Notice

This CableLabs security guideline document is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by CableLabs® in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open-source licenses, if any.

© Cable Television Laboratories, Inc. 2021
DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, infringement, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.
Document Status Sheet

<table>
<thead>
<tr>
<th>Document Control Number:</th>
<th>CL-GL-GDS-BCP-V01-211007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title:</td>
<td>Gateway Device Security Best Common Practices</td>
</tr>
<tr>
<td>Revision History:</td>
<td>D01 – Released 11/20/20</td>
</tr>
<tr>
<td></td>
<td>V01 – Released 10/07/21</td>
</tr>
<tr>
<td>Date:</td>
<td>October 7, 2021</td>
</tr>
<tr>
<td>Status:</td>
<td>Work in Progress</td>
</tr>
<tr>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td></td>
<td>Issued</td>
</tr>
<tr>
<td></td>
<td>Closed</td>
</tr>
<tr>
<td>Distribution Restrictions:</td>
<td>Author Only</td>
</tr>
<tr>
<td></td>
<td>CL/Member</td>
</tr>
<tr>
<td></td>
<td>CL/Member/</td>
</tr>
<tr>
<td></td>
<td>NDA-Vendor</td>
</tr>
<tr>
<td></td>
<td>Public</td>
</tr>
</tbody>
</table>

Key to Document Status Codes

Work in Progress  An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.

Draft  A document that is considered largely complete, but lacking review by members and vendors. Drafts are susceptible to substantial change during the review process.

Released  A generally public document that has undergone rigorous member and technology supplier review, cross-vendor interoperability, and is suitable for certification/qualification testing if applicable.

Closed  A static document, reviewed, tested, validated, and closed to further changes.

Trademarks

CableLabs® is a registered trademark of Cable Television Laboratories, Inc. Other CableLabs marks are listed at http://www.cablelabs.com/specs/certification/trademarks. All other marks are the property of their respective owners.
Contents

1 SCOPE .......................................................................................................................... 6
  1.1 Introduction and Overview.......................................................................................... 6
  1.2 Purpose of Document............................................................................................... 6
  1.3 Use of the Document.............................................................................................. 6

2 REFERENCES .................................................................................................................. 7
  2.1 Informative References............................................................................................ 7

3 TERMS AND DEFINITIONS ......................................................................................... 9

4 ABBREVIATIONS AND ACRONYMS ...................................................................... 10

5 REQUIREMENTS COMPLIANCE .............................................................................. 11
  5.1 Compliance Classification....................................................................................... 11

6 TECHNICAL REQUIREMENTS ................................................................................. 12
  6.1 General Hardware Requirements ........................................................................... 12
  6.2 Secure Boot Requirements .................................................................................... 13
  6.3 Secure Upgrade Requirements ............................................................................... 13
  6.4 Initial/Out-of-Box Configuration Requirements .................................................... 14
  6.5 Data-at-Rest Protection Requirements .................................................................. 15
  6.6 Data Exchange Encryption/Integrity Requirements ................................................. 16
  6.7 Securing Cryptographic Material Requirements ................................................... 17
  6.8 Physical and Remote Management Interfaces Requirements ................................ 18
  6.9 Diagnostic, Debug, and Development Access Requirements .............................. 19
  6.10 Logging Requirements ........................................................................................ 20
  6.11 Time Synchronization Requirements ..................................................................... 20
  6.12 Software BOM and Software Updates Requirements ............................................ 21
  6.13 Network Services and Listening Processes Requirements .................................... 22
  6.14 Network Access Mechanisms Requirements ........................................................ 23
  6.15 Additional Requirements ..................................................................................... 23

7 ADVERSARIAL ENGINEERING .................................................................................. 24

APPENDIX I ACKNOWLEDGEMENTS ........................................................................ 25

Tables

Table 1 - General Hardware Requirements (HR).......................................................... 12
Table 2 - Secure Boot Requirements (SB)..................................................................... 13
Table 3 - Secure Upgrade Requirements (SU)............................................................. 13
Table 4 - Initial/Out-of-Box Configuration Requirements (OOB)................................. 14
Table 5 - Data-at-Rest Protection Requirements (DRP)............................................... 15
Table 6 - Data Exchange Encryption/Integrity Requirements (DE).............................. 16
Table 7 - Securing Cryptographic Material Requirements (KEY).............................. 17
Table 8 - Physical and Remote Management Interfaces Requirements (MI)............... 18
Table 9 - Diagnostic, Debug, and Development Access Requirements (DIAG)........... 19
Table 10 - Logging Requirements (LOG)..................................................................... 20
Table 11 - Time Synchronization Requirements (TS).................................................. 20
Table 12 - Software BOM and Software Updates Requirements (SBOM)................... 21
Table 13 - Network Services and Listening Processes Requirements (NETS) ................................................................. 22
Table 14 - Network Access Mechanisms (Wi-Fi/Ethernet) Requirements (NETA) ........................................................... 23
Table 15 - Additional Requirements (AR) ..................................................................................................................... 23
1 SCOPe

1.1 Introduction and Overview

This Gateway Device Security document specifies best common practices to serve as an industry metric for retail and leased devices (both gateways and cable modems) for security—this includes manufacturing process, supply chain, hardware and firmware configuration procedures, software, and management protocols.

1.2 Purpose of Document

The purpose of this document is to provide a common set of requirements and best practices for vendors of gateway devices (routers, access points) and cable modems that are agreed upon by the operators and manufacturers. Note that each operator may have additional or different requirements from those specified in this document.

The requirements and best practices cover the following areas.

