Security requirement

Home Gateway

Deutsche Telekom Group

Version	3.5
Date	Dec 1, 2023
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.40	Security requirement
Version	**State**	**Status**
3.5	Dec 1, 2023	Released
Contact	**Validity**	**Released by**
Telekom Security psa.telekom.de	Dec 1, 2023 - Nov 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary
Home Gateway

Table of Contents

1. Introduction

This security document has been prepared based on the general security policies of the group.The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard for units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes.

When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

2. Technical Due Dilligence

Req 1	Any additional functionality that is implemented but not required by the Deutsche Telekom Group specification must be disclosed to and agreed with Deutsche Telekom Group.

The Deutsche Telekom Group provides a specification for the Home Gateway that represents all of the Group's device requirements. There generally is no need to implement additional functionality in the Home Gateway, which means functionality that is not covered by the specification. Nevertheless a Home Gateway may be based on an existing design or 3rd party (incl. open source) software components have to be used by the supplier in order to meet the DT Group's requirements. If it is not feasible or possible to fully customize all components of the device in order to solely provide the DT required functionality, then the DT Group must be aware of the additional functionality and DT must agree to it. Examples for "additional functionalities" are:

- A "hidden page" in the web GUI application that e.g. enables to download some diagnostic data.
- Disaster recovery functions: e.g. the possibility to interrupt the boot process in order to flash a corrupted firmware image via TFTP.

So we are only considering functions in the Home Gateway that can be used either remote via network or locally via access to the device's hardware.

Motivation: If the device implements features that are not required by the DT Group's specification then the DT Group's security risk analysis of the device is incomplete and has to be revised. Therefore it is necessary that DT Group is aware of and agrees to any additional functionality of the device.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-1/3.5

Req 2	A map of network services must be provided to and agreed with Deutsche Telekom Group.

The map of network services must indicate all active network services on every network interface of the Home Gateway, i.e. on any WAN and LAN interface. Services bound to the localhost interface only must not be taken into account.
The map must contain the interface, the network tcp/udp port of the service, the implemented protocol and a short description about the service usage. Furthermore it must be stated in which mode of operation a service is activated.

Motivation: Every active network service may result in a potential security risk. DT must be aware of any network service running on the device.

Implementation example: The following table illustrates the information that have to be provided by the map of network services:

Interface	**Port**	**Protocol**	**Remark**
WAN (PPPoE via VLAN 7)	5060/tcp	SIP	SIP User Agent for VoIP telephony. Open, if VoIP telephony is activated. IP ACL limits connetivity to call control.

WAN (PPPoE via VLAN 7)	7547/tcp	HTTP	HTTP Server for Connection Request. Open, if TR-069 is active. IP ACL limits connetivity to ACS.
LAN / WLAN	80/tcp	HTTP	Web GUI for Home Gateway administration
LAN / WLAN	53/udp	DNS	DNS proxy
LAN / WLAN	67/udp	DHCPS	DHCP server for the home network. Open, if DHCP service is active
LAN / WLAN	1900/udp	SSDP	Simple Service Discovery Protocol for TR-064
LAN / WLAN	49000/tcp	SOAP	TR-064 SOAP API via HTTP
LAN / WLAN	49443/tcp	SOAP	TR-064 SOAP API via HTTPS

The layout of the map of network services depends highly on the network architecture of the Home Gateway. Every network interface of the Home Gateway has to be taken into account.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-2/3.5

Req 3 Security algorithms must be disclosed to and agreed with Deutsche Telekom Group.

The vendor has to compile a security concept. This document must describe the implementation of all security features for the production (within a production support software) or within the Home Gateway's firmware. Especially the following information must be provided with the security concept:

- The algorithm for the generation of the pre-configured device passwords
- The algorithm for the generation of the pre-configured WLAN passwords
- The algorithm for the protection of confidential data in the firmware image file
- The key generation and encryption algorithms for the protection of confidential data in the Home Gateway (local storage and backup file)
- Integrity protection mechanism of the image file, of the bootloader, the kernel and the filesystem during boot procedure
- Integration of specific hardware security measures (SoC security features)
- Security hardening of the linux OS and the applications

The vendor must deliver a documentation and agree on its content with the Deutsche Telekom Group. Upon request of Deutsche Telekom Group the vendor must provide sample data sets e.g. of the generated passwords/keys.

Motivation: In the context of the technical due dilligence Deutsche Telekom Group wants to review some of the security algorithms implemented by the vendor. The description and -- upon request -- the sample data sets will help Deutsche Telekom Group to perform this task.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-3/3.5

Req 4	The vendor must provide release notes for each firmware that comprise a list of software components including their release information and security patch level.

The release notes must be provided as a companion documentation to the firmware delivery.

Motivation: In the context of the technical due dilligence Deutsche Telekom Group wants to assess whether the vendor implements only up to date software components including the latest security patches in the firmware release.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-4/3.5

Req 5	The vendor must provide an engineering version of each firmware release that features an access to a root shell via LAN/WLAN interface.

The shell access must be implemented via the SSH or the telnet protocol. A password based user authentication is mandatory. The credentials must be disclosed to Deutsche Telekom Group. Device-specific passwords are recommended.

It must be noted that this shell access is only required for the engineering version of the firmware release. The shell access must not be present in any kind of production version. The deactivation of this feature is not sufficient for the production firmware: software components like ssh or telnet server must be removed as well.

Motivation: In the context of the technical due dilligence the root shell access enables Deutsche Telekom Grioup to review the implementation of security requirements that can only be assessed via root shell access on the device.

For this requirement the following threats are relevant:
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-5/3.5

3. General System Hardening

Req 6	The operating system of the Home Gateway must be based on Linux using a latest stable kernel release with long term support.

All features available to mitigate buffer overflows like ASLR (address space layout randomisation) must be activated in the kernel and the latest security patches available must be applied even if a particular patch has to be backported.

Motivation: The Linux operating system provides a robust OS for embedded devices implementing a strong memory protection, some mitigation techniques for buffer overflows and POSIX compliant file system permissions. This enables a sound hardening the setup of a secure Home Gateway. A Home Gateway is used for many years by our customers, therefore a recent LTS release enables a long support period by the Deutsche Telekom Group.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-6/3.5

Req 7	The production version of the firmware release must not implement any kind of shell access or a similar command-line interface at all.

This requirement is related to a shell of the Linux operating system and it applies to all network interfaces as well as to any serial interface on the Home Gateway's printed circuit board: a commandline interface to the linux operating system or a similar commandline feature must not be implemented in the production firmware.

Motivation: Shell access in the production firmware is not required by Deutsche Telekom Group in the production version of a firmware release since such a privileged access enables attacks and reverse engineering of the Home Gateway's internal operation.

For this requirement the following threats are relevant:
- Unauthorized access to the system

For this requirement the following warranty objectives are relevant:

ID: 3.40-7/3.5

Req 8	Log messages must not disclose any confidential data like cryptographic keys and passwords.

This requirement is related to the logging of the Linux kernel as well as to the logging of any application components. Log messages can be accessed via a serial console interface on the Home Gateway's printed circuit board, via direct access to the operating system or via the web GUI of the Home Gateway. In no case any log messages must contain confidential data like the passwords, session keys or other confidential data stored in the file system of the Home Gateway.

Motivation: Confidential data in the Home Gateway must be protected even if an attacker get's access to the operating system or rather the hardware itself.

For this requirement the following threats are relevant:
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-8/3.5

Req 9	The Home Gateway must feature a hardware pushbutton that enables the user to reset the device to a “factory provided state”.

The factory reset must securely delete all customer specific configuration data and restore all configuration files of the Home Gateway to the default state.

Motivation: A customer may want to hand-over the device to a 3rd party. He must be able to delete his personal data on the Home Gateway even if he has only access to the hardware and doesn’t remember the GUI password.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-9/3.5

Req 10	By default only a minimum subset of network services required for the operation of the Home Gateway must be activated.

