Security requirement

COTS Residental Gateways

Deutsche Telekom Group

Version	1.0
Date	Dec 1, 2020
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
	3.71	Security requirement

Version	State	Status
1.0	Dec 1, 2020	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Dec 1, 2020 - Nov 30, 2025	Stefan Pütz, Leiter SEC-NIS

Summary

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.

These are the security requirements for Customer of the Shelf residential gateways that are valid for National Companies.

2. General System Hardening

Req 1	Firmware distributed on customer devices 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 operating system and it applies to any: • Network interface • On-board console interface • WebGUI interface.

Motivation: Having shell access enabled extends attacks surface (It exposes the device to more attacks).

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

ID: 3.71-1/1.0

Req 2	After resetting the Home Gateway to the initial state, optional network services must be disabled. These optional network services require explicit user activation and have to be listed in WebGUI as disabled (with respective network ports closed). Set of default services (required for basic operation) might depend on country / telco provider.

Motivation: Every enabled network service broadens the attack surface of the Home Gateway. The device must be configured securely by default and optional services must be disabled.

Implementation example:
- Optional network services: DLNA/UPnP A/V media sharing, File Transfer (FTP), NAS;
- Required network service: Remote Device Management (TR-069) providing automatic firmware updates for the Home Gateway.

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

ID: 3.71-2/1.0

Req 3	The TLS implementation of the embedded operating system must support TLS v1.2 or newer. TLS protocol versions older than TLS 1.2 are considered as deprecated since they contain security vulnerabilities. The cryptographic parameters for a TLS v1.2 implementation have to be implemented according the Technical Report TR-02102-2 "Cryptographic Mechanisms: Recommendations and Key Lengths" of the German Federal Office for Information Security (BSI).

Compliant configuration and settings:
- TLS 1.2
- Cipher suites
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

        - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
        - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
        - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
        - TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
        - TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
        - TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
        - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
        - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
        - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_DHE_RSA_WITH_AES_128_CCM
        - TLS_DHE_RSA_WITH_AES_256_CCM

    - Minimal key lengths

Algorithm	Minimal Key Length [bit]	Time period
ECDSA	224	up to 2015
ECDSA	250	2016 - 2026
DSS	2000	up to 2022
DSS	3000	2023 - 2026
RSA	2000	up to 2023
RSA	3000	2024-2026
ECDH	224	up to 2015
ECDH	250	2016 - 2026
DH	2000	up to 2022
DH	3000	2023-2026

    - Elliptic curves
        - brainpoolP256r1
        - brainpoolP384r1
        - brainpoolP512r1
        - secp256r1
        - secp384r1
    - No TLS compression
    - No client-side renegotiation

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

ID: 3.71-3/1.0

Req 4	The device is delivered with a pre-configured password which must satisfy at least these requirements: • A length of 10 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 Home Gateway could lead to attacks on devices when the user doesn't change the default password. These attacks are mitigated by individual device passwords.

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

ID: 3.71-4/1.0

Req 5	The device must not contain any accounts with predefined well known credentials (e.g. admin:admin, user:user, root:root, huawei:huawei).

Motivation: An identical standard password for every Home Gateway could lead to attacks on devices when the user doesn't change the default password. These attacks are mitigated by individual device passwords.

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

ID: 3.71-5/1.0

Req 6	Any passwords set by user must meet the following requirements: • The length of the password must be within the range of 8 - 32 characters; • The password must contain characters from two at least different classes; • Valid classes of characters for the password are uppercase letters, 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

ID: 3.71-6/1.0

Req 7	Password guessing attacks on any application or service on the Home Gateway must be mitigated by attempt rate limiting. After each failed authentication a delay mechanism has to block the authentication process from the same source (IP) 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 can 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 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);
- When there are 10 failed authentication attempts from a certain IP in last 1 hour, deny any further authentication attempts within 15 seconds from the last one.