1. hardware/manufacturing considerations
2. “default” security (out of box)
3. secure boot and root of trust
4. software/firmware verification
5. encryption requirements (data in transit and at rest)
6. physical security
7. privacy

The requirements and best practices elicited in this document are expected to be applied to “production” devices, i.e., devices that are to be deployed in an operational network. Devices that are meant for demonstrations and/or compliance testing, certification, or lab trials may not necessarily incorporate these requirements and best practices unless the device is explicitly being tested/validated for conformance to this document.

1.3 Use of the Document

These security best common practices are guidelines and not a CableLabs security specification. Therefore, the security practices are not prescriptive. Because security needs change over time and different networks may be architected and configured differently, cable operators and manufacturers may deviate from these security best practices. The guidelines in this document are focused on operational security based on existing industry practices. These security guidelines do not expressly cover protocol interoperability or implementation.

These security best common practices may be updated as needed. CableLabs’ Gateway Device Security Working Group will continue to work with cable Internet providers and cable gateway device manufacturers to update these guidelines to be in accordance with industry best practices.
2 REFERENCES

2.1 Informative References

The following references include documents/links to standards in different regions, including the European Union and North America, in order to align requirements within this document with these references.


[NIST 800-88r1] NIST Special Publication 800-88r1, Guidelines for Media Sanitization, http://dx.doi.org/10.6028/NIST.SP.800-88r1


[NIST 8259A] NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, https://doi.org/10.6028/NIST.IR.8259A

3 TERMS AND DEFINITIONS

This document uses the following terms.

**cryptographic material** Any material/data that is essential for encryption, decryption, verification, and/or authentication operations, including but not limited to asymmetric keys, symmetric keys, nonces, seeds for random functions, and parameters used for cryptographic functions.

**interface** Any physical, logical, network, or virtual communication port that is implemented on the device, including but not limited to the following:
- local communications ports (serial, USB),
- network interfaces (Ethernet, Wi-Fi, BT, etc.),
- IP listen ports/sockets,
- virtualized interfaces, and
- interfaces meant for operator management of device.

**operator interface** An interface meant for the network operator to access the device (either locally or over the network) primarily for management and configuration of the device.

**end-user interface** An end-user (non-management) interface primarily meant for regular operations and data exchange.

**persistent keys** Keys used in symmetric or asymmetric cryptographic operations that usually persist through device reboots and are used multiple times across different cryptographic sessions.

**secure channel** Any data exchange channel that provides confidentiality (through encryption) and integrity protection. The establishment of the secure channel includes authentication of one or both endpoints.

**tamper-evident** Pertains to mechanisms (mechanical or electronic) applied to reveal any unauthorized access to a device or its components. Examples of tamper-evident mechanisms can include but are not limited to security tape or seal that gets damaged or destroyed in the process of unauthorized access, pressure pads, infrared/light sensors, and trigger switches.

**tamper-resistant** Pertains to mechanisms (mechanical or electronic) applied to hinder and/or deter unauthorized access to a device or its components. Examples of tamper-resistant mechanisms can include but are not limited to one-way screws or bolts and secure cryptoprocessors.

**trust anchors** Public keys, certificates for which trust is assumed and not derived, which are used to verify digital signatures and validate certificate chains.
4 ABBREVIATIONS AND ACRONYMS

This document uses the following abbreviations.

- **AEAD**: authenticated encryption with additional data
- **BCP**: best common practices
- **BOM**: bill of materials
- **BPI+**: baseline private interface plus
- **BT**: Bluetooth
- **CVSS**: common vulnerability scoring system
- **CSRF**: cross-site request forgery
- **DE**: data encryption
- **EAE**: early authentication and encryption
- **FIPS**: federal information processing standards
- **FSBL**: first stage boot loader
- **GDS**: gateway device security
- **HR**: general hardware requirements
- **IoT**: Internet of Things
- **IP**: Internet protocol
- **JTAG**: joint test action group
- **MAC**: media access control
- **mDNS**: multicast domain name system
- **MI**: management interface
- **MoCA**: Multimedia over Coax Alliance
- **MSO**: multiple system operator
- **OEM**: original equipment manufacturer
- **OOB**: initial/out of box
- **OTP**: one-time password
- **OS**: operating system
- **PFS**: perfect forward secrecy
- **PKI**: public key infrastructure
- **ROM**: read-only memory
- **SB**: secure boot
- **SBOM**: software bill of materials
- **SNMP**: simple network management protocol
- **SSDP**: simple service discovery protocol
- **SSH**: secure shell
- **SWD**: serial wire debug
- **TLS**: transport layer security
- **TS**: time synchronization
- **UI**: user interface
- **UPnP**: universal plug and play
- **USB**: universal serial bus
- **WAN**: wide area network
- **WPA**: Wi-Fi protected access
5 REQUIREMENTS COMPLIANCE

The following requirement key words are used within this document:

- **SHALL** - This word means that the definition is as an absolute requirement of this document.
- **SHALL NOT** - This phrase means that the definition is an absolute prohibition of this document.
- **SHOULD** - This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

5.1 Compliance Classification

The requirements outlined in this document cover a wide range of criteria, and it is important that there be a mechanism by which a manufacturer can prove/demonstrate that its product complies with the requirements. Depending on the requirement, compliance checks are done by one of the following verification steps.

5.1.1 Compliance through Disclosure and Documentation

Certain requirements, such as disclosing all open source components used and their versions, are met in the form of relevant documents and links to information about how the manufacturer incorporated a specific feature in its product.