Network services that are not required for the typical operation of the Home Gateway must be deactivated by default. We consider services like DLNA/UPnP A/V media sharing, File Transfer (FTP) and NAS as optional services that require an explicit activation by the user.
Note that especially the Remote Device Management (TR-069) which is providing automatic firmware updates for the Home Gateway is not considered as an optional service here and thus TR-069 must be activated by default.

Motivation: Every active network service increases the attack surface of the Home Gateway. The device must be configured securely by default and services that are not required to be active by default must be inactive.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-10/3.5

Req 11	If a network service is deactivated by the Home Gateway’s configuration the related TCP/UDP network port on all network interfaces the service was bound to must be closed.

The service’s port can be closed by the firewall or it can be simply deactivated by stopping the service (deamon) which is the recommended solution.

Motivation: The network connectivity to a service that is deactivated must be prohibited in order to mitigate attacks (limit the attack surface).

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data

- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-11/3.5

Req 12	Any application or service on the Home Gateway that implements a password based authentication must mitigate password guessing attacks.

Password guessing attacks must be mitigated by implementing a “tar pit” that slows down the attacker: after each failed authentication a delay mechanism has to block the authentication process for a relevant amount of time. The delay time has to increase after successive authentication attempts failed. The delay mechanisms must be enforced on the server side (i.e. by the Home Gateway) since client side protection mechanisms can be bypassed by an attacker.
Note that at least the following applications and services require a tar pit implementation: the web GUI, the TR-064 service, the NAS and the file transfer service (FTP, FTPS service).

Motivation: A brute force attack one could lead to an unauthorized access to a service. Private data or the Home Gateway’s configuration can be disclosed or altered. This could lead to serious attacks and abuse scenarios. Therefore a tar pit implementation has to mitigate password guessing attacks.

Implementation example: An effective delay mechanism would e.g. delay login attempts for one second after the first authentication failed. The mechanism then would double the delay time after each successive failure (1, 2, 4, 8, 16, 32, 64, ... seconds).

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-12/3.5

Req 13	The TLS implementation of the embedded Linux operating system must support the protocol version 1.2 (TLS v1.2) or newer.

TLS protocol versions older than TLS 1.2 are considered as deprecated since they contain security vulnerabilities. Therefore Telekom backend services consumed by the home gateway support only recent TLS protocol versions like TLS v1.2. The cryptographic parameters for a TLS v1.2 implementation have to be implemented according the Technical Report TR-02102-2 "Cryptographic Mechanisms: Recommandations and Key Lengths" of the German Federal Office for Information Security (BSI).

Older TLS protocol versions than version 1.2 must not be supported any more.

Motivation: Some services of the Home Gateway require TLS support, like remote device management or Email notification. The Home Gateway must be able to support the current security standards of the corresponding DT backends for TLS.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-13/3.5

Req 14	Known vulnerabilities in the software or hardware of the system must be fixed or protected against misuse.

Known vulnerabilities in software and hardware components must be fixed by installing available system updates from the supplier (e.g. patches, updates/upgrades). Alternatively, the use of workarounds (acute solutions that do not fix the vulnerability, but effectively prevent exploitation) is permissible. Workarounds should only be used temporarily and should be replaced by a regular system update as soon as possible in order to completely close the vulnerabilities.

Components that contain known, unrecoverable vulnerabilities must not be used in a system.

The treatment of newly discovered vulnerabilities must also be continuously ensured for the entire deployment phase of the system and implemented in the continuous operating processes of security patch management.

Motivation: The use of components without fixing contained vulnerabilities significantly increases the risk of a successful compromise. The attacker is additionally favored by the fact that, as a rule, not only detailed information on vulnerabilities that have already become known is openly available, but often also already adapted attack tools that facilitate active exploitation.

Implementation example: Following the initial installation of an operating system from an official installation medium, all currently available patches and security updates are installed.

Additional information:
The primary sources of known vulnerabilities in software/hardware are lists in the release notes as well as the security advisories from the official reporting channels of the supplier or independent CERTs. In particular, the reporting channels are sensibly integrated into continuous processes of security patch management for a system, so that newly discovered vulnerabilities can be registered promptly and led into operational remedial measures.
As a complementary measure to the detection of potentially still contained types of vulnerabilities that have in principle already become known, targeted vulnerability investigations of the system can be carried out. Particularly specialized tools such as automated vulnerability scanners are suitable for this purpose. Examples include: Tenable Nessus, Qualys Scanner Appliance.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.01-10/7.0

Req 15	The system must be protected against overload situations.

A system must have protective mechanisms that prevent overload situations as far as possible.
In particular, a partial or complete impairment of the availability of the system must be avoided.

Examples of possible protective measures are:

- Limiting the amount of memory (RAM) available per application
- Limiting the maximum sessions of a web application
- Limiting the maximum size of a dataset

- Limiting CPU resources per process
- Prioritizing processes
- Limiting the number or size of transactions by a user or from an IP address over time

Note:
A system can usually not protect itself against network-based attacks with extremely high data or packet rates, the so-called "Distributed Denial of Service" (DDoS) attacks. To defend against DDoS attacks, an upstream solution in the network layer is required.

Motivation: Attackers can try to use up the resources of a system with targeted resource-intensive or large-volume requests, so that the system can no longer fulfill its regular tasks or intended task volumes and the availability of the services offered is effectively disrupted. Limiting the maximum resources that can be used per request made to the system is a fundamental measure to reduce the impact of such denial-of-service (DoS) attacks.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.01-12/7.0

Req 16 The user must be able to deactivate unused services and protocols.

It must be readily identifiable for the user what services and protocols are activated. The user must be able to independently deactivate unwanted services and protocols (e.g. in the device settings).

Motivation: Modern end user devices offer a multitude of functions where often convenience conflicts with data security or data privacy. At any time the user must be able to adjust usage of such functions according to his needs.

Implementation example: Based on a good user interface, or with the help of the user manual, the user can adjust the following settings according to his needs: Usage of temporary storage of secrets (e.g. password-storage in a browser), activation of interfaces (Bluetooth, WLAN, NFC, GPS, ...), usage of cloud-storage services including optional data synchronisation across devices.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.33-5/5.1

Req 17 Protocol stacks available on the device must be implemented robust.

Motivation: If protocol stacks like the IP stack or SIP stack are vulnerable to common threats, it may be possible to conduct Denial-of-Service attacks from remote (i.e., from the WAN network), or a remote attacker can take control over the device.

Implementation example: Well-known attacks against the IP protocol stack are detected and mitigated. Fuzzing tests have been performed against the device, yielding evidence of its robustness properties. Denial-of-Service (DoS) protection is enabled on every active network interface. - Information about well-known attacks can for example be found at organisations like www.sans.org.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.33-47/5.1

4. Bootloader

Req 18	The bootloader must check the integrity of the Linux kernel and of the root file system before the kernel is invoked.

The integrity check of the kernel must ensure that the kernel is upright and authenticated. The integrity check of the root file system must ensure that the partition is faultless. Deutsche Telekom Group requires an integrity protection mechanism but does not specifiy the mechanisms that have to be implemented. If available, SoC-based security mechanisms must be used to implement a secure boot procedure. The vendor can in clearance with Deutsche Telekom Group choose an appropriate implementation for a Home Gateway. The check of the root file system could alternatively be implemented by the kernel.

Motivation: The bootloader must ensure that only upright firmware images can be executed.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-18/3.5

Req 19	The bootloader must not permit the readout of confidential data in plaintext.

Bootloader often send log message via a console interface or they implement a command-line interface for some basic operations. The vendor must limit the capabilities of the bootloader so that confidential data stored in the firmware image (e.g. the root file system) can’t be readout in plaintext. E.g. cryptographic keys or passwords provided by the user are considered as confidential data here.

