SLOVENSKI STANDARD
SIST EN 9300-005:2017

01-december-2017

Aeronavtika - LOTAR - Dolgotrajno arhiviranje in iskanje digitalne tehnične dokumentacije o izdelkih, kot so podatki o 3D, CAD in PDM - 005. del: Avtentikacija in overjanje

Aerospace series - LOTAR - LOng Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data - Part 005: Authentication and Verification

Luft- und Raumfahrt - LOTAR - Langzeit-Archivierung und -Bereitstellung digitaler technischer Produktdokumentationen, wie zum Beispiel von 3D-, CAD- und PDM-Daten - Teil 005: Authentifizierung und Verifikation

Série aérospatiale - LOTAR - Archivage long terme et récupération des données techniques produits numériques telles que CAD 3D et PDM - Partie 005 : Authentification et Vérification

Ta slovenski standard je istoveten z: **EN 9300-005:2017**

ICS:

01.110	Tehnična dokumentacija za izdelke	Technical product documentation
35.240.30	Uporabniške rešitve IT v informatiki, dokumentiranju in založništvu	IT applications in information, documentation and publishing
49.020	Letala in vesoljska vozila na splošno	Aircraft and space vehicles in general

SIST EN 9300-005:2017 **en,fr,de**

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 9300-005

October 2017

ICS 01.110; 35.240.30; 35.240.60; 49.020

English Version

Aerospace series - LOTAR - LOng Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data - Part 005: Authentication and Verification

Série aérospatiale - LOTAR - Archivage long terme et récupération des données techniques produits numériques telles que CAD 3D et PDM - Partie 005 : Authentification et Vérification

Luft- und Raumfahrt - LOTAR - Langzeit-Archivierung und -Bereitstellung digitaler technischer Produktdokumentationen, wie zum Beispiel von 3D-, CAD- und PDM-Daten - Teil 005: Authentifizierung und Verifizierung

This European Standard was approved by CEN on 16 July 2017.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 9300-005:2017 E

Contents Page

Figures

European foreword

This document (EN 9300-005:2017) has been prepared by the Aerospace and Defence Industries Association of Europe - Standardization (ASD-STAN).

After enquiries and votes carried out in accordance with the rules of this Association, this Standard has received the approval of the National Associations and the Official Services of the member countries of ASD, prior to its presentation to CEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2018, and conflicting national standards shall be withdrawn at the latest by April 2018.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

EN 9300-005 describes the fundamentals and concepts of authentication and verification of the integrity of digital documents and their content during the archiving and retrieval processes. The Data Domain Parts EN 9300-x00 will specify qualification measures for the content of the document. The fundamentals given in this document cover the requirements, methods and recommendations for their implementation within an archiving system.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 9300 (all parts), *Aerospace series — LOTAR — LOng Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data*

3 Terms, definitions and abbreviations

For the purposes of this standard, the terms, definitions and abbreviations given in EN 9300-003 and EN 9300-007 shall apply.

3.1
authentication
authentication has to prove:

- the *originality* and *integrity* of a document and its contents;

- the identity of a user.

Authentication of an electronic document establishes that the content is unchanged from to the original information. Information is *original* if it is demonstrable that the information belongs to the supposed author.

Authentication may depend upon one or more authentication factors.

Unlike verification and validation, authentication makes no statement about the quality of data in terms of usability in the archiving process chain of e.g. conversion or reuse.

3.2
asymmetric keys
asymmetric keys are pairs of keys, created in one step; they can be used in both directions. Encryption with the public key can only be decrypted with the private key; if the encryption is done with the private key, the decryption can only done with the public key; such a key pair can be used for encryption and for signing

3.2.1
public key
public key is the part of the asymmetric key pair that is known to everyone

3.2.2
private key
private key is the part of the asymmetric key pair that is only known by the owner of the asymmetric key pair

3.3
electronic document
digital representation of a defined and structured amount of information which can be managed as a unit and be exchanged between users and systems; each revision of a given document is a new electronic document

[Copied and modified from ISO-IEC 82045]

3.4
electronic signatures
electronic signature is a defined method to sign an object in electronic environments; it provides means to authenticate the signatory and the signed object in an unambiguous and safe way by attaching to or logically associating data in electronic form to other electronic objects

In EN 9300 it is defined by an encrypted hash code with additional information such as time of creation and owner of the signature.

ASD-STAN LOTAR distinguishes between:

- engineering signature;
- time signature.

