Draft ETSI EN 303 800-2 V0.0.11 (2025-01)

Environmental Engineering (EE);
Assessment of material efficiency of ICT network infrastructure goods (circular economy);
Part 2: Server and data storage product secure data deletion functionality

Reference
DEN/EE-EEPS47-2

Keywords
environment, e-waste management, KPI, server, storage, waste management

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 4
Foreword 4
Modal verbs terminology 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 9
3.3 Abbreviations 9
4 Assessment of the secure data deletion functionality for servers and data storage products 10
4.1 Provision of functionality to perform secure data deletion 10
4.1.1 Availability of functionality 10
4.1.2 Availability of clear or purge method 10
4.1.3 Availability of destruct method and additional methods 10
4.1.4 Returning Server or Data Storage Equipment to usable state 10
4.2 Data exclusions from data deletion provision 10
4.3 Registration 11
5 End-user verification of successful Data Deletion 11
5.1 Means of end-user verification of the effectiveness of the deletion method 11
5.2 Record of Data Deletion 11
6 Assessment of data deletion documentation and functionality 12
6.1 Means of assessment 12
6.2 Verification of secure data deletion documentation 12
6.2.1 Information on secure data deletion functionality 12
History 13

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 is part 2 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.

Introduction

The present document addresses the requirements on secure data deletion. It aims to give a valid and compliant method to assess if this specific requirement on data deletion has been met.

The present document was developed jointly by ETSI TC EE and ITU-T Study Group 5 and published by ITU and ETSI as Recommendation ITU-T L.ME_DD [i.4] and ETSI EN 303 800-2 (the present document), which are technically equivalent.

1 Scope

The present document specifies a method for the verification of compliance with the requirements on the secure data deletion functionality for:

1) servers; and

2) data storage equipment.

The present document covers demonstration of compliance with the data deletion requirements:

- instructions on how to use the functionality;
- the techniques used; and
- the supported secure data deletion standard(s), if applicable.

The following products are out of scope of the present document:

- servers intended for embedded applications;
- servers classified as small scale servers in terms of Regulation (EU) No 617/2013 [i.2];
- servers with more than four processor sockets;
- server appliances;
- large servers;
- fully fault tolerant servers;
- network servers;
- small data storage products;
- large data storage products;
- servers or data storage products which in addition are used in means of transport for persons or goods;

NOTE: See Directive 2009/125/EC [i.1].

- data storage devices that are not included in the product placed on the market by the Manufacturer, their authorized representatives or importer, and are not included in modifications or updates provided or specified by the manufacturer, their authorized representatives or importer.

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.

[1] IEEE 2883™-2022: "IEEE Standard for Sanitizing Storage".

[2] ETSI EN 303 800-5: "Environmental Engineering (EE); Assessment of material efficiency of ICT network infrastructure goods (circular economy); Part 5: Server and data storage product disassembly and disassembly instruction".

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] 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 (recast).

[i.2] Commission Regulation (EU) No 617/2013 of 26 June 2013 implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to ecodesign requirements for computers and computer servers.

[i.3] European Commission Notice 2016/C 272/01: "The 'Blue Guide' on the implementation of EU products rules 2016".

[i.4] Recommendation ITU-T L.ME_DD: "Assessment of material efficiency of ICT network infrastructure goods (circular economy)- Part - 2: server and data storage product secure data deletion functionality".

[i.5] Commission Regulation (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

clear: sanitisation using logical techniques on user data on all addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user

NOTE: See IEEE 2883-2022 [1].

cryptographic erase: method of sanitisation in which the encryption key for the encrypted target data is sanitised, making recovery of the decrypted target data infeasible using state-of-the-art laboratory techniques

NOTE: See IEEE 2883-2022 [1].

data sanitisation: process of deliberately and irreversibly deleting or destroying any data stored in memory on a device to render it unrecoverable

data storage device: device providing non-volatile data storage, with the exception of aggregating storage elements such as subsystems of redundant arrays of independent disks, robotic tape libraries, filers, and file servers and storage devices which are not directly accessible by end-user application programs, and are instead employed as a form of internal cache

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

data storage product: Fully-functional storage system that supplies data storage services to clients and devices attached directly or through a network. Components and subsystems that are an integral part of the data storage product architecture (e.g. to provide internal communications between controllers and disks) are considered to be part of the data storage product. In contrast, parts that are normally associated with a storage environment at the data centre level (e.g. devices required for operation of an external storage area network) are not considered to be part of the data storage product. A data storage product may be composed of integrated storage controllers, data storage devices, embedded network elements, software, and other devices.

