Draft ETSI EN 303 800-3 V0.0.18 (2024-11)

Environmental Engineering (EE);
Assessment of material efficiency of
ICT network infrastructure goods (circular economy);
Part 3: Server and data storage product availability of firmware and of security updates to firmware

Reference
DEN/EE-EEPS47-3

Keywords
availability, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Environmental Engineering (EE), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI EN Approval Procedure (ENAP).

The present document establishes the means for the verification of compliance with the requirements for the availability of firmware and of security updates to the firmware for servers and data storage products.

The present document is part 3 of a multi-part deliverable covering Environmental Engineering (EE); Assessment of material efficiency of ICT network infrastructure goods (circular economy), as identified below:

Part 2: "Server and data storage product secure data deletion functionality";

Part 3: "Server and data storage product availability of firmware and of security updates to firmware";

Part 5: "Server and data storage product disassembly and disassembly instruction".

NOTE: Part 1 and Part 4 have been cancelled as their intended content is already covered by other standards.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document concerns server and data storage products, it establishes the means for the verification of compliance with the requirements for the availability of firmware and of security updates to the firmware for servers and data storage products.

Introduction

The present document specifies how to make available:

a) the latest available version of the firmware; and

b) the latest available security update to firmware,

for a period of eight years, after the placing on the market of the last product of a given product model.

The present document was developed jointly by ETSI TC EE and ITU-T Study Group 5. It is published respectively by ITU and ETSI as Recommendation ITU-T L.ME_AF [i.5]) and ETSI EN 303 800-3 (the present document), which are technically equivalent.

1 Scope

The present document specifies how manufacturers of server products and online data storage products make available the latest available firmware version and the security updates to the firmware, to whom these updates are made available to and the skill levels required to install these updates.

The present document covers the servers and online data storage products.

The present document does not cover the following products:

a) servers intended for embedded applications;

b) servers classified as small scale servers;

c) servers with more than four processor sockets;

d) server appliances;

e) large servers;

f) fully fault tolerant servers;

g) network servers;

h) small data storage products;

i) large data storage products;

j) are used in means of transport for persons or goods [i.3].

The present document covers the latest available firmware version which are system, hardware component or peripheral programming provided with server or storage products, to provide basic instructions for hardware to function inclusive of all applicable programming and hardware updates.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] EN 45554: "General method for the assessment of the ability to repair, reuse and upgrade energy-related products", (produced by CENELEC).

[i.2] Commission Notice: "The 'Blue Guide' on the implementation of EU products rules 2016".

[i.3] Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products.

[i.4] ICT Task Force Study: "Task 12 Final Policy Recommendations ICT".

[i.5] Recommendation ITU-T L.ME_AF: "Assessment of material efficiency of ICT network infrastructure goods (circular economy). Part 3: server and data storage product availability of firmware and of security updates to firmware".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

customer: individuals or organizations that have purchased products for their own internal use

deployment: process for server and storage device firmware preparation, installation and post installation

NOTE 1: The preparation includes product environment and product preparatory activities, the installation is the act of replacing one firmware version with another and the post installation activities serve to bring the prouct back to an operational status.

NOTE 2: See Annex A for the informative background and factors affecting deployment.

firmware: system, hardware, component, or peripheral programming provided with the product to provide basic instructions for hardware to function inclusive of all applicable programming and hardware updates

NOTE 1: Hardware, software, code, components, instructions, programming provided *for, with or to the* product to support enhancements, elements, features and added functionality *beyond* basic instructions for hardware to function are not within the scope of the present document.

NOTE 2: Firmware, that is necessary for the functioning of the device, is part of the device hardware and represented by the dark blue shade in figure 1. Device Software, such as Operating Systems, are represented by the light blue shade. The system level, which crosses the boundaries of the device, refers to application software (light orange shade), cloud services and other ICT services (dark orange shade). Only firmware is within the scope of the present document .

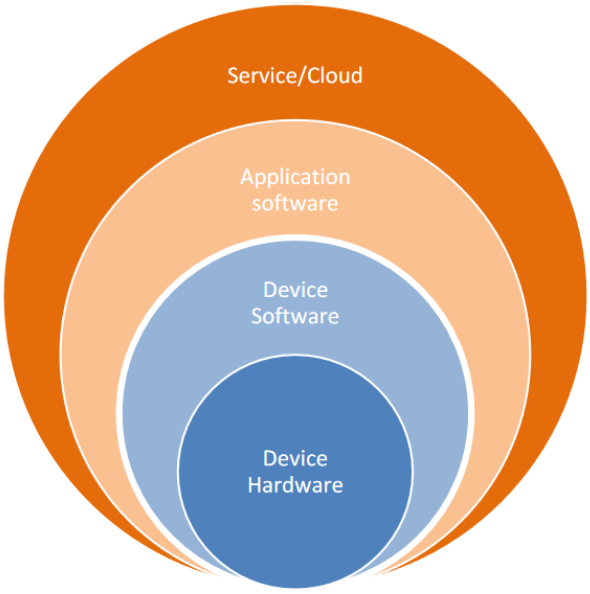

Figure 1: The multiple layers of ICT systems [i.4]