5.1.2 Compliance through Attestation by Manufacturer

Requirements that are not easily testable (either manually or using tools) need to be attested by the manufacturer, and compliance is confirmed through a legal agreement or disclosure. The customer/client also has the right to test/assess for compliance and not require explicit permissions for it (e.g., pen testing, destructive testing).

5.1.3 Compliance through Automated Testing/Tools

Requirements that can be validated by use of automated tooling will be tested by providing artifacts (e.g., binary firmware images, flash dumps, source code, or similar) into a tool for analysis. This is done by the customer/client or their authorized consultants/vendor. Results will be analyzed to ensure accuracy.

5.1.4 Compliance through Manual Verification

Requirements that can be validated by manual analysis are to be tested by basic dynamic testing (e.g., network scans) or by an in-depth hardware or firmware penetration test (as needed). This is done by the customer/client or their authorized consultants/vendor.
6 TECHNICAL REQUIREMENTS

The requirements are categorized in the following functional areas.

1. General hardware requirements (HR)
2. Secure boot (SB)
3. Secure upgrade (SU)
4. Initial/out-of-box configuration (OOB)
5. Data-at-rest protection (DRP)
6. Data exchange encryption/integrity (DE)
7. Securing cryptographic material (KEY)
8. Physical and remote management interfaces (MI)
9. Diagnostic, debug, and development access (DIAG)
10. Logging (LOG)
11. Time synchronization (TS)
12. Software BOM and software updates (SBOM)
13. Network services and listening processes (including APIs) (NETS)
14. Network access mechanisms (Wi-Fi/Ethernet) (NETA)
15. Additional requirements (AR)

6.1 General Hardware Requirements

Table 1 - General Hardware Requirements (HR)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR-001</td>
<td>No hardware-based serial consoles SHALL be left open or active in production devices.</td>
<td></td>
</tr>
<tr>
<td>HR-002</td>
<td>Any hardware-based connectors or ports used for debugging, testing and/or provisioning (e.g., JTAG/SWD) SHALL be disabled in production devices.</td>
<td></td>
</tr>
<tr>
<td>HR-003</td>
<td>A device that is expected to be deployed in a location outside an operator’s secure facility SHALL include tamper-evident capabilities.</td>
<td></td>
</tr>
<tr>
<td>HR-004</td>
<td>A device that is expected to be deployed in a location outside an operator’s secure facility SHOULD include tamper-resistant capabilities.</td>
<td></td>
</tr>
<tr>
<td>HR-005</td>
<td>A manufacturer SHALL provide a detailed component list of hardware for a device.</td>
<td></td>
</tr>
</tbody>
</table>

6.1.1 HR Requirements Clarifications

HR-001

The hardware console needs to be both electronically and physically disabled so that both the ability to manipulate the device and the ability to read the information from the device is prevented in production scenarios. This is intended to ensure that applicable hardware interfaces on the devices are secured.

HR-002

Connecting to these ports should not result in any information being available.

HR-003

The expectation is that the device is deployed outside the operator’s facility (e.g., subscriber’s premise).

HR-004

HR-003 is applicable for deployments where a device is in a facility or location where it is not easily accessible, whereas HR-004 is applicable for situations where the device may be openly accessible.
HR-005
The expectation is to provide a list of components (chipset, GPU/CPU, flash/memory, network adapter, etc.) that have processing capability and are applicable to security and/or can be used to access the device (through physical access or network access). The list includes the physical ports (USB, ethernet, serial, etc.). The list is to be provided to the operator and any test lab that is working on behalf of the operator.

6.2 Secure Boot Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB-001</td>
<td>A device SHALL verify the integrity of the firmware prior to transferring execution to it.</td>
<td></td>
</tr>
<tr>
<td>SB-002</td>
<td>A device SHALL have a hardware root of trust that is used to validate the integrity and authenticity of the bootloader and firmware.</td>
<td></td>
</tr>
<tr>
<td>SB-003</td>
<td>A device SHOULD have an anti-rollback mechanism to prevent any downgrade of the firmware during the boot process.</td>
<td></td>
</tr>
<tr>
<td>SB-004</td>
<td>A device SHALL validate the integrity and authenticity of each software component(s) prior to execution.</td>
<td></td>
</tr>
<tr>
<td>SB-005</td>
<td>Device firmware SHOULD be stored in encrypted form on the device.</td>
<td></td>
</tr>
</tbody>
</table>

6.2.1 SB Requirements Clarifications

SB-001
The intent is that every stage of the boot process be verified. The mechanism of integrity verification is expected to be implementation dependent.

SB-003
The specific mechanism to prevent downgrade is implementation dependent. This requirement needs to be balanced with SU-002 to ensure that the recovery mechanism is not abused to perform a downgrade attack.

SB-004
SB-001 ensures that the device starts in a trusted operational environment, and SB-004 ensures that only trusted software components are executed in the operational environment.

SB-005
Refer to Sections 6.5 and 6.6 for requirements related to encryption.

6.3 Secure Upgrade Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU-001</td>
<td>A device SHALL verify the integrity and authenticity of any new firmware that it downloads.</td>
<td></td>
</tr>
<tr>
<td>SU-002</td>
<td>A device SHALL gracefully recover to a working state using the last known good image in the event a software upgrade fails without enabling image downgrade attacks.</td>
<td></td>
</tr>
<tr>
<td>SU-003</td>
<td>All firmware updates SHALL be digitally signed by the manufacturer and the signature be verifiable to a trusted source.</td>
<td></td>
</tr>
<tr>
<td>SU-004</td>
<td>Any firmware updates SHALL be delivered to the device with integrity protection.</td>
<td></td>
</tr>
<tr>
<td>SU-005</td>
<td>A device SHOULD accept firmware updates in encrypted format.</td>
<td></td>
</tr>
<tr>
<td>SU-006</td>
<td>A device SHALL have a mechanism to prevent accepting an obsolete or revoked version of firmware.</td>
<td></td>
</tr>
</tbody>
</table>
6.3.1 SU Requirements Clarifications

SU-001
The integrity and authenticity can typically be verified by checking that the firmware is signed and the signature is valid. Other equivalent mechanisms based on cryptography recommendations in this document may be utilized (e.g., HMAC-based cryptographic hash functions). It is recommended that the manufacturer provides information of its verification process.

