, the tester verifies the configuration options for all network interfaces.

Using an IAP providing IPv6 support the tester configures the DUT to use the IPv6 protocol for the public and private network interfaces. The tester verifies the functionality for all private network interfaces using a test client with IPv6 support.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to configure the DUT for IPv6 support and verifies this by functional testing.

TR.J.2 It is RECOMMENDED that the DUT only supports the types of ICMPv6 messages marked with an "X" in Table 7 of [TR-03148].

TP.J.2.1 The tester verifies by functional testing that the DUT only supports the ICMPv6 messages marked with an "X" in the following Table 28.

This Test Procedure depends on all states of the DUT.

The tester verifies by functional testing for all public and private network interfaces listed in Table 6 and Table 10 that the DUT only supports the ICMPv6 messages marked with an "X" in the following Table 28.

ICMPv6 message type	in the private network	from the public network	to the public network
Destination unreachable (1)	X	X	X
Packet too big (2)	X	X	X
Time exceeded (3)	X	X	X
Parameter Problem (4)	X	X	X
Echo-Request (128)	X (1)		X (1)
Echo-Response (129)	X (2)	X (2)	
Multicast (130-132,143, 151-153)	X (3)	X (3)	X (3)
Router (133, 134)	X (3)		
Neighbor (135,136)	X (3)	X (3)	X (3)
Redirect (137)	X (3/ 4)		
ICMP-Information (139)	X (1)		
ICMP-Information (140)	X (2)		
Reverse-Neighbor (141)	X (1)		
Reverse-Neighbor (142)	X (2)		

Table 28: ICMPv6 message types

The following annotations to Table 28 apply.

(1) From the management station

(2) To the management station

(3) Without forwarding

(4) From the router

Test setup: The DUT is configured in *initialized* to use the Internet Protocol version 6 (IPv6). One IPv6 test system is used in the Internet and in each active private network segment (private WLAN, private LAN). Each test system is capable to send ICMPv6 packets (e.g. fping) and to sniff the local network segment using a network sniffer (e.g. tcpdump, wireshark). A network tap could be used to support testing.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify by functional testing that the DUT only supports the ICMPv6 messages marked with an "X" in Table 28.

TR.J.3 The DUT MUST NOT forward inbound IPv6 traffic, if it does not belong to a known connection.

TP.J.3.1 The tester verifies by functional testing that the DUT does not forward inbound IPv6 traffic if it does not belong to a known connection.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The tester performs a review of the DUTs IPv6 firewall filter rules using an access method listed in Section 3.6, Table 13, to configure the DUT. Alternatively the review can be performed on the technical documentation provided by the applicant/ manufacturer as referenced in the ICS, Section 3.1.1, Table 3.

The tester verifies by functional testing that these initial (preset) IPv6 firewall filter rules are functional and enforce the following rules:

- REJECT all incoming (new) IPv6 network traffic from the Internet to the DUT itself. ACCEPT all established/ related IPv6 network traffic in this direction.
- REJECT all incoming (new) IPv6 network traffic from the Internet to any private network segment. ACCEPT all established/ related IPv6 network traffic in this directions.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify the DUTs initial IPv6 firewall filter rules by functional testing according to the rules given above.

4.11 Module K - Remote Configuration

TR.K.1 **For retail devices that are not pre-configured with end-user specific settings no remote configuration MUST be active before *initialization*.**

TP.K.1.1 The tester verifies that the DUTs remote configuration functionality is not active before *initialization* if the DUT is a retail device without pre-configured end-user specific settings.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*.

The DUT may offer remote configuration of the device either by the IAP or the manufacturer.

The tester verifies the assertions of the applicant in Section 3.13. If the DUT is not pre-configured with end-user specific settings and belongs to the retail device class the tester verifies that no remote configuration functionality is active before the DUT is in state *initialized*.

Using the list of the DUTs remote configuration services identified in TR.B.4 the tester analyses during the *initialization* process that these services are not active.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the remote configuration service is not active before the DUT is in its state *initialized*.

TR.K.2 **Remote configuration MUST only be allowed with an encrypted and (server-) authenticated connection according to [TR-02102-2] or other techniques fulfilling the same security requirements.**

TP.K.2.1 The tester verifies by functional testing that the communication used for remote configuration is encrypted and (server-) authenticated using TLS according to [TR-02102-2], *Section 3: Recommendations*.

This Test Procedure depends on all states of the DUT.