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

ID: 3.71-7/1.0

Req 8	The application must feature a system log that informs the user about security relevant events. The following events are considered as security relevant and appropriate messages must be logged: • Successful and failed authentications at the: Web-GUI, TR 64 Interface, FTP(S) Service, NAS Service, and 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

ID: 3.71-8/1.0

Req 9	Log messages must not disclose any cryptographic keys, passwords, session keys or confidential data stored in the file system of the Home Gateway. This requirement is related to the logging of the operating system as well as to the logging of any application components.

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

ID: 3.71-9/1.0

Req 10	Check against known vulnerability database must be perform to ensure that any vulnerable hardware or software component is neither installed nor used. Exception from this rule are components

for which the vendor has already provided a measure to remedy the vulnerability (e.g. a patch, update or workaround) and this measure has been properly implemented.

Motivation: Publication of vulnerabilities increases the risk of successful exploitation by an attacker. The likelihood raises because of publication of detailed information and tools that help to exploit the vulnerability.

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

ID: 3.71-10/1.0

3. Networking, Interfaces, and Services

Req 11	If a network service or port forwarding is disabled by the Home Gateway's configuration, all related TCP / UDP network ports on all network interfaces must be closed. Closed means that the access is prohibited on Layer 4 (Transmission). There must not listen any service (in default configuration / displaying sorry page...).

Motivation: The network connectivity to a disabled service 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

ID: 3.71-11/1.0

Req 12	A user of the Home Gateway must not be able to disable 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 to the system
- Unauthorized use of services or resources
- Unnoticeable feasible attacks

ID: 3.71-12/1.0

Req 13	Port Restricted Cone NAT (as defined in RFC 3489 on IPv4 networks) is one where all requests from the same internal IP address and port are mapped to the same external IP address and port on Home Gateway's WAN interface. An external host can send a packet to the internal host only if the internal host had previously sent a packet to that external host's IP address and port (restriction includes both IP address and port of the external host). That means that Home Gateway allows through NAT only traffic that is coming in response to traffic originated in the internal network. Incoming packets with source IP address and port that do not match with destination in prior request (or requests) must be treated as unsolicited.

Motivation: Port-restricted cone NAT guarantees that any incoming datagram is related to a outbound connection (destination IP address and source port). Thus port-restricted cone NAT provides an adequate protection of the home network.

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

ID: 3.71-13/1.0

Req 14	The following requirements describe a blueprint for an IPv6 network security model: • Any incoming connections to IPv6 hosts in the LAN/WLAN must be denied. Exceptions have to be configured per host by the user. But it must not be possible to configure an ex-

	ception for an IP address of the LAN/WLAN interface of the Home Gateway itself; • Any incoming connection to any port at the WAN interface of the Home Gateway must be denied unless the connectivity is not explicitly needed by a particular service. 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

ID: 3.71-14/1.0

Req 15	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. Device in the initial state is expected to expose only minimal set of default services such as TR-069.

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

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

ID: 3.71-15/1.0

Req 16	Forwarding rules to any IP address of the home network (LAN / WLAN) interface on the Home Gateway must not be accepted by any device configuration option accessible to the user.

Motivation: The user must not be able to publish an internal Home Gateway's service (e.g., Web-GUI) to public network (WAN).

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

ID: 3.71-16/1.0

Req 17	The SIP user agent must only accept and process SIP requests from legitimate SIP proxy (server) 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

ID: 3.71-17/1.0

Req 18	The Query ID & Source Port values for outgoing DNS queries must be unpredictable (based on high quality pseudo random numbers).

Motivation: Using unpredictable Query IDs & Source Ports values make spoofing of DNS responses harder. This mitigates DNS cache poisoning attacks.

Implementation example: Using recent & mature implementation of DNS proxy (such as dnsmasq) and Linux kernel is often enough to satisfy this requirement.

For this requirement the following threats are relevant:

- Unauthorized modification of data

ID: 3.71-18/1.0

4. Wireless LAN

Req 19	The pre-configured WLAN password length must be at least 20 characters. The password may contain numbers 0-9 only but it is recommended to use wider character space, e.g. numbers 0 - 9 and uppercase characters (A-Z).