SU-002
The intent is to avoid the device being “bricked.”

SU-003
It is possible that the firmware/software updates are digitally co-signed by the operator.

SU-005
The intent here is to protect any embedded secret or cryptographic material. Refer to Sections 6.5 and 6.6 for requirements related to encryption.

6.4 Initial/Out-of-Box Configuration Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOB-001</td>
<td>A device SHALL NOT allow or accept an immutable login credential (username/password).</td>
<td></td>
</tr>
<tr>
<td>OOB-002</td>
<td>A device SHALL store passwords in a salted and hashed form.</td>
<td></td>
</tr>
<tr>
<td>OOB-003</td>
<td>A device SHALL NOT transmit a credential received in the clear for authentication.</td>
<td></td>
</tr>
<tr>
<td>OOB-004</td>
<td>A device SHALL be configured only with device unique passwords in default configuration.</td>
<td></td>
</tr>
<tr>
<td>OOB-005</td>
<td>A device SHALL disable optional network services by default.</td>
<td></td>
</tr>
<tr>
<td>OOB-006</td>
<td>A device SHOULD require that any device-unique default password be changed upon initial setup.</td>
<td></td>
</tr>
<tr>
<td>OOB-007</td>
<td>A device SHOULD support changing the host name where applicable of the device on the network.</td>
<td></td>
</tr>
<tr>
<td>OOB-008</td>
<td>A device SHALL NOT allow remote access to the user administrative interface unless a device-unique password is specified, or the initial password has been changed by the user.</td>
<td></td>
</tr>
<tr>
<td>OOB-009</td>
<td>A device SHALL be able to reset to the default factory settings and all customer and configuration data is erased.</td>
<td></td>
</tr>
<tr>
<td>OOB-010</td>
<td>A device SHALL have the means to authenticate itself to the operator’s network.</td>
<td></td>
</tr>
<tr>
<td>OOB-011</td>
<td>A device SHOULD have a logical identifier that is cryptographically attestable.</td>
<td></td>
</tr>
<tr>
<td>OOB-012</td>
<td>A device SHALL NOT allow a weak password or credential to be set.</td>
<td></td>
</tr>
</tbody>
</table>

6.4.1 OOB Requirements Clarifications

OOB-002
Refer to section 5.1.1.2 of [NIST 800-63B] for guidance on

- password storage,
- salt size,
- hash function strength, and
- cost factor of key derivation functions.

This document recommends that deprecated hashing functions like SHA1 and MD5 not be used.
OOB-003
Refer to NETS-001 for a recommendation.

OOB-004
Refer to OOB-001 for guidance on password strength.

OOB-005
Examples of optional services are UPnP/SSDP or even MoCA. Refer to Section 6.13 for more details.

OOB-008
Remote access to the administrative interface includes access to the device over the network through allowable
protocols like SSH, HTTPS, or equivalent mechanisms. OOB-004 specifies that a device be configured with device-
unique password and the changed password be strong as per OOB-001 and OOB-012. It is expected that access to an
interface that allows setting or changing the password will always be available.

OOB-009
The expectation is to ensure that any customer data (e.g., keys, passwords, confidential data, and any other data that
legally needs to be protected from disclosure) is cleared out, and the device is in factory out-of-box state to be
provisioned as a new device. Any logs that are retained need to be sanitized as well (see Section 6.10 for details).

OOB-010
The device is expected to authenticate and identify itself through a device-specific logical identifier and is
implementation specific. For CMs, it is recommended to use the Device Certificate ID. It is also recommended that
the identifier be attestable (see OOB-011); if manufacturer-specific values like a serial number are used, it is
recommended to namespace them.

OOB-012
It is recommended to use a passphrase instead of a password. If a password is to be used, it is recommended that the
password length be a minimum of 12 characters and not easily guessable, and the maximum supported value should
be no less than recommended by section 5.1.1.2 of [NIST 800-63B].

6.5 Data-at-Rest Protection Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRP-001</td>
<td>Any confidential or sensitive data/content in flash memory SHALL be encrypted.</td>
<td></td>
</tr>
</tbody>
</table>

6.5.1 DRP Requirements Clarifications

DRP-001
Confidential or sensitive data include data specific to the device and operational information (e.g., Wi-Fi
SSID/password), as well as data that legally needs to be protected from disclosure. It is recommended that all data,
including the firmware as well as operational/configuration data, be encrypted. Refer to KEY-002 for guidance on
storage of encryption/decryption keys. If the firmware is also encrypted, it is possible that the mechanism (e.g.,
usage of key/algorithm) to encrypt the firmware may be different from the mechanisms used to encrypt the data.
6.6 Data Exchange Encryption/Integrity Requirements