free of charge: no financial charge by a manufacturer, their authorized representatives or importers

latest available version: latest version of firmware or security update to the firmware, as applicable, that the manufacturer determines at their discretion is the latest version, and has made generally available for all customers of a product model, which has been placed on the market by a manufacturer

manufacturers: This definition is present within section 3.1 of the EU Blue guide [i.2].

security update to firmware: change made to firmware to mitigate, or remove, an identified vulnerability

NOTE 1: Different term for security update is a "remediation".

NOTE 2: Different terms used for remediation could include mitigation, patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures. The remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile.

vulnerability: weakness or flaw in the computational logic of firmware that, when exploited, results in a negative impact to confidentiality, integrity, or availability of an impacted firmware or software component

NOTE: "computational logic" can also be referred to as "code".

3.2 Symbols

Void.

3.3 Abbreviations

Void.

4 Technical requirements specifications

4.1 Environmental profile

The technical requirements of the present document apply under the environmental profile for operation of the equipment, which shall be in accordance with its intended use. The equipment shall comply with all the technical requirements of the present document at all times when operating within the boundary limits of the operational environmental profile defined by its intended use.

4.2 Conformance requirements

4.2.1 Time period of availability

Availability of security updates, to the firmware version, begins when the product is first placed on the market, provided that date occurs after March 1st 2021.
Availability of firmware will begin 2 years from when the product is first placed on the market, provided that date occurs after March 1st 2021 e.g. an April 2021 date will equate to an April 2023 availability date.

Final availability, for both firmware and security updates, to the firmware version, will be at least 8 years from when the product was last placed on the market. The 8-year availability period applies only to the placement on the market of the last product model in scope. The availability period does not apply from the point when firmware version and security updates are released, which may occur after the placement on the market of the last product model in scope.

4.2.2 Skill level

Manufacturers shall determine the skill classification, A to D, for any given firmware version, or security updates to the firmware version, as per table 1. Only technical factors shall be used for this determination and are subject to verification (see clause 4.2.4).

Table 1: Alignment of deployment to skill level for firmware updates

Manufacturers Classification	Class & category (see note 1)	Category detail
User deployment	A - C Layman, Generalist, Independent Expert	The process can be reasonably carried out by persons with the relevant knowledge and experience, following written instructions, taking into account: • Industry standard technologies. • The risk of product or environmental damage from a mishandled deployment process.
Supported or specialist deployment	D Authorized Partner or Manufacturer	The process requires specialist skills, knowledge or direct support from the manufacturer due to: • Genuine physical safety risks. • Significant risk of product or environment damage from mishandled deployment process. • High product complexity that may require: – manufacturer developed tools and associated training/experience in their use; – custom developed deployment process; – Intervention required by/from Manufacturer's support systems. Neither business nor commercial justifications are acceptable.
NOTE 1: Class and category descriptions from EN 45554 [i.1]. NOTE 2: IEC safety standard references of Ordinary Person, Instructed Person and Skilled person. The EN 45554 [i.1] terms are Layman, Generalist, Independent Expert, Authorized Expert and Manufacturer.		

See Annex A for more information.

4.2.3 Distribution

For the distribution of firmware, in cases where a Manufacturer's classification is "user deployment" (classes A to C) see clause 4.2.2, then manufacturers shall make firmware versions and security updates to the firmware versions available in an accessible manner to customers and Independent Repair Service Providers.

For distribution of firmware, in cases where a manufacturer's classification is "Supported or specialist deployment" (class D), see clause 4.2.2, then the provision of firmware will be part of the deployment process

NOTE: By way of an example, a manufacturer may distribute on an available website or via electronic communication.

4.2.4 Verification

Verification of compliance is performed by member state authorities verifying that the chosen condition for a given firmware version or security update to the firmware version meets the requirements.