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

destruct: sanitisation using physical techniques that make recovery of target data infeasible using state of the art laboratory techniques and results in the subsequent inability to use the storage media for storage

NOTE: See IEEE 2883-2022 [1].

embedded application: software application that permanently resides in an industrial or consumer device, typically stored in a non-volatile memory such as read-only memory or flash memory

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

full verification: process of validating each area of memory to ensure the success of a data sanitisation attempt

fully fault tolerant server: server that is designed with complete hardware redundancy (to simultaneously and repetitively run a single workload for continuous availability in mission critical applications), in which every computing component is replicated between two nodes running identical and concurrent workloads (i.e. if one node fails or needs repair, the second node can run the workload alone to avoid downtime)

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

large data storage product: high end or mainframe data storage product that supports more than 400 data storage devices in its maximum configuration and with the following required attributes: no single point of failure, non-disruptive serviceability and integrated storage controller

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

large server: resilient server which is shipped as a pre-integrated/pre-tested system housed in one or more full frame racks and that includes a high connectivity input/output subsystem with a minimum of 32 dedicated input/output slots

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

manufacturer: any natural or legal person who manufactures a product or has a product designed or manufactured, and places it on the market under their own name or trademark

NOTE: See Commission Notice [i.3] (p. 28).

multi-node server: Server that is designed with two or more independent server nodes that share a single enclosure and one or more power supply units. In a multi-node server, power is distributed to all nodes through shared power supply units. Server nodes in a multi-node server are not designed to be hot-swappable.

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

network server: network product which contains the same components as a server in addition to more than 11 network ports with a total line rate throughput of 12 Gb/s or more, the capability to dynamically reconfigure ports and speed and support for a virtualized network environment through a software defined network

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

online data storage product: data storage product designed for online, random-access of data, accessible in a random or sequential pattern, with a maximum time to first data of less than 80 milliseconds

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

overwriting: process of replacing old data with new data

purge: sanitisation using logical techniques or physical techniques that make recovery of target data infeasible using state of the art laboratory techniques, but that preserves the storage media and the storage device in a potentially reusable state

NOTE: See IEEE 2883-2022 [1].

resilient server: server designed with extensive reliability, availability, serviceability and scalability features integrated in the micro architecture of the system, Central Processing Unit (CPU) and chipset

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

responsible entity: entity employing the responsible person

responsible person: person or entity responsible for Data Sanitisation on a Server or Data Storage Product

server: Computing product that provides services and manages networked resources for client devices, such as desktop computers, notebook computers, desktop thin clients, internet protocol telephones, smartphones, tablets, tele-communication, automated systems or other servers, primarily accessed via network connections, and not through direct user input devices, such as a keyboard or a mouse and with the following characteristics:

a) it is designed to support server Operating Systems (OS) and/or hypervisors, and targeted to run user-installed enterprise applications;

b) it supports error-correcting code and/or buffered memory (including both buffered dual in-line memory modules and buffered on board configurations);

c) all processors have access to shared system memory and are independently visible to a single OS or hypervisor.

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

server appliance: server that is not intended to execute user-supplied software, delivers services through one or more networks, is typically managed through a web or command line interface and is bundled with a pre-installed OS and application software that is used to perform a dedicated function or set of tightly coupled functions

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

server with more than four processor sockets: Server containing more than four interfaces designed for the installation of a processor. For multi-node servers, this term refers to a server having more than four processor sockets in each server node.

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

small data storage product: data storage product containing a maximum of three data storage devices

NOTE: See Commission Regulation (EU) 2019/424 [i.5].

3.2 Symbols

Void.

3.3 Abbreviations

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

CPU	Central Processing Unit
MAC	Media Access Control
OS	Operating Systems

4 Assessment of the secure data deletion functionality for servers and data storage products

4.1 Provision of functionality to perform secure data deletion

4.1.1 Availability of functionality

Server and Data Storage Products shall provide a Data Deletion function.

In the event of the Server or Data Storage Equipment end user wishing to perform secure data deletion, it shall be possible to perform data sanitisation on all data storage devices that may contain end user data.

The data controller shall decide on the minimum appropriate method of data deletion.

4.1.2 Availability of clear or purge method

Server or Data Storage Equipment end users shall be provided with the ability and information on how to apply the clear method or purge method of sanitisation.

4.1.3 Availability of destruct method and additional methods

The Server or Data Storage Equipment end user shall also have the ability and information on how to apply additional or alternate methods of data deletion. This may include the Destruct method.

It shall, in addition, be possible to disassemble according to ETSI EN 303 800-5 [2] the data storage devices from the Server or Data Storage Equipment so that the devices can be destroyed in cases of highly sensitive data or where data storage devices may have developed a fault that prevents data deletion. Where faults are detected in the data deletion process, a warning shall be presented that the Data Deletion may not have been successful on the device.