Table 6 - Data Exchange Encryption/Integrity Requirements (DE)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-002</td>
<td>A device SHALL only use approved and non-deprecated cipher suites for TLS connections.</td>
<td></td>
</tr>
<tr>
<td>DE-003</td>
<td>A device’s factory default configuration SHALL select key agreement protocols that provide forward secrecy (FS).</td>
<td></td>
</tr>
<tr>
<td>DE-004</td>
<td>A device’s factory default configuration SHALL select encryption algorithms that provides authenticated encryption with additional data (AEAD).</td>
<td></td>
</tr>
<tr>
<td>DE-005</td>
<td>The AEAD data SHOULD be used to provide additional context for the encryption.</td>
<td></td>
</tr>
<tr>
<td>DE-006</td>
<td>A device’s factory default configuration SHALL select a hash function that has equivalent security strength to SHA2 or higher.</td>
<td></td>
</tr>
<tr>
<td>DE-007</td>
<td>A device SHALL support disabling a given cipher suite.</td>
<td></td>
</tr>
</tbody>
</table>

6.6.1 DE Requirements Clarifications

DE-002

The list of recommended/approved cipher suites includes TLS 1.3 non-deprecated cipher suites [RFC 8446]. The following TLS 1.2 cipher suites also are allowed.

- DHE_RSA_AES128_CBC (only for cable modems)
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- DHE-DSS-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-AES256-SHA256

Any additional cipher suites explicitly required by the operator also are allowed. These suites may be needed to support legacy devices or services, and the expectation is to restrict their usage to the extent possible.

DE-003

Forward secrecy is defined as per section 7.6 of [NIST 800-56A].

The following key types are recommended in key-agreement schemes.

- For elliptic curve-based protocols, use protocols from curves in [NIST 800-56C].
- For RSA-based protocols, use keys as per [NIST 800-56B], with 4096 bit keys preferred.
- For TLS connections, see the clarification for DE-002 for allowed cipher suites.

For backwards compatibility, devices using DOCSIS BPI+ v1 are allowed even though it does not provide FS.
DE-004

It is expected that given a choice of available cipher suites, if a cipher suite that provides AEAD is available and supported, then that cipher suite be selected for usage over non-AEAD cipher suites.

DE-006

It is expected that the usage of SHA1 and/or MD5 be deprecated and be used only for supporting legacy services and/or backward compatibility. Refer to [FIPS 180-4] for correct usage of secure hash algorithms.

DE-007

It is recommended that there be two different cipher suites available for a given cryptographic function to support continued operation in the face of a cryptographic vulnerability. It is expected that disabling a cipher suite will typically be done by a network operator or manufacturer in situations when such a cipher suite is deemed unsuitable or compromised for the intended usage.

6.7 Securing Cryptographic Material Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEY-001</td>
<td>Any private keys used by the device for asymmetric cryptography SHALL be stored in tamper-resistant hardware-based secure storage or protected by a key-encryption key stored in tamper-resistant hardware.</td>
<td></td>
</tr>
<tr>
<td>KEY-002</td>
<td>Any persistent keys used by the device SHALL be stored in tamper-resistant hardware-based secure storage or protected by a key-encryption key stored in tamper-resistant hardware.</td>
<td></td>
</tr>
<tr>
<td>KEY-003</td>
<td>The device SHALL maintain integrity protected trust store to store any certificate (trust anchors) the device uses to validate certificates from remote end-points.</td>
<td></td>
</tr>
<tr>
<td>KEY-004</td>
<td>The gateway SHALL provide a mechanism to securely update trust anchors.</td>
<td></td>
</tr>
<tr>
<td>KEY-005</td>
<td>The gateway SHOULD provide a mechanism to securely renew any certificates and associated key pairs issued to the device.</td>
<td></td>
</tr>
<tr>
<td>KEY-006</td>
<td>Any device specific cryptographic material SHALL be unique for each device.</td>
<td></td>
</tr>
</tbody>
</table>

6.7.1 KEY Requirements Clarifications

KEY-001

Tamper-resistant storage mechanisms are expected to be implementation specific (e.g., Microchip ECC608B module).

KEY-002

Persistent keys are different from ephemeral keys that are generated and/or derived for each cryptographic session.

KEY-004/KEY-005

The manufacturer is to provide documentation for the mechanism(s). It is possible that the trust anchor for validation of firmware (secure boot) may not be updatable. Currently, certificates issued to devices for DOCSIS networks are not upgradeable.

KEY-005

Devices might not have the mechanisms to generate new private keys (e.g., in a crypto module).

KEY-006

The intent is to ensure any cryptographic material (e.g., keys) that the device uses to identify itself (to assert its identity, any device specific configuration, establishing authenticated sessions, etc.) is derived in a manner to ensure it is unique for that device.
6.8 Physical and Remote Management Interfaces Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MI-001</td>
<td>A device SHALL receive any operational configuration over a secure channel.</td>
<td></td>
</tr>
<tr>
<td>MI-002</td>
<td>A device SHALL only use secure protocols to establish any control and management channel(s).</td>
<td></td>
</tr>
<tr>
<td>MI-003</td>
<td>A device SHALL disable by default any physical and/or local communications ports that are not required for normal operations.</td>
<td></td>
</tr>
<tr>
<td>MI-004</td>
<td>A device SHALL support multi-factor authentication for administrative access.</td>
<td></td>
</tr>
<tr>
<td>MI-005</td>
<td>A device SHALL implement mechanisms to prevent brute force login/access attacks as recommended in [NIST 800-63B].</td>
<td></td>
</tr>
<tr>
<td>MI-006</td>
<td>A device that provides multiple simultaneous access sessions SHALL limit administrators to one session per login credential by default.</td>
<td></td>
</tr>
<tr>
<td>MI-007</td>
<td>A device SHALL NOT expose administrative access on a public/internet facing interface by default.</td>
<td></td>
</tr>
<tr>
<td>MI-008</td>
<td>Devices supporting advanced architectures such as virtual interfaces SHALL secure the virtual interfaces with the same controls as applied to physical interfaces to prevent unauthorized access.</td>
<td></td>
</tr>
<tr>
<td>MI-009</td>
<td>A device SHALL require periodic reauthentication (or authentication) following a configurable period of inactivity.</td>
<td></td>
</tr>
<tr>
<td>MI-010</td>
<td>Login sessions to a device SHALL have a configurable session inactivity timeout not to exceed 30 minutes.</td>
<td></td>
</tr>
<tr>
<td>MI-011</td>
<td>Devices SHALL support enabling and disabling any service or protocol and all associated ports or interfaces.</td>
<td></td>
</tr>
<tr>
<td>MI-012</td>
<td>Devices SHALL validate all inputs to the device to prevent improper resource use.</td>
<td></td>
</tr>
<tr>
<td>MI-013</td>
<td>Devices SHALL enable secure device management protocols only on interfaces over which they are expected to be used for the operation of the device.</td>
<td></td>
</tr>
<tr>
<td>MI-014</td>
<td>All end-user interfaces and protocols on the device SHALL be documented by the manufacturer.</td>
<td></td>
</tr>
</tbody>
</table>