Motivation: The Home Gateway must protect confidential data from unauthorized readout. Some confidential data like passwords never should be recoverable from the Home Gateway. Even if an attacker has access to the hardware of the device.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-19/3.5

5. Firmware Image File

Req 20	Confidential data in the firmware image file must be stored encrypted using the Advanced Encryption Standard (AES) algorithm.

The requirement applies if confidential data have to be pre-configured within the firmware image file. Credentials (i.e. passwords) and cryptographic keys (e.g. private keys belonging to x509v3 certificates used for TLS client authentication) are considered as confidential data in this requirement.
AES supports key lengths of 128, 192 and 256 bits. The preferred key length for AES is 256 bit. The AES encryption key for the protection of confidential data in the firmware image file is named as “data-encryption-key” in this document.

Motivation: If an attacker analyzes the firmware image file (which is typically available freely for download) he must not be able to disclose confidential data, if such data need to be pre-configured within the firmware image file.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-20/3.5

Req 21	The data-encryption-key must be derived at runtime from a key-specific set of certain attributes stored obfuscated within the firmware image file including a random seed.

The data-encryption-key must not be stored in the firmware image file as a contiguous binary object. The key must be derived at runtime after installing the firmware image in the flash memory. The complexity of the obfuscation algorithm must mitigate that an attacker can identify the set of attributes and the algorithm e.g. by comparing different releases of a firmware image file or by simply decompressing the image file and analyzing its content.

Motivation: An attacker should not be able to easily reverse engineer the algorithm and the storage of the attributes to generate the data-encryption-keys. Otherwise the attacker would be able to decrypt confidential data stored within the firmware image file.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-21/3.5

Req 22	The firmware image file must feature a sound integrity protection mechanism and the integrity of the image file must be validated successfully before the image file is installed in the flash memory of the Home Gateway.

A digital signature of the firmware image is considered as a sound integrity protection mechanism. Appropriate algorithms for digital signatures are e.g. HMAC-SHA-256, RSA or DSA.

Motivation: The integrity of the firmware image file must be guaranteed before the image is installed into flash memory. Therefore a sound integrity protection mechanism must be part of the image file and the integrity of the image must be validated by every software component that is going to install the image file in the flash memory.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:
- Integrity

ID: 3.40-22/3.5

Req 23	The device (e.g. its bootloader) must allow updating the whole device’s firmware.

Motivation: This enables users to update their devices’ firmware in case that errors or vulnerabilities have been found in the firmware.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.33-16/5.1

Req 24	The device must allow a rollback to the last known good firmware in case that the installation of an update/patch has failed.

Motivation: Rollback functionality ensures that a device will be able to continue working with the old firmware version in the case that the integrity of an updated firmware could not be verified successfully. Customers have less fear to install updates and devices are operated with current firmware versions.

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:
- Integrity

ID: 3.33-19/5.1

Req 25	The device must provide a means to notify users of available updates.

The user who is notified may be an administrative user (e.g. in the case of a home gateway). If the device supports notifications, then this function should be used (“push”); otherwise the information can be given in the administrative user interface (“pull”).

Motivation: The installation of updates may yield to service interruption. Depending on the device, different preconditions have to be met in order for an update to be installed without difficulty, e.g. power supply, free memory, type of connection (speed, costs incurred) to the update server, etc. Updates should only be pushed out to the device and their installation should only be enforced, if the update is very security-critical. If the update is not installed automatically, the device administrator has to be made aware of available updates.

Implementation example:

- Mobile operating systems offer energy-efficient notification services (iOS: Apple Push Notification Service, Android: Google Firebase Cloud Messaging).
- Notification may also be done via e-mail. The e-mail address can, e.g., be requested during first use of the

device.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.33-20/5.1

6. Networking and Interfaces

6.1. Firewall

Req 26	The firewall must implement a stateful packet filter.

A stateful firewall performs a stateful packet inspection and keeps track of the state of each connection and it is able to drop inbound protocol data units if they do not belong to a known connection.

Motivation: A stateful packet filter mitigates e.g. spoofing attacks. The stateful packet firewall provides the required security level.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-26/3.5

Req 27	The firewall/network subsystem must implement a strong end system model according to section 3.3.4.2 multihoming requirements of RFC1122.

The Home Gateway acts as a multihomed host according to section 3.3.4.1 of RFC1122. That means the Home Gateway has multiple IP addresses which are associated to at least two physical interfaces that are connected to different networks: the WAN (Internet) and the LAN (home network) interface. According to the discussion within section 3.3.4.2 multihoming requirements of RFC1122 the strong end system model means that outgoing datagrams must be sent on the interface with the source IP address and that incoming datagrams must arrive on the interface with the destination IP address. That means e.g. that it is not possible to connect to the WAN IP address of the Home Gateway via any LAN interface.

Motivation: The strong end system model mitigates DNS-rebinding attacks that target the Home Gateway.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-27/3.5

Req 28	The firewall must be always acitvated.

A user of the Home Gateway must not be able to deactivate the firewall by any device configuration option provided by the web GUI or other device management facilities.

Motivation: The firewall is the most important security feature of the Home Gateway. This service must be always on, operate stable and fault tolerant.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-28/3.5

Req 29	As a default rule for the firewall all incoming connections on any WAN interface must be denied.

The firewall must block unsolicited incoming traffic on any WAN interface unless a dedicated connection or a rule, e.g. a port-forwarding, explicitly allows such traffic.

Motivation: The home network must be protected properly from the Internet.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-29/3.5

Req 30	Forwarding rules to any IP address of the LAN/WLAN interface of the Home Gateway must not be accepted by any device configuration option accessible to the user.

The user must not be able to configure a port forwarding e.g. to port 80 (of the Web-GUI) on the Home Gateway's LAN/WLAN interface.

Motivation: Otherwise the user would be able to make services that are designed for the home network be accessible from the public internet e.g. by a misconfiguration of the device.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-30/3.5

Req 31	Common attack vectors such as SYN Flooding, ICMP Flooding, UDP Flooding, Ping of Death, Smurf attack, LAND attack and IP fragmentation-related attacks must be mitigated adequately by the firewall.

The following attacks must be mitigated by the Home Gateway's network stack or rather by the HG's firewall implementation:

- TCP SYN, ICMP, UDP flooding attacks:
  These flooding attacks involve the sending of many TCP SYN, ICMP or UDP packtes to the intended victim.
- Ping of Death:
  A ping of death is a denial-of-service attack that involves sending a malformed or otherwise malicious ICMP echo request ("ping") to the intended victim's IP address.
- Smurf Attack:
  A smurf attack is a distributed denial-of-service attack in which large numbers of ICMP packets with the intended victim's IP address as a spoofed source IP adress are broadcasted within a network using an IP broadcast address. All host of the broadcast domain would then send their response to the victim's IP address.
- LAND Attack:
  The LAND (local area network denial-of-service) attack involves sending a spoofed TCP SYN packet

(connection initiation) with the intended victim's IP address to an open port as both source and destination. This causes the machine to reply to itself continuously and would lead to a denial of service condition.

- IP fragmentation-related attacks:
  These attacks rely on IP fragmentation in order to conduct the attack. The goal is to attack the reassembly mechanism of the Internet Protocol itself and thus conduct a denial-of-service or rather to undermine firwall rulesets. E.g. the teardrop attack is a Ip fragmentation related denial-of-service attack that involves sending mangled IP fragments with overlapping, over-sized payloads to the target machine.

Please note that the primary target of protection is the Home Gateway itself. The HG must be robust against these attacks as far as possible and as far as feasible. Regarding flooding attacks this e.g. means that the Home Gateway must resist such attacks without any significant service impact for QoS classified traffic like Voice-over-IP traffic.

Motivation: If the IP stack is vulnerable to common threats it may be possible to conduct e.g. Denial of Service attacks from remote (i.e. from the WAN network).

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.40-31/3.5

Req 32	If the device has firewall functionality, an IPv4 stack and NAT functionality (network address translation), the firewall must implement "port-restricted cone" NAT.