Table 2: Verification

Type	Condition	Means of verification
Version of the firmware	Latest available version	Confirm a given version is the latest one made generally available for all customers of a product model, which has been placed on the market by a manufacturer.
	Made available	Versions are available in an accessible manner to audiences identified in clause 4.2.3.
	From two years after the placing of the market of the first product of a certain product model	Confirm the initial firmware availability is in line with the placement on the market of the first product of a certain product model.
	For a minimum period of eight years after the placing on the market of the last product of a certain product model	Confirm that the end of availability date is at least eight years after the placing on the market of the last product of a certain product model.
	Free of charge or at a fair, transparent and non-discriminatory cost	Confirm that: i) there is no financial charge by a manufacturer, their authorized representatives or importers associated with the firmware update; or ii) the cost is fair, transparent and non- discriminatory.
	Skill level for deployment	Confirm that the skill level classification is class A to C, or class D (see table 1).
Security update to the firmware	Latest available version	Confirm a given version is the latest one made generally available for all customers of a product model, which has been placed on the market by a manufacturer.
	Made available	Versions are available in an accessible manner to audiences identified in clause 4.2.3.
	From the time a product model is placed on the market	Confirm the availability of initial security update to the firmware, is in line with the placement on the market of the first product of a certain product model.
	Until at least eight years after the placing on the market of the last product of a certain product model	Confirm that the end of availability date is at least eight years after the intended placing on the market of the last product of a certain product model.
	Free of charge	Confirm there is no financial charge by a manufacturer, their authorized representatives or importers associated with the security update to the firmware update.
	Skill level for deployment	Confirm that the skill level classification is class A to C, or D (see table 1).

Annex A (informative): Skill levels for firmware deployment

A.1 Background

A.1.1 Directive 2009/125/EC - establishing a framework for the setting of ecodesign requirements for energy-related products

Article 15 of Directive 2009/125/EC [i.3] states that:

"5. Implementing measures shall meet all the following criteria:

(a) there shall be no significant negative impact on the functionality of the product, from the perspective of the user;
(b) health, safety and the environment shall not be adversely affected;
(c) there shall be no significant negative impact on consumers in particular as regards the affordability and the life cycle cost of the product;
(d) there shall be no significant negative impact on industry's competitiveness;
(e) in principle, the setting of an ecodesign requirement shall not have the consequence of imposing proprietary technology on manufacturers; and
(f) no excessive administrative burden shall be imposed on manufacturers."

A.1.2 Consumer vs "Business to Business" product

Consumer ICT (or business to consumer) products, e.g. laptops, smart phones, printers, are purchased by individuals, or households, for personal use. These products are limited in complexity and workloads with a resulting simplicity in operation and maintenance.

There are a broad range of server and storage products, within scope for the present document, and these are all Enterprise products. They contain multiple elements, both software and hardware, which often need to be specifically configured for the environment they are operating within (environments which consumers do not have). These are products which are sold to a business to support the activities of that business. The technologies, scale and cost of these devices varies but in the majority of instances they do not work independently, but are typically part of, and inter-dependant with, a much wider infrastructure or environment. The operation of the device itself becomes a component of the overall business solution it is supporting.

The vast majority of consumer devices are entirely independent and failure in many cases is limited to consumer inconvenience. The impact for Enterprise ICT devices depends entirely on environment they are supporting and the design and requirements of business environments vary greatly, in terms of volume and mix of industry standard and proprietary devices both hardware and software. Distributed, or edge, environments add more complexity. Many organizations utilize a mix of technologies from different manufacturers, which introduces further interoperability challenges

Management of updates across one of these Enterprise environments could take substantial knowledge, training and a suite of commercial and proprietary software tools: many organizations contract support back to the manufacturers or out to specialized third parties (of which there are many) for this reason. The impact of a failed process could negatively impact the environment the infrastructure is managing, e.g. could be hazardous in themselves (e.g. nuclear), critical to human life (e.g. medical, avionics, mass transit) or impact the social fabric (e.g. personal data, education, banking, internet, military).

Consumer products are typically sold in multiple millions. Enterprise products are sold in their hundreds to hundreds of thousands, depending on technology. It is important to note that, from a volume perspective, there are far more low/medium complexity products vs high complexity in the market, indicating a majority of products being classified as "user deployment", with regards to their deployment process.

A.2 Deployment process

A.2.1 Introduction

The definition of Firmware installation, in the present document , is the physical act of replacing one firmware version with another. However, for enterprise product, installation is just one part of an overall deployment process, which includes environment and product preparation, the actual installation piece together with post installation activities in order to bring the product back to operational status.

In addition, firmware updates can have product or environment configuration pre-requisites that are often more complex and exacting than the actual deployment itself.

For consumer devices, deployment and installation are often the same and consist of just hitting the "install" button.