6.8.1 MI Requirements Clarifications

**MI-001**
For CMs, the operational configuration is provided through a config file using mechanisms like BPI+ v1 with EAE.

**MI-002**
For example, if SNMP is being used and the device supports SNMP v3, an operator may enable SNMP v2 or v1 explicitly.

**MI-004**
The requirement is for the device to be able to support multi-factor authentication so that it can be enabled by the operator. See section 4.2.1 of [NIST 800-63B] for recommended multi-factor authenticator types. Support for multi-factor authentication can be in the form of a software-based implementation. The manufacturer may require that the device be online in order to support multi-factor authentication. An example of support for multi-factor authentication is the Linux PAM-based framework to support secondary authentication.

**MI-006**
In most common usages, a single administrative session is sufficient to perform administrative operations. If multiple sessions are being opened simultaneously, it can indicate a security event (e.g., an unauthorized access), a possible erroneous access (e.g., multiple authorized individuals accessing simultaneously), or in rare instances, a legitimate multiple session access (e.g., for debug/diagnostic purposes). Getting a notification of simultaneous access and enforcement of a single session by default allows the administrator to take appropriate action depending on the situation.
MI-007
A device is expected to have multiple interfaces, including but not limited to Ethernet, Wi-Fi, and virtualized interfaces. During normal operations, these interfaces can have different accessibility scope:

- accessible only on a local/LAN IP subnet for the subscriber,
- accessible only on the WAN side by the network operator’s infrastructure if it is also the operator management interface,
- accessible by any endpoint within certain physical proximity of the device (administrative access disabled by default), or
- accessible by any endpoint on the Internet (administrative access disabled by default).

Documentation for all operator interfaces needs to be provided to the operator.

MI-009
Refer to sections 4.3.3 and 7.2 of [NIST 800-63B] for recommended reauthentication timeout and periodic reauthentication.

MI-010
The session inactivity timeout needs to be provided as a global configurable option.

MI-011
A device is expected to disable by default any services that are not required for the device to become operational. Additional services are to be enabled based on configured operational configuration. Services like mDNS, SSDP/UPnP, etc., that are meant to operate within a subnet should not respond on management interfaces.

MI-012
Validating inputs can include using best practices for input sanitization (sections C4 and C5 of [OWASP PC]).

MI-013
Management protocols like TR-069/TR-369/SNMP/RESTCONF are not to be enabled on end-user interfaces. However, it is possible, such as in the case of DOCSIS CMCI interface, for SNMP to be enabled on that interface to support a self-install deployment model. In such instances, the access is to be authentication based on best practices specified in this document.

MI-014
Documentation on end-user interfaces and protocols is typically provided in an instruction manual and includes supported protocols that are available on the interfaces (what is available on the device).

6.9 Diagnostic, Debug, and Development Access Requirements

Table 9 - Diagnostic, Debug, and Development Access Requirements (DIAG)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAG-001</td>
<td>All access methods SHALL be documented (including any diagnostic access methods by supplier).</td>
<td></td>
</tr>
<tr>
<td>DIAG-002</td>
<td>Devices SHALL support enabling/disabling all methods of access to the device (local and remote).</td>
<td></td>
</tr>
</tbody>
</table>

6.9.1 DIAG Requirements Clarifications

DIAG-001
In conjunction with MI-003, this requirement ensures any access methods are disabled/secured by default. This information can be documented in an instruction manual if applicable and/or provided to the operator as part of an agreement.
DIAG-002
This includes any mechanisms covered by MI-003, MI-008, and MI-011.

6.10 Logging Requirements

Table 10 - Logging Requirements (LOG)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG-001</td>
<td>A device SHALL support logging of all administrative events.</td>
<td></td>
</tr>
<tr>
<td>LOG-002</td>
<td>A device SHOULD support remote logging via syslog or equivalent standard protocol.</td>
<td></td>
</tr>
<tr>
<td>LOG-003</td>
<td>A device SHOULD allow two or more remote logging endpoints to be defined.</td>
<td></td>
</tr>
<tr>
<td>LOG-004</td>
<td>A device SHALL use a secure channel for sending all remote logging traffic.</td>
<td></td>
</tr>
<tr>
<td>LOG-005</td>
<td>A device SHALL NOT log any sensitive information, including but not limited to passwords, encryption keys, API keys, usernames for unsuccessful login attempts, session keys, or other forms of credentials.</td>
<td></td>
</tr>
</tbody>
</table>

6.10.1 LOG Requirements Clarifications

LOG-001

The specific mechanism of logging will depend on the types of events being logged and is beyond the scope of this document.