A definition of port-restricted cone NAT can be found in RFC3489: An external host with source IP address X and source port P can send a packet to a port of the internal host only if the internal host has previously sent a packet to IP address X on port P.

Motivation: This ensures that only answers to requests sent from the end user device will be processed further. Any unsolicited packets are dropped.

Implementation example: A smartphone with tethering / personal hotspot feature must implement "port restricted cone".

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.33-52/5.1

6.2. Firewall / Network Subsystem with IPv6 Support

Req 33	The IPv6 firewall must enforce a similar network security model than the IPv4 NAT firewall.

The following requirements describe a blueprint for an IPv6 network security model:

- As a default deny any incoming connections to IPv6 hosts in the LAN/WLAN. Exceptions have to be configured per host by the user. But it must not be possible to configure an exception for an IP address of the LAN/WLAN interface of the Home Gateway itself.
- Deny any incoming connection to any port at the WAN interface of the Home Gateway if the connectivity is not needed by a particular service.
- Handle ICMPv6 as restrictive as possible, e.g.:

- The ICMPv6 message types 133/134 for router solicitation and advertisement should be accepted on all network interfaces. These messages must not be forwarded between WAN and LAN/WLAN interfaces and vice versa.
- The ICMPv6 message types 135/136 for neighbour solicitation and advertisement should be accepted on all network interfaces. These messages must not be forwarded between WAN and LAN/WLAN interfaces and vice versa.
- The ICMPv6 message types 128/129 (echo request/reply), 1 (destination unreachable), 2 (packet too big) and 3 (time exceeded) must be accepted on LAN/WLAN and WAN interfaces and only these message types must be forwarded between WAN and LAN/WLAN interfaces.
- Any other ICMPv6 message types must be discarded.

Note that some requirements in the blueprint strongly depend on the IPv6 deployment model in the access network the Home Gateway is intended to interoperate with.

Motivation: Adding IPv6 to the Home Gateway must not compromise the security of the Home Gateway and the home network.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-33/3.5

Req 34	The IPv6 firewall must mitigate the Neighbour Discovery Protocol table exhaustion attack.

The Neighbour Discovery Protocol (NDP) table exhaustion attack is a Denial-of-Service attack: an attacker floods the Home Gateway by advertising bogus neighbours (hosts) as long as the maximum number of entries in the Home Gateway’s internal NDP table has exceeded. In such a case the Home Gateway’s ICMPv6 implementation must fail safe, e.g. delete NDP table entries. This error condition must not result in a Denial-of-Service condition.

Motivation: An attacker must not be able to disturb the operation of the Home Gateway by means of a simple and non-distributed DoS attack like the NDP table exhaustion attack.

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.40-34/3.5

6.3. Wireless LAN

Req 35	The wireless LAN interface must support WPA2 and WPA3. By default the wireless LAN must be encrypted using at least WPA2 and the CCMP protocol.

This requirement is applicable to a private wireless LAN that is implemented according to IEEE802.11 series standards. WP2 and WPA3 provide the security measures to protect a wireless network. It is recommended to implement the WPA2/WPA3 mixed mode by default so that WPA3 enabled clients can already use the most recent WPA version without any reconfiguration of the home gateway.

Motivation: WPA2 CCMP is the most secure encryption method for wireless networks, if not all network clients support WPA3.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-35/3.5

Req 36	The pre-configured WPA2/WPA3 key (i.e. the WLAN password) must be a random and per device unique value.

The term “random” includes the requirement that the pre-configured WPA2/WPA3 key is not related to any attributes of the Home Gateway like MAC addresses, the serial number, etc.

Motivation: A guessable or default WLAN password does not protect the customer’s wireless home network since this password could be considered as weak and could be disclosed by an attacker. Only strong, random and per-device unique WLAN passwords mitigate WLAN fraud.

Implementation example: Proper randomness of the pre-configured WPA2/WPA3 keys can be archived by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described in RFC 4086.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-36/3.5

Req 37	The pre-configured WLAN password must meet the following minimum requirements: a length of 20 characters, consisting of the numbers 0-9.

This statement defines the minimum requirement for a pre-configured WLAN password. It is recommended to use a wider character space, e.g. the numbers 0 - 9 and uppercase letters A – Z.

Motivation: 20 randomly chosen numbers provide enough entropy to mitigate common brute force attacks on the WLAN password but they guarantee that the password can easily be printed on a label on the device without confusing the customer.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-37/3.5

Req 38	It must not be possible to set a WLAN password that is shorter than 8 characters.

Annex M.4 of the IEEE802.11-2012 standard defines a passphrase (i.e. a password) as a sequence of between 8 and 63 ASCII-encoded characters. Although it is technically feasible to derive WLAN keys from shorter passwords, the minimum password length of 8 characters for WPA / WPA2 encrypted wireless networks must be enforced according to annex M.4.

Motivation: This requirement should only define a minimum policy, i.e. our motivation is not to define a strict policy that only allows strong WLAN passwords due to usability reasons.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-38/3.5

6.4. USB Subsystem

Req 39	The Home Gateway must not execute any code that is stored on USB mass storage devices.

Any partitions on external mass storage devices must be mounted as “non-executable”.

Motivation: Executing code from external mass storage devices is not required and it could be abused for attacks.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-39/3.5

Req 40	The USB device class support of the embedded Linux operating system of the Home Gateway must be limited to the required ones.

Typically a Linux operating system supports many different USB device classes which are not required by any functional requirement for the Home Gateway. The device class support for the Home Gateway must be limited to the required one. In a typical Home Gateway scenario e.g. only the device classes "mass storage" and "printer" need to be supported by the firmware.

Motivation: Any additional device class may result in a security risk if someone gets access to the USB port of the Home Gateway.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-40/3.5

6.5. DECT / CAT-iq Subsystem

Req 41	The DECT/CAT-iq base station implemented in the Home Gateway must enforce a mutual authentication between a hand set and the base station.

Hand sets that do not support mutual authentication must be rejected. The DECT base station must implement the recent DSSA2 authentication algorithm. And the "authentication vector" must have a minimum length of 32 bit.

Motivation: Without mutual authentication the DECT connection can not be considered to be secure.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-41/3.5

Req 42	The DECT/CAT-iq base station in the Home Gateway must enforce an encrypted transmission of voice and signalling data to the hand set.

Hand sets that do not support the encrypted data transmission must be rejected. Furthermore the DECT base station must only implement secure encryption algorithms of recent DECT standards like the LU14 algorithm.

Motivation: If the data encryption is not enforced by the Home Gateway it may be able that voice and signalling data is send in plain text and can easily be eavesdropped.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-42/3.5

Req 43	The DECT base station in the Home Gateway must implement a cryptographic strong random number generator so that strong encryption keys are generated.

Cryptographic strong random numbers can be generated by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described e.g. in RFC 4086. Hint: On embedded Linux systems the random number generators provided by the kernel via the two devices /dev/random and /dev/urandom are considered as cryptographic strong random number generators, if the implementation takes care that the initialization of the Linux RNG (the seeding) at system start up provides enough entropy. It is e.g. not recommended that the Linux RNG is seeded by the same constant value at every device start up.

Motivation: Several DECT implementation use weak random numbers in order to generate encryption keys. This enables an attacker to brute force the encryption key and then calls could be eavesdropped.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-43/3.5

7. Web GUI

7.1. Embedded HTTP Server

Req 44	The embedded HTTP server on the Home Gateway must be installed in an absolutely minimum configuration.

Functionality of the HTTP server that is not needed for the Home Gateway operation must be deactivated e.g. by configuration. This includes especially the following requirements:

- Directory listing must be deactivated.
- Only the required HTTP methods must be enabled, in a typical scenario only the HTTP GET and POST methods are requried.
- The HTTP server must NOT support Server Side Includes (SSI).

Motivation: Every additional component may contain security vulnerabilities and may be used to attack the HTTP server.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-44/3.5

Req 45	The web server document root directory must be separated from any Linux system directory and it must not include any files containing confidential information.