It is important to link the decision around classifying the deployment process of a product to:

a) The complexity of the deployment process.

b) The complexity of the product and its environment.

c) The risks, of deployment, to both to the product itself and the environment in which it is operating.

Given the broad range of product technologies, within scope, and the diversity of environments they are utilized within then deployment processes will vary widely in complexity and difficulty. Expertise in one technology and/or environment, from one manufacturer, may not equate expertise in others.

The difficulty of the deployment process can be classified using a variety of factors. This may result in some products currently on the market being considered simpler to deploy than Class C (expert - see table 1 in the present document) and some more difficult.
Difficulty may also be aligned with potential disastrous outcomes (risks) of the process.

A.2.2 Factors affecting deployment

A.2.2.1 Interoperability & compatibility

Deploying firmware to a single element, e.g. a network card in a server or a hard drive in a storage array, may be seen as fairly straightforward. However, these elements function in conjunction with many others, inside the product. In addition, the product is required to function with other hardware and software in the wider environment.

Changes to one element may require changes to others in order to maintain the integrity of the product itself, solution and environment. Ensuring compatibility for just one update can be a complex task, in itself.

A.2.2.2 Industry standard technology

Products which utilize mature and well understood design technologies of both hardware and software, usually termed industry standard such as x86 architecture, networking and communications protocols, etc., would usually fall into classes A to C. This would encompass the majority of products, within scope for the present document. Industry standard does not equate to a Consumer product.

A.2.2.3 Risk of business interruption and data loss.

With complex products, there is always a risk associated to the business of updating a product in a live environment. Data unavailability (which results if/when a system upgrade is not successfully applied resulting in the data storage being offline for longer than planned) or loss/corruption of data can result. This cost could equate to more than the systems themselves.

Where the product is deployed to applications in sensitive environments such as critical infrastructure or supporting the processing sensitive workloads, which cannot suffer interruption, then a deployment process may not have scope for failure and customers may prefer that their updates are supported by the product manufacturer.

A.2.2.4 Loss of physical product integrity

Potential damage to the product, hardware or software may occur through an incomplete or incorrect deployment of an update. The most common issue arises from an interruption of the actual installation process, but may equally stem from interoperability and other inadequate steps in the deployment process.

Where "re-levelling or re-baselining" a product, without live production data, the process can still be complex with a similar risk of unrecoverable inoperability.

A.2.2.5 Multi-step process

In order to deploy a firmware revision on a product, the product may be required to be on certain revisions across it is different elements. This may require a sequence of carefully managed updates in order to reach that revision, e.g. version 1 to version 2 through to version 10. The multi-step upgrade process, and the dependencies required to perform a successful upgrade of each, leads to higher risk.

A.2.2.6 Compromise to product configuration

Products placed on the market by Manufacturers are tested to ensure interoperability for their expected use. Only certain configurations of hardware and software are tested.
Correct configuration, of the software and hardware elements, on complex products is essential or there is a risk of failure, which may be unrecoverable. Sometimes, the deployment process itself may necessitate reconfiguration of the product.

A.2.2.7 Transferable expertise

There may be differences in configuration, in both product (hardware and software) and environment, across products ostensibly within the same product group which may vary the deployment process and complexity. In addition, the product offerings from different manufacturers (in the same product group) may also vary enough to require different expertise/skillsets.

A.2.2.8 Genuine physical safety risks

In rare instances, the updating of a product may carry a genuine physical safety risk if not correctly carried out.

A.3 Conclusion

A manufacturer does not purposefully design complexity into products, this comes are a result of the requirements of organizations who have increasingly unique and complicated business environments and requirements. Solving these challenges may come at the expense of simplicity.

To overcome this inherent complexity, and associated risk, Manufacturers invest significant resources into extensive training and software tools which enable them to consistently complete successful deployment of firmware updates.

Given:

a) the broad nature of the product technologies within scope; and

b) implementing simplification of high complexity products may mean negative impact to their functionality, from a user perspective; and

c) evolving business requirements and associated (new) technologies to resolve them.

Manufacturers cannot guarantee that given firmware versions, or security updates to the firmware versions can be deployed successfully by any fixed or pre-defined level of skill. Firmware versions, or security updates to the firmware versions, will align to the appropriate class and category in the standards document (see table 1) taking into account a variety of factors affecting the deployment process. This reflects the technical issues surrounding the deployment process including the complexity of the product, environment and the associated risks, but not any commercial or business justifications.

History

Document history			
V0.0.18	November 2024	EN Approval Procedure	AP 20250205: 2024-11-07 to 2025-02-05