For each remote configuration functionality identified in TR.B.4 the tester verifies the method to encrypt and (server-) authenticate the communication. The tester verifies if these methods use different TLS implementations or all methods are linked to the same implementation.

The tester performs functional testing to verify the following details of the recommendations given in Section 3 of [TR-02102-2]. Other techniques fulfilling the same security requirements are accepted.

These tests can be performed using tools like wireshark or tcpdump.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

TLS Requirements:

- The TLS version MUST be TLS 1.2 or TLS 1.3.
- The requested minimum key lengths stated in Table 13 of [TR-02102-2] are implemented. The TLS implementation does not use any keys not fulfilling this requirement.

Requirements for TLS 1.2:

- Only cipher suites listed in Section 3.3.1 of [TR-02102-2] are supported.

- Cipher suites using Pre-shared Keys (TLS_PSK_*) are not supported.
- Only the signature procedures rsa, dsa and ecdsa according to Table 6 of [TR-02102-2] are implemented.
- SHA-1 is prohibited for all digital signatures. Only hash functions listed in Table 7 of [TR-02102-2] are acceptable.
- Only the Diffie-Hellman groups listed in Table 5 of [TR-02102-2] are supported.

Requirements for TLS 1.3:

- Cipher suites using Pre-shared Keys (psk_ke, psk_dhe_ke) are not supported.
- Only the Diffie-Hellman groups listed in Table 9 of [TR-02102-2] are supported.
- Only the signature procedures listed in Table 10 and Table 11 of [TR-02102-2] are implemented.
- Only cipher suites listed in Table 12 of [TR-02102-2] are supported.

The tester verifies the (server-) authentication mechanism of the communication used for remote configuration. The DUT MUST authenticate the remote configuration server/ client before accepting the remote configuration.

If the communication to provide remote configuration functionality is based on a server implementation on the DUT the following aspect MUST be considered by the tester:

> In addition to the tests required above the tester MUST verify the TLS implementation to be robust against common attack vectors like heartbleed or POODLE vulnerability. One recommended tool is testssl.sh (https://testssl.sh/), which provides an output showing the found issues in red lines, which SHOULD be green, except it is a false positive. The tester MUST analyze the red lines.
>
> Alternative tools can be used, but all tools MUST be mentioned in the test report including log files and/ or screenshots.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the communication for remote configuration is implemented according to [TR-02102-2] *Section 3: Recommendations* as requested above and (server-) authentication is performed. Other techniques fulfilling the same security requirements are accepted. In addition the tester find no common vulnerabilities in server implementations using test tools like testssl.sh.

TR.K.3 All private cryptographic keys and secrets MUST NOT be shared by multiple devices in the *factory setting* and *initialized* state.

TP.K.3.1 The tester verifies the assertions of the applicant given in Section 3.13, Table 24.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*. It is not required for *customized*.

The applicant MUST state that no cryptographic key or secret is shared between multiple DUTs.

If the generation method for any private cryptographic key or secret is not disclosed by the applicant or manufacturer the tester MUST verify this Test

Procedure using ten DUTs of the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any private cryptographic key or secret used for remote configuration demonstrates that the generated key value or secret is unique, except by chance.

TR.K.4 It MUST be visible to the end-user if remote configuration is currently activated.

TP.K.4.1 The tester verifies that the status of remote configuration (active/ inactive) is visible to the end-user.

This Test Procedure depends on all states of the DUT.

The same requirement is subject of TP.D.27.1.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify TP.D.27.1.

4.12 Module L - Voice over IP (VoIP)

TR.L.1 If the DUT provides support for Voice over IP (VoIP) this functionality SHOULD be implemented in a way that the end-user can turn off the functionality completely.

TP.L.1.1 The tester verifies that the DUTs VoIP functionality can be turned off completely by the end-user.

This Test Procedure depends on all states of the DUT.

The tester verifies using an access method listed in Section 3.6, Table 13, to configure the DUT, that the VoIP functionality can be turned off completely.

The function verification is done in TP.B.3.2, which is verified by the tester.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to turn off the VoIP functionality completely.

TR.L.2 If the DUT provides support for Voice over IP (VoIP) this functionality SHOULD be implemented in a way that certain phone numbers can be blocked in a dedicated black list.

TP.L.2.1 The tester verifies that the DUTs VoIP functionality provides a dedicated black list to allow the end-user to block certain phone numbers.

This Test Procedure depends on the DUTs state *initialized* and *customized*.