Motivation: Files in the web server’s document root can be accessed by an attacker.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-45/3.5

Req 46	The CGI directory must not contain executables which can be used for attacks, e.g. interpreters and shells.

System directories like /bin or /usr/bin on UNIX systems must not be used as a CGI directory. Any sensitive file must not be placed in the cgi-bin directory, because doing so exposes them to anyone who uses the web server. The CGI directory has to be a separate directory in within the document root directory.

Motivation: System executables in the CGI directory can be used for attacks.

For this requirement the following threats are relevant:
- Unauthorized access to the system

For this requirement the following warranty objectives are relevant:

ID: 3.40-46/3.5

7.2. Basic GUI Hardening

Req 47	The web GUI must only be accessible via private LAN/WLAN interfaces.

The Home Gateway must not provide any option to enable the web GUI on a WAN interface.

Motivation: The web GUI enables security relevant configurations of the Home Gateway. In order to protect the GUI application against attacks it has only to be accessible via the home network.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-47/3.5

Req 48	The web GUI must prevent the browser from storing the content of any password in form fields.

This requirement applies to the AutoComplete of form fields with the device GUI password, the Internet access credentials, the credentials for VoIP telephony, and any other credentials. Since AutoComplete makes it easier for malware to get unauthorized access to the confidential form field data.

Motivation: Confidential form field data stored in a web browser are likely to be disclosed.

Implementation example: AutoComplete is deactivated by adding the attribute "autocomplete" with the value "off" in form elements. This can be achieved either directly in an input tag

<input name = "pass" type= "password" autocomplete = "off"/>

or in a form tag

<form name = "form" action = "" autocomplete ="off"> </form>.

The first variant should ensure that any data entered into precisely this field is not stored, while the second variant ensures that data entered in any field on the form is not stored.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-48/3.5

Req 49	Any response of the web GUI application must not contain confidential data that are not absolutely necessary for any use case.

Especially usernames and passwords are considered as confidential data in this requirement. E.g. there exists no use-case to display the configured Internet access password in the web GUI. Therefore the web GUI must not implement any method that enables to readout of this password.

Motivation: The web GUI must not enable to disclose confidential data that are not needed by any use case.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-49/3.5

Req 50	Any input data sent by a client must be validated by the web GUI application.

The minimum requirement for the validation is that at least the parameters length and valid character space have to be checked.

Motivation: The corruption of the Home Gateway configuration will be prevented.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-50/3.5

Req 51	For every request to the web GUI application that causes data to be read or modified, an additional security attribute ("anti-CSRF token") must be incorporated as a hidden field, transmitted and successfully validated by the web application before the requested action is executed.

The anti-CSRF token is a random number, i.e. an attribute that can be predicted by an attacker. The anti-CSRF token must be validated in every request that causes data to be read or modified. If the GUI application detects an invalid token, it must refuse the operation and invalidate the GUI session.
If the realization of a hidden field is not possible or reasonable, e. g. in case of AJAX requests, the anti-CSRF token can be transmitted in a custom HTTP header (e. g. “X-anti-CSRF-Token”).

Motivation: Requests that are not protected in this way are susceptible to cross-site request forgery (XSRF or CSRF, also known as session riding). Here the victim is induced to unwittingly send a prepared HTTP request which then triggers an action in his/her name within a current session. This can happen, for example, when visiting a malicious website that contains a corresponding link, e.g., as an img, script or iframe tag, to another application in such a way that the victim is unaware of this link. The browser follows the link, however, and – as it were, in the background – successfully triggers an action in so far as the victim currently has a valid session for this other application. The incorporation of the token as a hidden field requires that POST requests are to be used for requests that cause a data modification. To ensure comprehensive protection against CSRF, a different anti-CSRF token would have to be used for each individual request in a web application that causes data to be modified. This prevents intercepted anti-CSRF tokens from being used for a CSRF attack.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-51/3.5

7.3. User Authentication

Req 52	The user must authenticate himself by the device password before using the web GUI application.

The web GUI must only support one single user: the device administrator. This user must authenticate using the device password as an authentication credential. An authentication must be mandatory to access any web GUI application components – except the login page itself and a status page that only contains only non-confidential data.

Motivation: The Home Gateway could easily be abused by an attacker if one can access the web GUI without authentication.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-52/3.5

Req 53	A challenge handshake authentication protocol implementing mechanisms comparable to CHAP defined in RFC1994 must be implemented to verify the device password.

The key elements of a RFC1994 compliant CHAP authentication protocol are:

- The Home Gateway initiates every login request by sending a challenge to the client.
- The response to the challenge (the login request) contains the result of a hash function of the concatenated challenge and the device password. No clear text device password will be transmitted.
- The use of a random value as a challenge mitigates replay and – to some extent – brute force attacks.

The challenge C must be generated using at least a 64-bit random number as an entropy source each time before a login page is delivered to a client. Adequate random numbers can be generated by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described e.g. in RFC4086. The length of the challenge must be constant and it must be chosen in such a way that the sum of the minimum password length (in bits) and the length of C (in bits) equals the length of the hash value (in bits). The minimum password length is defined as 48bits. If SHA-256 is used as a hash function then the length of C is 208 bits. The challenge should be encoded as a hexadecimal number (or base64).
The challenge C may be used as an identifier of an unauthenticated session before Login.
The algorithm for the hash function must be a function of the Secure Hash Algorithm (SHA) family that is defined in FIPS180-4. It is recommended to use SHA-1, SHA-224 or SHA-256.

Motivation: The challenge handshake authentication protocol prevents the clear text transmission of the device password: CHAP uses a hash function in order to "encrypt" the device password. A random challenge received by the Home Gateway is concatenated with the password before applying the hash function as a mitigation of replay and brute force attacks. In RFC1994 the algorithm for the hash function is MD5. We do not recommend MD5 here, since this algorithm (extremely fast implementations exists) may easily enable a brute force attack, if a corresponding pair of challenge and response is eavesdropped by an attacker.

Implementation example: The Stanford JavaScript Cryptographic Library "sjcl" currently only implements the SHA-256 hash function. It is recommended to use the "Sjcl.hash.sha-256" library function.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-53/3.5

Req 54	Device passwords must be pre-configured in each Home Gateway that meet the following minimum requirements: • A length of minimum 12 characters. • Unique for each device (a device individual manufacturing default password). • The password consists of a random ASCII character string containing numbers (0 – 9) and letters.

Motivation: An identical standard password for every HG could lead to attacks on devices when the user doesn’t change the default password. These attacks are mitigated by individual device passwords. The limited character space consisting only of numbers enables that the printed device password is easily readable by the customer without having to guess any characters (like the uppercase letter “O” and the number “0”).

Implementation example: Proper randomness can be archived by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described in RFC 4086.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-54/3.5

Req 55	At any password change the following password policy must be enforced for the device password: • The length of the password must be within the range of 8 - 32 characters. • The password must contain characters from two different classes. • Valid classes of characters for the password are uppercase and lowercase letters, numbers and special characters (e.g. “!”§$%&/()=+*#:;.,”).

Motivation: A trivial password could very easily be guessed by an attacker. This trivial password policy only establishes absolute minimum requirements for the GUI password.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-55/3.5

7.4. Session Management

Req 56	The Home Gateway web GUI application must rely on session cookies (cookies that contain a session identifier) to implement an adequate secure session management.

Motivation: A secure session mechanism protects the web GUI access.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-56/3.5

Req 57	A session identifier (session cookie) must be not guessable, that means: • The session identifier must be unique for each session. • The entropy of the session identifier must be at least 64 bit, which means > 20 digits [0...9] or > 10 characters [A-Z, a-z, 0-9]. • Session identifiers must be generated randomly each time a session starts.

Motivation: Since the web GUI is a single user application this quite relaxed requirements for a session identifier define an adequate security level for the Home Gateway. That means it is not feasible for an attacker to guess the one single valid ID of the authenticated user's session.

