BSI TR-03148-P:  
Test Specification

Implementation Conformance Statement (ICS)

Editable  
  
Version: 1.1  
Date: 30/04/2020

# 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.

## General

### 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 1: 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 2: Technical Documentation Reference

### 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 3: Identification of the DUT

## Applicability of Test Requirements

The applicant is asked to fill in the following Table 4: 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 [TR-03148-P] *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.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.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.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.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.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.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.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.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.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 4: Applicability of Test Requirements

## Module A - Private Network

Using the following Table 5 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]](#footnote-2) | Port/ Protocol | Description |
| --- | --- | --- | --- | --- |
|  | [factory] |  |  |  |
|  | [initialized] |  |  |  |
|  | [customized] |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 5: 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]](#footnote-3) | Description |
| --- | --- | --- | --- |
|  | [customized] |  |  |
|  | [initialized] |  |  |
|  | [factory] |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 6: Private Network Interfaces and client software of the DUT

### Local Area Network (LAN) Interfaces

No questions for the Implementation Conformance Statement.

### 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)

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 7: 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 8: 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)

## Module B - Public Network

Using the following Table 9 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]](#footnote-4) | Port/ Protocol | Description |
| --- | --- | --- | --- | --- |
|  |  | [factory] |  |  |
|  |  | [initialized] |  |  |
|  |  | [customized] |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 9: 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]](#footnote-5) | Description |
| --- | --- | --- | --- |
|  | [customized] |  |  |
|  | [initialized] |  |  |
|  | [factory] |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 10: Public Network Interfaces and client software of the DUT

### Wide Area Network (WAN) Interfaces

No questions for the Implementation Conformance Statement.

## 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 2, 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 11: Functionalities of the DUT

## Module D - Configuration and Information

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

1. configure the DUT and/ or
2. 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 12: List of access methods

If passwords are used to restrict access to a method listed in Table 12 the following password policies are implemented.

| Policy | Description |
| --- | --- |
| password policy A |  |
| password policy B |  |
|  |  |

Table 13: 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 14: List of preset passwords

If passwords are used to restrict access to a method listed in Table 12 the DUT provides the following procedures for an authenticated end-user to change his password:

| procedure | Description |
| --- | --- |
| A |  |
| B |  |
|  |  |

Table 15: 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 1.6, Table 12, 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 16: 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 secrets | generated by/ unique per DUT | alternative authentication method |
| --- | --- | --- | --- |
| [customized] |  |  |  |
| [initialized] |  |  |  |
| [factory] |  |  |  |

*Table 17: 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 18 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 18: Security relevant events

## 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 2, 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 19: 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 2, Technical Documentation Reference).

| Authentication mechanism | Description and documentation reference |
| --- | --- |
| digital signature |  |
|  |  |
|  |  |
|  |  |

Table 20: 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 21: 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)

## 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)

## 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)

## 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)

## 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 1, User Guidance Reference).

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

Table 22: Factory Reset Mechanisms

## Module J - Internet Protocol version 6 (IPv6)

No questions for the Implementation Conformance Statement.

## 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 23: Remote configuration functionalities

## Module L - Voice over IP (VoIP)

No questions for the Implementation Conformance Statement.

## 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 24: VPN cryptographic keys and secrets

1. Please refer to Table Fehler: Verweis nicht gefunden, Fehler: Verweis nicht gefunden, for the interpretation of this term. [↑](#footnote-ref-2)
2. Please refer to Table Fehler: Verweis nicht gefunden, Fehler: Verweis nicht gefunden, for the interpretation of this term. [↑](#footnote-ref-3)
3. Please refer to Table Fehler: Verweis nicht gefunden, Fehler: Verweis nicht gefunden, for the interpretation of this term. [↑](#footnote-ref-4)
4. Please refer to Table Fehler: Verweis nicht gefunden, Fehler: Verweis nicht gefunden, for the interpretation of this term. [↑](#footnote-ref-5)