The tester verifies using an access method listed in Section 3.6, Table 13, to configure the DUT, that the VoIP functionality provides a dedicated black list to allow the end-user to block certain destination phone numbers.

The tester uses an *initialized* DUT with activated VoIP functionality for testing. The tester configures the VoIP black list with 5 different destination phone numbers including numbers of special rate services (e.g. 0900, 0137). For all possible telephone interfaces (e.g. analog, ISDN, DECT, LAN, WLAN) the tester verifies that the destination phone numbers of the black list are blocked. The log file of the DUT for the VoIP functionality could be used as supporting evidence.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is not able to call a destination number of the VoIP black list using any phone interface of the DUT.

TR.L.3 The DUT MUST NOT respond to SIP requests to unknown communication partners on the WAN interface.

TP.L.3.1 The tester verifies that the DUT does not respond to SIP request of unknown communication partners on the WAN interface.

This Test Procedure depends on the DUTs states initialized and customized.

The tester uses an *initialized* DUT with activated VoIP functionality for testing. Using a test SIP server in the Internet or tools like svmap of the SIPVicious project the tester verifies if the DUT respond to SIP requests of this server/ tool. The communication between the test SIP server and the DUT can be monitored at the side of the test SIP server using tools like wireshark or tcpdump. The tester verifies that no SIP packets send by the DUT can be monitored at the interface of the test SIP server.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the DUT does not respond to SIP requests send by the testers SIP server.

TR.L.4 The WAN interface does not have extensions that do not require an authentication (noauth).

TP.L.4.1 The tester verifies that the DUTs WAN interface(s) do(es) not have extensions that do not require an authentication (noauth).

This Test Procedure depends on the DUTs states initialized and customized.

The tester uses an *initialized* DUT with activated VoIP functionality for testing. Using a test SIP server in the Internet or tools like svwar of the SIPVicious project the tester verifies if the DUTs WAN interface provides extensions that do not require an authentication (noauth).

Criteria to Pass

This Test Procedure is successfully passed, if the tester is not able to identify any extensions on the DUTs WAN interface(s) that accept noauth.

TR.L.5 The services providing VoIP functionalities MUST only be running as long as IP based communication is activated.

TP.L.5.1 The tester verifies by functional testing that the DUTs VoIP functionalities are only running as long as IP based communication is activated.

This Test Procedure depends on all states of the DUT.

The tester verifies that the DUTs VoIP functionalities are stopped as soon as the IP based communication is deactivated. Using an access method listed in Section 3.6, Table 13, to configure the DUT, the tester deactivates the DUTs IP based communication (e.g. deactivates the WAN interface(s)) and verifies that the VoIP service(s) are stopped.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to verify that the VoIP functionalities of the DUT are stopped as soon as the IP based communication is deactivated.

4.13 Module M - Virtual Private Network (VPN)

TR.M.1 **If the DUT offers a Virtual Private Network (VPN) feature it SHOULD allow the end-user to configure it as a VPN server.**

TP.M.1.1 The tester verifies that the VPN feature of the DUT can be configured by the end-user as a VPN server.

This Test Procedure depends on the DUTs state *customized*.

Using an access method listed in Section 3.6, Table 13, to configure the DUT, the tester configures the VPN functionality of the DUT (e.g. IPsec, L2TP over IPsec, OpenVPN). The tester verifies that this VPN functionality can be configured as a VPN server.

Criteria to Pass

This Test Procedure is successfully passed, if the tester is able to configure the VPN functionality of the DUT as a server.

TR.M.2 **The cryptographic parameters for IPsec defined in [TR-02102-3] SHOULD be used accordingly.**

TP.M.2.1 The tester verifies by functional testing that for IPsec based VPN functionalities the DUTs implementation is compliant with the requirements of [TR-02102-3].

This Test Procedure depends on the DUTs states *initialized* and *customized*.

For each IPsec based VPN solution of the DUT the tester verifies that the implementation is according to [TR-02102-3], Section 3 Recommendations.

The tester performs functional testing to verify the following details of the recommendations given in Section 3 of [TR-02102-2]. These tests can be performed using tools like wireshark, tcpdump or ike-scan.

The tester MUST detail the test setup. Log files and/ or pictures of the used tools MUST be provided.