Administrative events are events mandated by respective specifications.

Administrative events can result from changes/modifications to the operational configuration of the device and its services or can be notifications generated by the system in relation to the state of running processes. Some examples of administrative events are

- multiple failed login attempts,
- change of an administrative and/or user password,
- change in the firewall rules,
- change in the DNS or other network configuration, and
- a process or service exits abruptly.

LOG-004

This requirement is only applicable if LOG-002 is implemented.

Refer to the Data Encryption/Integrity section, specifically DE-002 and DE-004, for recommended encryption methods.

LOG-005

Any customer data that legally need to be protected from disclosure will not be logged.

6.11 Time Synchronization Requirements

Table 11 - Time Synchronization Requirements (TS)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS-001</td>
<td>A device SHALL support the capability to synchronize time using a standards-based time synchronization protocol.</td>
<td></td>
</tr>
</tbody>
</table>

6.11.1 TS Requirements Clarifications

TS-001

It is expected that the network provides the mechanism to synchronize the time on the device.
Common protocols include NTP [RFC 5905] and PTP [IEEE 1588-2019]. This requirement helps ensure operations that depend on time (e.g., certificate validation, incident response).

6.12 Software BOM and Software Updates Requirements

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBOM-003</td>
<td>A device SHALL provide downgrade protection to prevent installation of a prior version of firmware that may contain known vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>SBOM-004</td>
<td>A manufacturer SHALL NOT use software components/libraries that have publicly known vulnerabilities of [CVSS v3.1] base severity level of Medium and higher.</td>
<td></td>
</tr>
<tr>
<td>SBOM-005</td>
<td>A manufacturer SHALL maintain a list of all software/libraries used and provide the specific version of each component.</td>
<td></td>
</tr>
<tr>
<td>SBOM-006</td>
<td>A device SHALL use a [FIPS 140-3]-compliant version of a cryptographic library for new protocol implementations.</td>
<td></td>
</tr>
<tr>
<td>SBOM-007</td>
<td>A manufacturer SHALL NOT use a deprecated version of software components/libraries.</td>
<td></td>
</tr>
<tr>
<td>SBOM-008</td>
<td>A manufacturer SHOULD use the most recent stable versions of the software/libraries.</td>
<td></td>
</tr>
<tr>
<td>SBOM-009</td>
<td>All firmware updates SHOULD be capable of being digitally co-signed by the operator.</td>
<td></td>
</tr>
<tr>
<td>SBOM-010</td>
<td>A manufacturer SHOULD upgrade any software components/libraries with known applicable security vulnerabilities in a timely manner.</td>
<td></td>
</tr>
<tr>
<td>SBOM-011</td>
<td>Where allowable by contractual, legal, and regulatory requirements, discovered security vulnerabilities SHALL be disclosed to the operator and applicable partners.</td>
<td></td>
</tr>
</tbody>
</table>

6.12.1 SBOM Requirements Clarifications

SBOM-001

Refer to DE-002 and KEY-001 for recommendations on acceptable cryptographic functions for encryption and integrity protection.

SBOM-003

Note that downgrade protection is different from being able to roll back to a previous working version if the new version may break certain functionality of the device. Refer to [NIST 8259A] for guidance.

SBOM-004

Note that software components also include the underlying operating system, system libraries, and bootloaders. This is intended to apply to known vulnerabilities at the time of device firmware release. In certain circumstances (e.g., software components for legacy features or specialized capabilities), it is possible to not have feasible alternatives. Such situations need to be handled on a case-by-case basis.

SBOM-005

It is recommended that this list be maintained in a commonly used machine-readable format (e.g., [SWID], [SPDX], [CycloneDX]). The list may be provided to the operator as part of an agreement.

SBOM-006

There are limited notable legacy exceptions to this requirement, like DOCSIS versions below 3.1 and SNMPv3 key derivation functions (uses SHA1).

SBOM-007

The intent here is to avoid using deprecated software and versions at the time of the firmware/software release. A specific version of software may be deprecated after it has been used in a release. In such cases, SBOM-004 and SBOM-010 allow upgrading to a non-deprecated version.
It is recommended that any software components/libraries with known security vulnerabilities (publicly provided or identified through internal process) be upgraded in the subsequent release. It is recommended that software components/libraries are always kept up to date in each release, regardless of known applicable security vulnerabilities as part of life-cycle management, including avoiding software that is no longer supported. This reduces the difficulty of update when a vulnerability is detected. The expectation is that this is handled on a case-by-case basis.

The specific procedure and timeline for such disclosures are beyond the scope of this document.

### 6.13 Network Services and Listening Processes Requirements

#### Table 13 - Network Services and Listening Processes Requirements (NETS)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETS-001</td>
<td>A device that serves a Web UI SHALL use HTTPS to serve the UI.</td>
<td></td>
</tr>
<tr>
<td>NETS-002</td>
<td>A device that serves a Web UI SHALL follow [OWASP WSTG] security best practices (CSRF, session management, etc.).</td>
<td></td>
</tr>
<tr>
<td>NETS-003</td>
<td>A device that uses TLS SHALL use TLS 1.2 or higher.</td>
<td></td>
</tr>
<tr>
<td>NETS-004</td>
<td>A device SHALL NOT enable protocols primarily meant to operate on a local network on its WAN interface under any circumstances.</td>
<td></td>
</tr>
<tr>
<td>NETS-005</td>
<td>A device SHALL NOT implement or enable Telnet or FTP services.</td>
<td></td>
</tr>
<tr>
<td>NETS-006</td>
<td>Any firewall on the device SHALL support ingress and egress filtering of IPv4 and IPv6 packets.</td>
<td></td>
</tr>
<tr>
<td>NETS-007</td>
<td>Any firewall on the device SHALL permit only required protocols and services by default.</td>
<td></td>
</tr>
<tr>
<td>NETS-008</td>
<td>A device that serves a Web UI SHOULD support mutual authentication for operator-only administrative interfaces.</td>
<td></td>
</tr>
</tbody>
</table>

