ETSI TS 103 643 V1.2.1 (2022-01)

Techniques for assurance of digital material used in legal proceedings

Reference
RTS/CYBER-0079

Keywords
information assurance

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

1 Scope

The present document defines a process of receiving, transforming and outputting material that can be assured digitally. The process is called the "Digital Evidence Bag" (DEB). The present document identifies the ways that a DEB can be used to provide assurance of material used in legal proceedings. Specifically, the assurance of the material is not dependent on the process having been carried out by a qualified or trained human expert.

The present document is designed to be used in situations where a risk assessment of the handling of digital material has identified that extra assurance of the integrity, provenance, continuity and validity of the digital data is required.

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 at https://docbox.etsi.org/Reference/.

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] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[2] ETSI TS 103 307: "CYBER; Security Aspects for LI and RD Interfaces".

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 necessary for the application of the present document.

[i.1] ISO/IEC 17025: "General requirements for the competence of testing and calibration laboratories".

[i.2] Lives and Opinions of Eminent Philosophers, Diogenes Laërtius (c. 225 CE).

[i.3] Navigation and Nautical Astronomy, James Inman (1835).

[i.4] ISO 8601: "Date and time -- Representations for information interchange".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

case-specific input material: input material for a Digital Evidence Bag that is specific to the particular investigation or case

Digital Evidence Bag (DEB): process of storing digital evidence which can be assured digitally

Purely Digital Transformation (PDT): transformation in which a repeatable, deterministic, pre-specified, fail-safe, well-defined digital function is performed on entirely digital data

NOTE: See clause 5.3.1 for more information.

reference input material: relevant material (if any) which is used to support the case-specific input material by adding context or background

3.2 Symbols

Void.

3.3 Abbreviations

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

ADT	Assured Digital Transformation
B-DEB	Basic Digital Evidence Bag
DEB	Digital Evidence Bag
DEB+H	Digital Evidence Bag with Hashing
DEB+HIA	Digital Evidence Bag with Hashing and Input Assurance
DEB+IA	Digital Evidence Bag with Input Assurance
DIPCV	Data Integrity, Provenance, Continuity and Validity
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
PDT	Purely Digital Transformation

4 Basic principles

4.1 Summary

The present document gives a definition for a "Digital Evidence Bag", which is a process for storing and transforming digital material. Annex A provides an informative description of when this process is intended to be used.

The present document defines and specifies requirements for the following types of Digital Evidence Bag:

1) A Basic Digital Evidence Bag (B-DEB) (see clause 5).
2) A Digital Evidence Bag with Hashing (DEB+H) (see clause 6).
3) A Digital Evidence Bag with Input Assurance (DEB+IA) (see clause 6).
4) A Digital Evidence Bag with Hashing and Input Assurance (DEB+HIA) (see clause 6).

Annex F provides recommendations for testing a DEB.

NOTE: A Digital Evidence Bag with Digital Signature would also meet many of the same goals as the Digital Evidence Bag with Hashing and Input Assurance and this is being considered for a future version.

5 Definition of a Basic Digital Evidence Bag

5.1 Reference model

The model for a Basic Digital Evidence Bag is as shown in Figure 1.

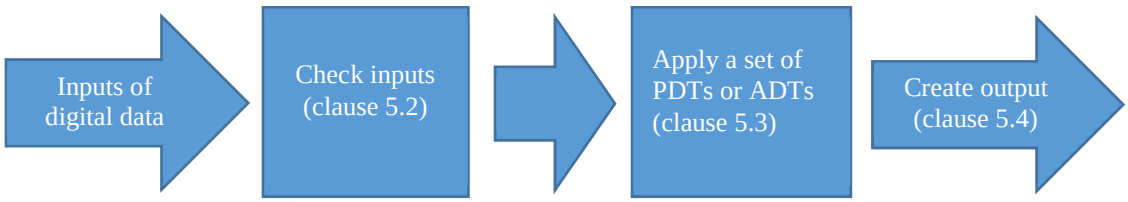

Figure 1: Model for Basic Digital Evidence Bag

5.2 Inputs of digital data

5.2.1 Nature of inputs

There are two types of input material: case-specific input material and reference input material (as defined in clause 3).

EXAMPLE: Examples of reference input material are maps or publicly available reference data.

Basic DEBs shall follow the specifications for input material as listed in clauses 5.2.2 to 5.2.4.

5.2.2 A unique identifier for each input

5.2.2.1 Identifiers for case-specific input material

For a Basic DEB, each input of case-specific input material (see clause 3) shall have a unique identifier attached to it. One of the two following approaches shall be used:

1) The identifier shall consist of:

   a) an identifier supplied by the originating organization; and

   b) a unique identifier for the originating organization. A globally-unique identifier shall be created for the originating organization, using a combination of a nationally-unique identifier together with a country code.

2) The identifier shall be a randomly chosen globally unique identifier as defined in IETF RFC 4122 [1].

Each piece of case-specific input material should include where relevant an identifier of a request that prompted the generation of the input.

5.2.2.2 Identifiers for reference input material

For a Basic DEB, the reference input material (see clause 3) should also have an identifier to make it clear where it came from, and should also identify the time it was collected if that is significantly different from the time the material is being submitted to the DEB.