Requirements for Internet Key Exchange (IKE):

- Only protocol version IKEv2 is recommended. The use of protocol version IKEv1 is accepted if IKEv2 is implemented too. The tester MUST verify all implementations.
- Only the recommended encryption techniques listed in Table 2 of [TR-02102-3] are implemented to protect the IKE messages.
- Only the pseudorandom functions (PRF) listed in Table 3 of [TR-02102-3] are implemented for key generation.
- Only the recommended functions to protect the integrity of the IKE messages listed in Table 4 of [TR-02102-3] are implemented.
- Only the recommended Diffie-Hellmann groups listed in Table 5 of [TR-02102-3] are implemented for key exchange.
- Only the authentication mechanisms listed in Table 6 of [TR-02102-3] are implemented.

Requirements for IPsec:

- Only the encryption methods listed in Table 7 of [TR-02102-3] are implemented to encrypt ESP packets.

- Only the mechanisms listed in Table 8 of [TR-02102-3] are implemented to protect the integrity of the ESP packets.
- Only the mechanisms listed in Table 9 of [TR-02102-3] are implemented to protect the integrity of the AH packets.

The tester verifies that the IKE-SA-Lifetime is configured to not exceed 24 hours whereas the IPsec-SA-Lifetime does not exceed 4 hours.

Criteria to Pass

This Test Procedure is successfully passed, if the tester can verify that the IPsec VPN functionality of the DUT is implemented according to [TR-02102-3] *Section 3: Recommendations*.

TR.M.3 All private cryptographic keys and secrets MUST NOT be shared by multiple devices in the *factory setting* and *initialized* state.

TP.M.3.1 The tester verifies the assertions of the applicant given in Section 3.15, Table 25.

This Test Procedure depends on the DUTs states *factory setting* and *initialized*. It is not required for *customized*.

The applicant MUST state that no cryptographic key or secret is shared between multiple DUTs.

If the generation method for any private cryptographic key or secret is not disclosed by the applicant or manufacturer the tester MUST verify this Test Procedure using ten DUTs of the same manufacturing batch (e.g. all samples are taken from the same production series out of the same production line at the same time).

Criteria to Pass

This Test Procedure is successfully passed, if the generation method for any private cryptographic key or secret used for any VPN functionality of the DUT demonstrates that the generated key value or secret is unique, except by chance.

Appendix

Reference Documentation

IEEE 802.11i	IEEE: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications
IETF RFC 2119	IETF: Key words for use in RFCs to Indicate Requirement Levels
IETF RFC 6698	IETF: The DNS-Based Authentication of Named Entities (DANE)
IETF RFC 6781	IETF: DNSSEC Operational Practices, Version 2
SOG-IS	SOG-IS Crypto working Group: Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, current version (https://www.sogis.eu/uk/supporting_doc_en.html)
TR-02102-2	BSI: TR-02102-2; Cryptographic Mechanisms: Recommandations and Key Lengths: Use of Transport Layer Security (TLS)
TR-02102-3	BSI: TR-02102-3; Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)
WSC2	Wi-Fi Alliance: Wi-Fi Simple Configuration Technical Specification v2.0.2

Abbreviations

Abbreviation	Meaning
2FA	two-factor authentication
AES	Advanced Encryption Standard
AH	Authentication Header
CBC	Cipher Block Chaining
CCMP	Counter-Mode/ CBC-MAC Protocol
CSRF	Cross-Site-Request-Forgery (CXRF or XSRF)
CVSS	Common Vulnerability Scoring System
DANE	DNS-based Authentication of Named Entities
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DUT	Device Under Test
EoS	End of Service
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
FTTH	Fibre-to-the-Home
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
MAC	Media Access Control; Message Authentication Code
MSD	Mass Storage Device (e.g. USB MSD)
NFC	Near Field Communication
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
NAS	Network Attached Storage
NAT	Network Address Translation
PRF	pseudorandom functions
PSK	pre-shared key
rDNS	Reverse DNS Lookup
SMTP	Simple Mail Transfer Protocol

SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WPS	Wi-Fi Protected Setup
WSC[5]	Wi-Fi Simple Configuration

Table 29: Abbreviations

5 "Wi-Fi Simple Configuration" (WSC) refers to the protocol version 2 (WSC2), certified in the Wi-Fi Protected Setup program (WPS). Early in 2006 the "Wi-Fi Protected Setup", shortcut also WPS, refers to the former version 1 of the WSC protocol. The acronym WPS is still commonly used to refer to the connection techniques like WPS PIN, WPS push button or WPS NFC specified in the WSC protocol. In this test specification WSC/ WSC2 is used to refer to the protocol in general and WPS PIN, WPS push button or WPS NFC to refer to the connection techniques (specified in the WSC protocol).