#### 6.13.1 NETS Requirements Clarifications

**NETS-001**

It is recommended that any services and traffic to HTTP be redirected to HTTPS. If a TLS domain certificate is not feasible, a self-signed certificate should be used. Note that DOCSIS systems specify access over HTTP on the CMCI interface that currently does not require TLS.

**NETS-002**

Refer to [OWASP] and [OWASP 10] for more details.

**NETS-003**

Recommended to use TLS 1.3.

**NETS-004**

Certain home networking protocols, like SSDP/UPnP, mDNS, and MOCA, are meant to be operated within a local network segment, and services utilizing such protocols should not listen and/or respond on WAN and/or Internet-facing interfaces.

**NETS-005**

Insecure protocols, such as telnet/FTP/TCP Small Services, are to be kept disabled.

**NET-007**

It is recommended that a set of firewall rules be available in the form of an easy-to-apply profile (e.g., high/medium/low). It is recommended that firewalls implement a least privileged design restricting services/protocols only to those required to deliver services to the customer.
6.14 Network Access Mechanisms Requirements

Table 14 - Network Access Mechanisms (Wi-Fi/Ethernet) Requirements (NETA)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETA-001</td>
<td>A device that hosts a Wi-Fi access point (or mesh controller) SHALL use Wi-Fi credentials that are unique for each customer.</td>
<td></td>
</tr>
<tr>
<td>NETA-002</td>
<td>A device that hosts a Wi-Fi access point (or mesh controller) SHALL enable WPA2 [WFA Security] or higher by default.</td>
<td></td>
</tr>
<tr>
<td>NETA-003</td>
<td>A device that has wired ethernet ports SHOULD support 802.1X network authentication on those ports.</td>
<td></td>
</tr>
</tbody>
</table>

6.14.1 NETA Requirements Clarifications

NETA-001/NETA-002

WPA3 is recommended. See [WFA Security] for more details. Anything below WPA2 is not to be allowed.

NETA-003

The intent is to ensure all ports are secured and avoid misuse (e.g., theft of service, unauthorized access) where the device is deployed in a public setting (ports can be accessed by unauthorized individuals).

6.15 Additional Requirements

Table 15 - Additional Requirements (AR)

<table>
<thead>
<tr>
<th>REQ#</th>
<th>Description</th>
<th>Status/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AR-001</td>
<td>A device that includes any audio, video, or other sensors (e.g., microphone/camera) SHALL inform the consumer that the capability exists.</td>
<td></td>
</tr>
<tr>
<td>AR-002</td>
<td>A device while using any audio, video, or other sensors (e.g., microphone/camera) SHALL have an indication to show that the capability is active.</td>
<td></td>
</tr>
</tbody>
</table>

6.15.1 AR Requirements Clarifications

AR-001/AR-002

Both AR-001 and AR-002 are security requirements in the context of ensuring that unauthorized or unintentional use can be monitored by the user. The end user can be informed by having an icon/sticker indicating that the capability/sensor exists and/or alternately document it in the instruction manual.

AR-002

The mechanism of providing the indication is implementation dependent (i.e., tied to the hardware). If the gateway includes a surveillance function by design, implementation requirements are left to the operator.
7 ADVERSARIAL ENGINEERING

This document is intended to provide basic requirements that will improve the experience of subscribers. However, security functions and features always exist in an adversarial context—there are people actively trying to subvert or change the subscriber experience. Moreover, new exploits are often discovered that are not addressed by existing security requirements. Gateway devices must respond to this environment. New requirements can be developed at any time; parties responsible for the security of gateway devices are expected to diligently improve security even beyond current requirements.

Two unique resources that may assist in achieving this goal are the OWASP Top 10 [OWASP 10] and the CWE Top 25 Most Dangerous Software Weaknesses [2021 CWE 25]. These are periodically updated, and links are provided in the References section.
Appendix I  Acknowledgements

We wish to thank the following participants contributing directly to this document.

Contributors

Jeff Rowell, Travis Naas, Tyler Sutterby, Charles Cook
Wes Beebee
Yeqing Wang, Michael Baker, Vaibhav Garg, Omolewu Oluwatosin, Thomas Schiavinato
Robin Lavoie
Ali Negahdar
David Taylor, Kinney Bacon
Travis Stricklin, Mark Ambrozin
Harvey Lodder
Satish Mudugere, Onur Zengin
Pradeep Kanda, Hitesh Khurana
Ryan Speers
Andy Chan, Greg Macijuk, Ron Ripley
Andrew Barber, Jonathan Towers
Michael Gaul, Richard Pitts
Darshak Thakore, Simon Krauss, Brian Scriber, Kyle Haefner, Steve Goeringer, Mark Walker, Gabby Gordon, Max Pala

Company Affiliation

Charter
Cisco
Comcast
Cogeco
Commscope
Cox
Kyrio
Liberty Global
Maxlinear
Mediacom
River Loop Security
Shaw
Sparklight/Cable One
Technicolor
CableLabs

***