Implementation example: Proper randomness of a session identifier can be archived by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described in RFC 4086.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-57/3.5

Req 58	The Home Gateway web GUI application must only accept one active authenticated session at any time.

If a new admin session is established that terminates an existing one, then the user should be advised that e.g. he did not log-out correctly.

Motivation: The Home Gateway can only be managed by one administrator.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-58/3.5

Req 59	The Home Gateway web GUI application must provide a logout functionality that enables the user to terminate the current web GUI session.

The logout must invalidate the current GUI session ID immediately.

Motivation: A user must be able to terminate the web GUI session.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-59/3.5

Req 60	The Home Gateway web GUI application must invalidate the authenticated session after a time of inactivity that is not longer than 20 minutes.

Motivation: If a user doesn't logout explicitly the session must terminate after an appropriate time.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-60/3.5

7.5. Transport Security

Req 61	The Web GUI must support Transport Layer Security (TLS).

The Web GUI must support HTTPS by default (i.e. in the factroy provided state).

Motivation: Even in the quite protected Home Network an attacker may be able to eavesdrop messages exchanged between the client and the web GUI of the Home Gateway. Even in this unlikely case the attacker should not be able to disclose confidential data (e.g. passwords) or to alter configuration requests.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-61/3.5

Req 62	The Home Gateway must provide a device specific self-signed sever certificate for TLS.

The TLS server certificate must be generated on the Home Gateway and the private key of the server certificate must be protected properly.

Motivation: In a private home network it is not possible to use a commercial CA that is already trusted by the operating system or browser vendors. Therefore a self-signed certificate will be generated on the device. And the experienced user can manually import this certificate into the trusted root store of his browser or operating system in order to avoid certificate warnings.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-62/3.5

Req 63	A reset to the factory-default state of the Home Gateway must trigger the generation of a new self-signed TLS server certificate.

Motivation: The TLS server certificate is considered as an user-specific object since a user migth import this certificate into this devices/browser. Therefore the current server certificate must be deleted by a fatory reset.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-63/3.5

7.6. Protection of Configuration Data

Req 64	Confidential configuration data must be stored encrypted using the Advanced Encryption Standard (AES).

Especially Usernames and passwords (incl. the WLAN password) are considered as confidential data. These configuration data must be stored encrypted, i.e.

- in the Home Gateway,
- in the backup file that can be exported via the Web-UI, or rather
- in the backup file that can be exported via remote device management (i.e. via TR-069).

AES supports key lengths of 128, 192 and 256 bits. The preferred key-length is 256 bits. The AES key to encrypt the confidential data in the backup is called the “backup-key”.

Motivation: An attacker must not be able to export clear text credentials via the Web-UI backup function. And even if the attacker has access to the flash filesystem, he must not be able to easily compromise the credentials.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-64/3.5

Req 65	The backup-key must be derived at runtime from a key-specific set of certain attributes including hardware attributes as well as a random seed.

The backup-key must not be stored in the flash file system as a coherent binary data object. The key must be derived at runtime, i.e. during the system boot process. The key derivation algorithm must ensure that a random an per device unique key is generated. The attributes and the algorithm for the generation of the backup-key must be stored obfuscated in the flash memory.

Alternatively the backup-key could be derived from a specific password provided by the user. Such a feature would enable the exchange of backup files between different devices of the same type.

Motivation: A -- without the knowledge of the attributes and the key derivation function -- randomly looking AES backup-key mitigates brute force key guessing attacks.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-65/3.5

7.7. System Log

Req 66	The application must provide a system log that informs the user about security relevant events.

The following events are considered as security relevant and appropriate log messages must be defined:

- Successful and failed authentications at the:
    - Web-GUI
    - TR-064-Interface
    - FTP(S)-Service
    - NAS-Service
    - WLAN
- WPS/WSC Registration Protocol activation and exchange of WLAN password
- WPS/WSC subsystem enteres "locked down state"
- Detected & mitigated attacks by the firewall (according to the firewall security requirements)
- Successful and failed connections to the Auto Configuration Server (TR-069)

Multiple events in short time intervals can be summarized to one single log message.

Motivation: The user will be informed about the basic security status of his Home Gateway and he will be able to detect some attacks, e.g. if someone tries to get access to the web GUI by password guessing.

For this requirement the following threats are relevant:
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-66/3.5

8. Services

8.1. SIP User Agent

Req 67	The RTP protocol implementation must not disclose any confidential information about the source of the data stream.

RTP includes the control protocol RTCP, both protocols are defined in the RFC3550. The RTCP protocol data unit SDES (source description) features mandatory and optional items that could disclose sensitive information about the source of the RTP data stream. Neither the mandatory CNAME item nor any other optional item of the SDES data unit must disclose the WAN IP address / DNS name of the Home Gateway or the username of the VoIP account.

Motivation: This prevents an attacker from getting the WAN IP / Email address of the communication peer via a VoIP call.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-67/3.5

Req 68	The SIP user agent must only accept and process SIP requests from the call control it is registered to.

Motivation: If the SIP user agent accepts SIP requests from any communication peer, then it could be attacked easily. Limiting the connectivity to the registered call control protects the SIP user agent from being attacked.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.40-68/3.5

8.2. WAN Management Protocol

Req 69	The Broadband Forum TR-069 CPE WAN Management Protocol must be implemented for remote device management.

TR-069 is a well established remote device management protocol, that features the security building blocks in order to implement a secure remote device management. The remote device management must be activated by default. The device management must support the download and installation of firmware updates without any kind of user interaction.

Motivation: DT Group wants to rely on secure industry standards for the remote device management of Home Gateways.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-69/3.5

Req 70 The HTTP connection request URL must be unique for each device.

The connection request URL must not be identical for all devices. Since then an attacker could invoke connection requests on a large installation base of affected devices which would lead to a denial-of-service condition at the auto configuration server. A device specific connection request URL could be derived from a random number or rather from appropriate device-specific attributes.

Motivation: Otherwise an attacker could easily perform a DoS attack on the Auto Configuration Server.

Implementation example: Proper randomness of the backup-key can be archived by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described in RFC 4086.

For this requirement the following threats are relevant:
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.40-70/3.5

Req 71 The Home Gateway must validate the certificate path of the Auto Configuration Server's TLS sever certificate according to chapter 6 of RFC3280.

Motivation: Only if the server certificate of the ACS is valid the Home Gateway can trust the server authentication and thus guarantee that it communicates with the genuine Auto Configuration Server.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-71/3.5

Req 72 The TR-069 implementation must not enable the readout of passwords in plain text.

Neither via the TR-069 Method GetParameterValues, GetParameterAttributes nor via the Upload method (e.g. used for the export of the device configuration data) passwords that have to be protected must be disclosed as a plaintext value.

Motivation: The Auto Configuration Server's database must not contain any user's passwords. It is not a required use case of the remote device management to readout passwords in plain text. It may be necessary to readout encrypted passwords (e.g. as part of a device configuration file) to enable a backup and restore service.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-72/3.5

8.3. LAN Management Protocol

Req 73	The Broadband Forum TR-064 CPE LAN Management Protocol must be implemented for local device management.

This requirement is applicable if local device management is in scope for the Home Gateway development project. TR-064 is quite similar to the UPnP IGD profile (i.e. the Universal Plug and Play Internet Gateway Device profile), but the TR-064 protocol adds the required security functions like authentication and authorisation to the UPnP IGD profile standard. Therefore plain UPnP IGD must not be implemented for LAN-side device management.

Motivation: The device configuration via TR-064 must be secured similar to the Web GUI.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-73/3.5

Req 74	The TR-064 service including the corresponding UPnP SSDP service must only be accessible via LAN and private WLAN interfaces.

The TR-064 protocol features two services needed for operation: The SSDP (Simple Service Discovery Protol) and the TR-064 SOAP web services. Both services are designed for the usage within a protected network. Therefore these services must be bound solely to LAN interfaces.