Motivation: Pre-configured WLAN password must provide enough entropy to mitigate common brute force attacks. It's usually printed on a device label.

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

ID: 3.71-19/1.0

Req 20	The private wireless LAN implements WPA2 standard and/or stronger. The default WLAN encryption must be WPA2/CCMP or better.

Motivation: WPA2/CCMP is the minimal acceptable method for wireless networks.

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

ID: 3.71-20/1.0

Req 21	The minimum WLAN password length must be 8 characters. It must not be possible to set a shorter value.

Motivation: This requirement define minimal acceptable length due to usability reasons.

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

ID: 3.71-21/1.0

Req 22	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 access or tapping of data
- Unauthorized use of services or resources

ID: 3.71-22/1.0

Req 23	When the WSC protocol is disabled by configuration the Home Gateway must not include any WSC Information Elements in the beacon or management frames. I.e. no WSC protocol frames have to be exchanged. WSC scanning tools like Wash must not show the Home Gateway in results.

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

ID: 3.71-23/1.0

Req 24	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

ID: 3.71-24/1.0

Req 25	This requirement applies to 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

ID: 3.71-25/1.0

Req 26	When using external registrar PIN method, the WLAN access point must generate new random device PIN each time before WSC registration. 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

ID: 3.71-26/1.0

5. WebGUI, Authentication, and Session Management

Req 27	Functionality of the HTTP server that is not needed for the Home Gateway operation must be deactivated. This includes especially the following requirements: • Directory listing must be disabled (The web server is not configured to display the list of files contained in this directory); • Only needed HTTP methods must be implemented, typically only HTTP GET and POST. The others (e.g. PUT, HEAD, DELETE, PATCH, OPTIONS, TRACE) must be disabled; • The HTTP server must NOT support Server Side Includes (SSI); • Web server responses should not contain any information on web server type and version (e.g. HTTP headers).

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

ID: 3.71-27/1.0

Req 28	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

ID: 3.71-28/1.0

Req 29	The response from GUI web server must not contain any unnecessary confidential data that are especially user and Wi-Fi passwords, encryption keys, etc. It must not be possible to display passwords in clear-text form, e.g. for internet access or users. The web GUI must not implement any method that enables to readout of passwords.

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

ID: 3.71-29/1.0

Req 30	Any client data must be validated at server side by the web GUI application. Minimal criteria are length and character space for each parameter. Invalid request must result in session termination.

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

Implementation example: Example of client data: URL, GET / POST parameters, headers and cookies.

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

ID: 3.71-30/1.0

Req 31	There must be only one user account on the device by default. Authentication is mandatory to access any web GUI application components – except the login page itself and a status page that only contains only non-confidential data. Unauthenticated user should be redirected to the login page and no further execution of any script must be performed.

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

ID: 3.71-31/1.0

Req 32	A session identifier (session cookie) must be not guessable, that means: • 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 (to prevent session fixation attack).

Motivation: 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

ID: 3.71-32/1.0

Req 33	The Home Gateway web GUI application must invalidate the authenticated session after at most 20 minutes of inactivity.

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

ID: 3.71-33/1.0

Req 34	The Home Gateway web GUI application must provide a logout functionality that enables the user to terminate the current web GUI session invalidating the 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

ID: 3.71-34/1.0

Req 35	The anti-CSFR token must be present in every state changing request sent from the client back to the web server. The anti-CSRF token is a random unpredictable string generated on server side included in the response to the client. The server must then validate the anti-CSRF token in following request and the requests with no or invalid token must be rejected and the session immediately terminated. The token is usually transmitted in a form of a hidden field in html form, however custom HTTP header (e. g. “X-anti-CSRF-Token”) can also be used. Request is considered state changing when it affects stored configuration (password change, running services...).Note: It is also best practice the state changing requests to be POST requests.

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.

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
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

ID: 3.71-35/1.0