NOTE: The destruct method does not enable reuse of the device.

4.1.4 Returning Server or Data Storage Equipment to usable state

After completing data deletion using a method described in clause 4.1.2, means should be provided to return the data storage devices to a usable state.

4.2 Data exclusions from data deletion provision

In order to allow for device reuse, the following data types should not be deleted in a standard data deletion process:

- Essential Product Data, including software and firmware required for the functioning of the Server or Data Storage Equipment.

NOTE 1: Examples include MAC address, hard drive size or format, firmware contained in modules, etc.

- Product Data Required for Regulatory or Legal Compliance.

NOTE 2: Examples include permitted frequency bands by country for Wi-Fi® modules, soft copies of certification marks and texts (e.g. CE, FCC, CCC, E-labelling), etc.

Where the above data is deleted, the user should be provided with a function to reinstate it.

4.3 Registration

In the case of information being made available to the target group of independent repair service providers/operators, the manufacturers or their authorized representatives and importers:

- may request the third party to qualify that it is dealing with maintenance, repair, reuse, recycling and upgrading of servers;
- may require registration by the interested third party on a website.

NOTE: This target group includes any self-employed professional, as well as any legally established organization, providing services dealing with maintenance, repair, reuse, recycling and upgrading of servers (including brokers, spare parts repairers, spare parts manufacturers, recyclers and third party maintenance).

Manufacturers - or their authorized representatives and importers - are able to reject the application based e.g. on the following conditions:

- If the third party is on the counterfeit watchlist, or if the third party is located in a country under embargo or if the third party has been convicted of counterfeiting in the past.
- If the third party is a direct or potential competitor.

The third party rejected needs to be informed of the reasons for rejection.

5 End-user verification of successful Data Deletion

5.1 Means of end-user verification of the effectiveness of the deletion method

For equipment in a state where data has been deleted and Data Deletion has been verified, means shall be provided to confirm all traces of data have been erased from the Server or Data Storage Device. If it is found that data is still recorded on the Server or Data Storage Device, this will be notified to the end user via a symbol or message and the verification status updated.

Server or Data Storage Equipment end users shall be provided with information and functionality to verify successful data deletion, as appropriate depending on the data deletion method:

- by physical inspection as defined in IEEE 2883-2022 [1]; or
- using full verification as defined in IEEE 2883-2022 [1] where it is possible; or
- using verification for media based cryptographic erase as defined in IEEE 2883-2022 [1] where it is not possible to use full verification.

Where Data Deletion cannot be verified according to the above then an alternate method acceptable to the end user may be offered, otherwise the destruct method as defined in clause 4.1.3 shall be available for data deletion.

5.2 Record of Data Deletion

Results of the verification shall be recorded. The record for each Data Deletion operation on Servers and Data Storage Equipment shall include:

- The Responsible Person, Responsible Entity.
- Date of Data Deletion.
- Warnings or errors detected during the Data Deletion process.
- Provision for the Responsible Person for Data Deletion to record remedial action for errors and warnings.

If the record is held on the Server or Data Storage Product, it shall be considered under the exclusions listed in clause 4.2.

Optionally, the media can be marked to indicate that the data deletion function has been performed and no additional data has been placed on it.

6 Assessment of data deletion documentation and functionality

6.1 Means of assessment

Verification of the secure data deletion functionality for servers and data storage products shall be ensured via provision of the following documentation regarding the secure data deletion functionality:

- information on the availability of secure data deletion functionality;
- instructions on how to implement the data deletion functionality and the supported secure data deletion standard(s) if applicable;
- information as described in clause 5.2 on the availability of a method for the end-user to evaluate the effectiveness of data deletion functionality.

6.2 Verification of secure data deletion documentation

6.2.1 Information on secure data deletion functionality

Table 1 shows the means by which the conditions and requirements of the present document can be verified. Documentation provided with the product shall contain at least the following information:

Table 1: Verification Approach

Product	Memory type	Deletion method /techniques/ tool available	Instructions on how to use deletion functionality	End-user verification method for effectiveness of deletion	GUI / UI availability
E.g. SKU, PID	E.g. SSD, HDD	E.g. clear, purge, destruct	E.g. command line sequence	E.g. read-back check	E.g. Yes/No

If a storage device has multiple types of storage media (e.g. magnetic and NAND), then the method of sanitisation shall be specified for each storage media type. More information on media type-specific sanitisation methods is available in IEEE 2883-2022 [1].

History

Document history			
V0.0.11	January 2025	ENAP process	AP 20250424: 2025-01-24 to 2025-04-24