Motivation: TR-064 is a LAN-side configuration service; it is not designed for WAN-side operation. Accessibility from the WAN interface would only increase the attack surface of the Home Gateway.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-74/3.5

Req 75	All TR-064 actions that are modifying the configuration of the Home Gateway and that are reading out confidential data (e.g. usernames, firewall configuration, etc.) must require a HTTP digest authentication by the device password.

The device password must be used as the state variable “ConfigPassword” defined in the TR-064 specification. Since the device password can be reset to the factory given state, the additional state variable “ResetPassword” also defined in TR-064 must not be implemented.
Deutsche Telekom Group provides a TR-064 functional specification that rates security relevant actions that require an authentication as “have to be secured”. These actions must require an authentication. The HTTP digest authentication has to be implemented according to RFC2617 using the option “cnonce”.

Motivation: Some of the TR-064 SOAP actions allow the change or readout of confidential or sensitive parameters.

These actions have to be protected by a HTTP digest authentication.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-75/3.5

Req 76	The TR-064 web service must enforce transport layer security (TLS 1.2) for all actions, which require an authentication and which transport confidentials data.

Secure ciphersuites have to be configured for TLS, i.e. cipher suites that contain server authentication, data encryption and support cryptographic key lengths of at least 128 bits.

Motivation: Even in the LAN confidential data transmitted in TR-064 SOAP requests and responses should be encrypted and the integrity of the communication should be guaranteed.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-76/3.5

Req 77	The TR-064 web-service implementation must validate each SOAP request so that malformed requests or requests that contain invalid parameters are rejected.

Motivation: It must not be possible to trigger buffer overflows e.g. by sending malformed requests or requests containing parameters which are too long.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability

For this requirement the following warranty objectives are relevant:

ID: 3.40-77/3.5

Req 78	The TR-064 actions “AddPortMapping” and “AddForwardingEntry” must only accept IP addresses within the subnet range of the trusted home network (i.e. any LAN and private WLAN interface) for internal clients. But these actions must not accept an IP-address of any LAN / WLAN interface of the Home Gateway itself.

The TR-064 implementation must restrict forwarding to clients of the home network, i.e. to any host within the local network but not to the Home Gateway itself. In addition the TR-064 implementation must not allow to forward traffic to external IP-addresses.

Motivation: It must be prevented that LAN-side services can be exposed to the internet, or that the Home Gateway can be turned into a proxy which can be abused by attackers.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-78/3.5

Req 79	The TR-064 implementation must not enable the readout of passwords in plain text.

Any state variable that represents a password with need of protection by the Home Gateway must not be recoveraby in plaintext once stored in the Home Gateway. This applies nearly to all passwords beside the WLAN password.

Motivation: Passwords are considered as confidential data and thus once stored in the Home Gateway they must not be recoverable in plain text via management interfaces. Exceptions from this requirement have to be choosen carefully according to the user's needs.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-79/3.5

8.4. Home Media Sharing

Req 80	The UPnP A/V server must only be accessible via the home network (i.e. via LAN and private WLAN interfaces).

The UPnP A/V (DLNA) Server is a service designed for local networks, since this service enables unauthenticated access to a media directory of the USB file system. Therefore all network services related to the UPnP A/V Server must be restricted to LAN and WLAN interfaces.

Motivation: Only members of the home network must be able to access the media files without any authentication.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-80/3.5

Req 81	The UPnP A/V server must limit the file system access to the file system of an attached USB storage.

The internal file system of the Home Gateway must not be accessible via the UPnP A/V (DLNA) service.

Motivation: The UPnP A/V server must prohibit the file system access to the internal flash files systems in order to protect the Home Gateways configuration and system files.

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized access or tapping of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-81/3.5

8.5. Network Attached Storage (SMB/CIFS)

Req 82	The NAS server must only be accessible via the home network (i.e. via LAN and private WLAN interfaces).

Motivation: The network attached storage is a service for the home network. Some users even may configure a network drive to be accessible without any authentication. The NAS server can be attacked if the service is bound to the Internet.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-82/3.5

Req 83	The NAS server must limit the file system access to the file system of an attached USB storage.

The internal file system of the Home Gateway must not be accessible via NAS service.

Motivation: The NAS server must prohibit the file system access to the internal flash files systems in order to protect the Home Gateways configuration and system files.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-83/3.5

Req 84	The NAS server must support users with different access rights to the file system of the attached storage.

It must be possible to set passwords for NAS users via the web GUI.

Motivation: Users and access rights help the customer to protect confidential information on the file system. It enables him to share access to files on a need-to-know basis. User authentication is mandatory if the customer wants to enforce the access rights.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-84/3.5

Req 85	If NAS user passwords are set the Home Gateway must enforce the following policy: • The password has a length of 8 - 32 characters. • The password can consist of the following classes of characters: numbers, lowercase/uppercase letters and special characters (e.g. “ !”§$%&/()=+*#:;., “). • The password must at least consist of two different character classes.

Motivation: Enforcing a minimum password length ensures a certain minimum strength of the protection provided by the password mechanism.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-85/3.5

8.6. File Transfer

Req 86	The FTPS protocol must be supported in order to enable a secure file transfer over the Internet.

FTPS relies on the security mechanisms of the TLS protocol in order to provide encryption and integrity protection of any transmitted data. The FTP protocol does not provide adequate security mechanisms if the protocol has to be used over insecure networks like the Internet: all transmitted data and even the authentication data (username/password) are transmitted in plain text and can easily be eavesdropped by an attacker.

Motivation: The authentication and the user's data must not transmitted in cleartext over the Internet, so that these information could b eavesdropped easily. Therefore it is mandatory to support a secure protocol for the file transfer over insecure networks.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-86/3.5

Req 87	The FTP(S) server must rely on the identity management of the NAS server.

The NAS server already implements an identity management, i.e. a management of users, passwords and permissions. Since file tranfser and NAS are similar service the user of the Home Gateway must not be confused by different identity management systems withing the Home Gateway.

Motivation: There is no need to define a separate user and rights management.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-87/3.5

Req 88	If WAN access is required for FTP(S) then the identity management must support to enable / disable FTP(S) WAN access for each NAS user individually.

By default, i.e. if a new user is generated, the rigth to access the FTP(S) service via WAN interface must be disabled. The Home Gateway administrator must be able to enable the FTP(S) WAN access on a per user basis.
If the identity management also supports to enable or disable the FTPS (TLS) support on WAN interface, then the Home Gateway administrator must be warned by the web GUI that it can not considered to be secure to use the FTP protocol on the Internet if he doesn't activate FTP over TLS.
Note that the FTP(S) service port(s) on the WAN interface must be closed if no user has the permission to access the FTP(S) service from the Internet.

Motivation: This helps the customer to enable the Internet access only for resources that need to be accessed over the Internet. And it enables to deactivate the Internet FTP(S) access at all.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-88/3.5

Req 89	The FTP(S) Server must limit the file system access to the file system of an attached USB storage

The internal file system of the Home Gateway must not be accessible via the FTP(S) service.

Motivation: The FTP(S) service must prohibit the file system access to the internal flash files systems in order to protect the Home Gateways configuration and system files.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-89/3.5

8.7. DNS Proxy

Req 90	The DNS proxy implementation must be compliant to chapter 3 “Transparency Principle” and chapter 4 “Protocol Conformance” of RFC 5625.

The DNS proxy of the Home Gateway must support the security extensions of the DNS protocol i.e. the “Secret Key Transaction Authentication for DNS” (TSIG) defined by RFC 2854 and the DNS Security Extensions (DNSSEC) defined by RFC 4033, RFC 4034, RFC 4035, and beyond.
RFC 5625 defines guidelines for the implementation of DNS proxies. Especially chapter 3 “Transparency Principle” and chapter 4 “Protocol Conformance” of RFC 5625 define mandatory requirements for the support of TSIG and DNSSEC.