5.2.3 Time and location information for input material

The time information in a Basic DEB shall consist of the following:

- All time information as supplied by the originating organization. The input material should contain time and date information, including indication of the time zone, for the point at which the data was generated or created (or for the period over which the data was generated).
- DEB Entry Time: A timestamp shall be added to indicate the time and date, including indication of the time zone, the data was received at the Digital Evidence Bag.

In the case that the time of creation is clearly indicated by the originating organization, it shall be checked that the DEB Entry Time is after the time of creation of the material.

The location of collection of information should be included where the point of collection is not necessarily fixed to one place and is relevant to the value of the material collected.

EXAMPLE: A contract has been placed with a laboratory to provide information, and the contract includes a statement of the formats in which the data will be provided.

5.2.4 Format of input material

The format for each input file to a Basic DEB should be known or clear (i.e. known via a communication in advance of sending the data, or clear from the evidence file itself). Each input file should be checked syntactically for data formats where there are suitable automated checks.

EXAMPLE: If data is submitted in XML and the XML schema is known and agreed, then each input file is checked against the schema.

5.3 Applying Purely Digital Transformations and Assured Digital Transformations

5.3.1 Definition of a Purely Digital Transformation

A Purely Digital Transformation (PDT) is one in which a repeatable, deterministic, pre-specified, fail-safe, well-defined digital function is performed on entirely digital data.

Specifically:

- It is repeatable in that if the step is performed again by a different computer or operator, in a different environment, in a different country or at a different time, the outcome is always the same.
- It is deterministic in that the same inputs to the process always give the same outputs, which is not dependent on the training or skill level of an operator.
- It is pre-specified in that the full details of the process are known to all relevant parties in advance and (ideally but not essentially) the details are published.
- It is fail-safe in that its failure modes are easily distinguishable from successful outcomes (in particular, that a failure mode looks very different from a successful output with no records in it).
- It is well-defined in that the version numbering is present and accurate and that the formatting is clear and specified in all places.
- It is digital in that its input and output are digital.

5.3.2 Use of PDT in a Digital Evidence Bag

Within the Digital Evidence Bag, one or more PDTs (as defined in clause 5.3.1) may be applied.

For each transformation, the DEB shall check:

- That the formatting and definition of input files is clear.
- That any standards referred to have a correct version number and are designed for the purpose in question.
- That the input(s) each has an identifier for the material in question.

The DEB shall record:

- The time and date that the transformation took place, ensuring time zone is clear.
- A unique identifier to the output.
- An identification of the process that took place and an identifier to the entity that performed it.

The recommendations in Annex E should be followed when handling the types of data listed in Annex E. Examples of PDT are given in Annex D.

5.3.3 Definition of an Assured Digital Transformation

An Assured Digital Transformation (ADT) is one in which a documented, fail-safe task is performed on entirely digital data by a suitably qualified person.

Specifically:

- The task is documented, in that there is a document listing how the task is to be performed, which was available to the person performing the task and is available to be referenced during legal proceedings. The document lists the inputs required and, where appropriate, the format of each input. The areas that require human judgement or skill are explicitly stated in the documentation. If the task needs suitable facilities, this is stated in the documentation. If the task needs suitable software, this is stated in the documentation.

NOTE 1: The present document does not define what suitable facilities or suitable software are.

NOTE 2: The present document records what was required and what was used so that the court can decide whether it was suitable, perhaps by referring to other standards in this area e.g. ISO/IEC 17025 [i.1].

- The task is fail-safe, in that the documentation lists the common failure modes, showing how failure modes are easily distinguishable from successful outcomes (in particular, that a failure mode looks very different from a successful output with no records in it).
- The task is digital in that its input and output are digital.
- The person is qualified for the task, in that they have suitable recorded experience or qualifications to cover the areas of the task that have been identified as requiring human judgement or skill.

NOTE 3: The present document does not specify what qualifications would count as suitable.

NOTE 4: The purpose of the present document is to define how to create a record of the task that was performed, including details of the person who performed the task including their qualifications. The content of the record can allow a court to establish whether it considered the qualification suitable for the task, perhaps by referring to other standards in this area.

5.3.4 Use of ADT in a Digital Evidence Bag

Within the Digital Evidence Bag, one or more ADTs (as defined in clause 5.3.3) may be applied.

For each transformation, the DEB shall:

- Check formatting of input files is clear (in line with the documentation).
- Check that the input(s) each has an identifier.

The DEB shall record:

- The time and date that the transformation took place, ensuring time zone is clear.
- A unique identifier for the output.
- An identification of the process that took place, giving a link to the documentation that describes the required human judgement, facilities and software (described in clause 5.3.3).
- A unique way to identify the person who performed it. Where possible, this should be done using an identifier for an organization (e.g. the person's employer) together with a unique ID within that organization. This requirement may also be met using a country code plus a unique identifier for a person within a country.
- The qualification of the person who performed, as described in clause 5.3.3. No unrelated qualifications shall be added.
- The location of performing the task, if the task needed suitable facilities (as stated in the documentation).