Motivation: The Home Gateway must support DNS protocol extensions for security by design.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-90/3.5

Req 91	The DNS proxy must apply the query matching rules defined in section 9.1 “Query Matching Rules” of RFC 5452.

Section 9.1 of RFC 5452 defines a set of matching rules that a resolver implementation has to apply in order to detect forged answers to DNS queries. If a mismatch of any rule occurs then the response must be considered as invalid by the DNS proxy. If a DNS proxy detects forged answers the implementation should abandon the UDP query and re-issue it over TCP according to section 9.3 of RFC 5452.

Motivation: The detection of forged answers to DNS queries mitigates DNS cache poisoning attacks.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-91/3.5

Req 92	The DNS proxy must uimplement an unpredictable query ID for outgoing queries, utilizing the full range available (0-65535).

The Query-ID must be generated by a high quality (pseudo-) random generator that generates uniformly distributed random numbers.

Motivation: Using unpredictable query IDs makes it harder for an attacker to forge the answer to a DNS query. This mitigates DNS cache poisoning attacks.

Implementation example: Adequate generators are described in RFC 4086, e.g. in section 7.1.2 the /dev/random device on a Linux/Unix system1 is regarded as an adequate implementation.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-92/3.5

Req 93	The DNS proxy must extend the query ID space by using unpredictable source ports.

This extension of the ID space must be compliant to the query ID related requirements of section 9.2 “Extending the Q-ID Space by Using Ports and Addresses” of RFC 5452. Especially the proxy implementation must use an unpredictable source port for outgoing queries from a range of available ports that is as large as possible and must use multiple different source ports simultaneously in case of multiple outstanding queries.

Motivation: The extension of the query ID space by using unpredictable source ports makes it harder for an attacker to forge the answer to a DNS query. This mitigates DNS cache poisoning attacks.

Implementation example: Proper unpredictability can be archived by employing a high quality (pseudo-) random generator that generates uniformly distributed random numbers. Such generators are described in RFC 4086, e.g. in section 7.1.2 the /dev/random device on a Linux/Unix system1 is regarded as an adequate implementation. 1 On embedded Linux systems the random number generators provided by the kernel via the two devices /dev/random and /dev/urandom are considered as “cryptographic strong random number” generators, if the implementation takes care that the initialization of the Linux RNG (the seeding) at system start up provides enough entropy. It is e.g. not recommended that the Linux RNG is seeded by the same constant value at every device start up.

For this requirement the following threats are relevant:
- Unauthorized modification of data

For this requirement the following warranty objectives are relevant:

ID: 3.40-93/3.5

Req 94	The DNS proxy must not support DNS queries on any WAN interface.

Note that section 6.2 “Interface Binding” of RFC 5625 also addresses the accessibility of the DNS proxy but RFC 5625 contains a more relaxed requirement that is not considered as adequate.

Motivation: Open resolvers enable DNS reflector attacks as described in RFC5358. These kind of attacks must be mitigated by the DNS proxy implementation.

For this requirement the following threats are relevant:
- Disruption of availability
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-94/3.5

Req 95	The DNS Proxy must mitigate DNS rebinding attacks.

The goal of a DNS rebinding attack is to overcome restrictions which are enforced by the Same-Origin-Policy of a Web-Brower. This attack is mainly used to get unauthorized access to local resources within a private home network in order to conduct further attacks. DNS rebinding does work, if an external DNS server responds to a query with IP-addresses that belong to the private home network. Therefore the DNS-Proxy must delete such entries in the responses of an external DNS server.

Motivation: Mitigating the unauthorized access to local ressources in the home network from a web-application.

Implementation example: The DNS proxy must delete any A/AAAA records in responses to DNS queries that contain private or rather link local IP addresses. I.e. the following address ranges must be filtered:

- 192.168.0.0/16 as defined in RFC1918
- 172.16.0.0/12 as defined in RFC1918
- 10.0.0.0/8 as defined in RFC1918
- 169.254.0.0/16 as defined in RFC5735
- fe80::/10 IPv6 link local addresses
- fd::/10 IPv6 Unique Local Addresses as defined in RFC4139

The filtered resonse will be sent back to the client in order to avoid timeouts. Furthermore the DNS Proxy implements a user configurable whitelist of FQDNs that are not affected by this filtering.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-95/3.5

8.8. WiFi Simple Configuration / WiFi Protected Setup

Req 96	The Wi-Fi Simple Configuration protocol version 2.0.2 or above must be implemented.

The technical specification version 2.0.2 was released at January 30th, 2012, and it obsoletes the WSC 2.0 specification. WSC 2.0.2 contains a mandatory mitigation mechanism to brute force attacks on the Access Point's (the Home Gateway's) device PIN using an external registrar: the Access Point must enter a "locked down state" after at most 10 failed, consecutive PIN verification attempts are detected, with no time limitation, and from any number of external registrars. In the locked down state the Access Point must refuse to run the registration protocol with any external registrars. An user interaction is mandatory to cancel the locked down state, i.e. to re-enable the WSC registration protocol for external registrars. In addition to the WSC 2.0.2 specification the Access Point must implement the "locked down state", even if it provides a dynamically generated random device PIN.

Motivation: The latest protocol specification contains important security requirements that fix a protocol flaw in the WSC 2.0 specification. Implementing the latest WSC standard closes a commonly known vulnerability.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.40-96/3.5

Req 97	The user must be able to permanently deactivate the WSC (WPS) protocol.

If the WSC protocol is deactivated by configuration the Access Point must not include any WSC Information Elements in the beacon or management frames. I.e. no WSC protocol frames have to be exchanged.

Motivation: WSC allows the easy integration of new clients in wireless networks. Therefore WSC may lead to the loss of the confidentiality of the WLAN password, if the functionality can be abused by an unauthorized entity. An experienced user may want to configure his Home Gateway as secure as possible, i.e. he may want to deactivate WSC. By deactivating WSC the user can protect his wireless network even in the case if a critical vulnerability in the particular Home Gateway's WSC implementation is detected.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-97/3.5

Req 98	The activation of the WSC registration protocol must require an user interaction at the Home Gateway.

This requirement must be fulfilled for any implemented WSC method. The Push Button Configuration (PBC) method requires the user to trigger a hardware or software push button, the PIN method using an internal registrar requires the entry of the client's device PIN into a form field of the Home Gateway's protected Web-GUI. Both methods fulfil the requirement by design.
The PIN method using an external registrar could be implemented without any user interaction at the Home Gateway, which is prohibited by this requirement. The external registrar PIN method must also require an explicit activation via

Web-GUI interaction, e.g. by pressing a push button on a protected WSC configuration page.

Motivation: WSC methods that require an user interaction can't be abused easily by an attacker from remote (i.e. within the range of the wireless network), since the user interaction requires a physical access to the Home Gateway or an access to the protected Web-GUI application.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-98/3.5

Req 99	The WLAN access point of the home gateway must limit the activation time of the registration protocol.

This requirement must be fulfilled for any WSC method. In accordance with the specification a limited life-time of 120 seconds is mandatory for the PBC method.
For any PIN-based (i.e. password-based) WSC method the maximum activation time must be limited as well, it must not exceed 600 seconds.

Motivation: The WSC registration protocol handles the exchange of the WLAN password and therefore this functionality is the target of any attack, if an unauthorized entity tries to compromise the WLAN password via WSC. Terminating the registration protocol after a limited life-time re-enters a secure state.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

For this requirement the following warranty objectives are relevant:

ID: 3.40-99/3.5

Req 100	The WLAN access point must always generate a fresh, random device PIN each time before the WSC registration protocol with the external registrar PIN method is activated.

Specifically this requirement means, that the access point must not feature static WPS PINs.

Motivation: A dynamic, random Access Point's device PIN mitigates PIN guessing attacks.

For this requirement the following threats are relevant:
- Unauthorized use of services or resources

For this requirement the following warranty objectives are relevant:

ID: 3.40-100/3.5