In the context of the EN 9300, an electronic signature shall be:

- uniquely linked to the signatory;
- capable of identifying the signatory;
- created using means that the signatory can maintain:
  - under their sole control.
- linked to the data to which it relates in such a manner that:
  - any subsequent change of the data is detectable.

Note 1 to entry: This definition complies with that given by:

- Directive in 1999/93/EC of the European parliament and the council from the 13th of December, 1999 concerning collective basic conditions of electronic signatures.

3.4.1
engineering signature
engineering signature expresses and fixes a volition of the signatory it gives evidence of:

- the process of testifying quality of data against process / quality requirements by linking the signature owner to the data;
- the identity of the signatory by usage of appropriate methods of authentication;

- the integrity of the data by using appropriate methods protecting the signed object against unauthorized changes.

3.4.2
time signature
time signature is created automatically as part of a certified process and requires certified hardware; it provides a legal guarantee for time and owner of the data

3.5
hash code
hash code is represented by a number calculated by a One-Way-Hash function. It represents the electronic document in a unique way

3.6
signer
signer is an entity that initially creates the electronic signature; when the signer digitally signs data using the prescribed format, this represents a commitment on behalf of the signing entity about the data being signed

3.7
verifier
verifier is an entity that verifies evidence (ISO/IEC 13888-1); within the context of this document this is an entity that validates an electronic signature

3.8
trust center
trust center is one or more entities that help to build trust relationships between the signer and verifier; use of some specific technical service provider (TSP) services MAY be mandated by signature policy. TSP supporting services may provide the following information: user certificates, cross-certificates, time-stamping tokens.

3.9
verification levels
in the context of EN 9300 Verification Levels indicate a risk assessment; verification levels here will indicate the maximum acceptable risk for a specific process

4 Applicability

Refer to applicability of EN 9300-001, clause 4.

5 Authentication

The necessity of authentication and verification of digital information results from the legal requirement of ensuring the authenticity (*originality* and *integrity*) of stored data.

5.1 Authentication of User

The authentication of the user is necessary to ensure only authorised persons initiate controlled processes.

The legal status of an engineering signature will be enhanced by means of authentication.

5.1.1 Authentication by means of a PKI (Public Key Infrastructure)

The application of a PKI is recommended to guarantee the quality of an engineering signature.

Advantage:

- delivers a higher evidential value.

Disadvantages:

- the need to provide an Infrastructure (PKI) with key ring administration;
- each release of a document creates electronic signatures with metadata to manage.

NOTE Currently there are different national laws and/or standards defining different security levels for PKI. By applying these levels different legal qualities for documents can be obtained.

5.1.2 Authentication by User Key and Password

EN 9300 recommends authentication policies based on current business practices for user keys and passwords as the initial user authentication quality level.

Advantages:

- legal recommendations for documentation of the release process are fulfilled;
- there is no need for a PKI and no additional hardware for identification is required.

Disadvantage:

- the validity in the context of lawsuits is less than under PKI.

5.2 Authentication of Document and Content

Applying authentication to a document and its content will improve its evidential weight in the context of legal proceedings. The authenticity of a digital document can be proved with the document hash code. In case of a change of content, a new electronic document must be created and authenticated.

5.2.1 Requirements to Hash Codes

For signing and verification a hash code will be used like a digital finger print. To ensure that no security gaps occur, the hash code must fulfil the following criteria:

- *it should practically be impossible to find a collision* (where two or more different digital documents generate an identical hash code);
- *creating hash codes shall be an one way function.* It should not be possible to find a file that generates a given hash code.

NOTE From a theoretical point of view collisions are inevitable.

5.2.2 Usable Hash Functions

It is recommended that the practice applied has the highest security level. Its validity depends on the technical development in hardware, cryptography and networking. It is also recommended that hash codes have the maximum lifetime, in order to avoided renewing the hash code after a short period.

NOTE 1 See, for example, the recommendations of the German Federal Network Agency (for Electricity, Gas, Telecommunications, Post and Railway) in 2006

NOTE 2 Analysis of hash functions indicates that the following 160 bit functions may be considered as secure up to the end of 2009:

- RIPEMD-160;
- SHA-1.

NOTE 3 The following hash functions with different hash code length (SHA-224 is a 224-bit hash function etc.) are expected to be secure for Long Term Archiving:

- SHA-224, SHA-256, SHA-384, SHA-512 [2]; FIPS PUB 180-3 "Secure Hash Standard (SHS)".

The actual permission has to be renewed in accordance to the highest applicable requirements in a defined and appropriate time frame. See figure below.

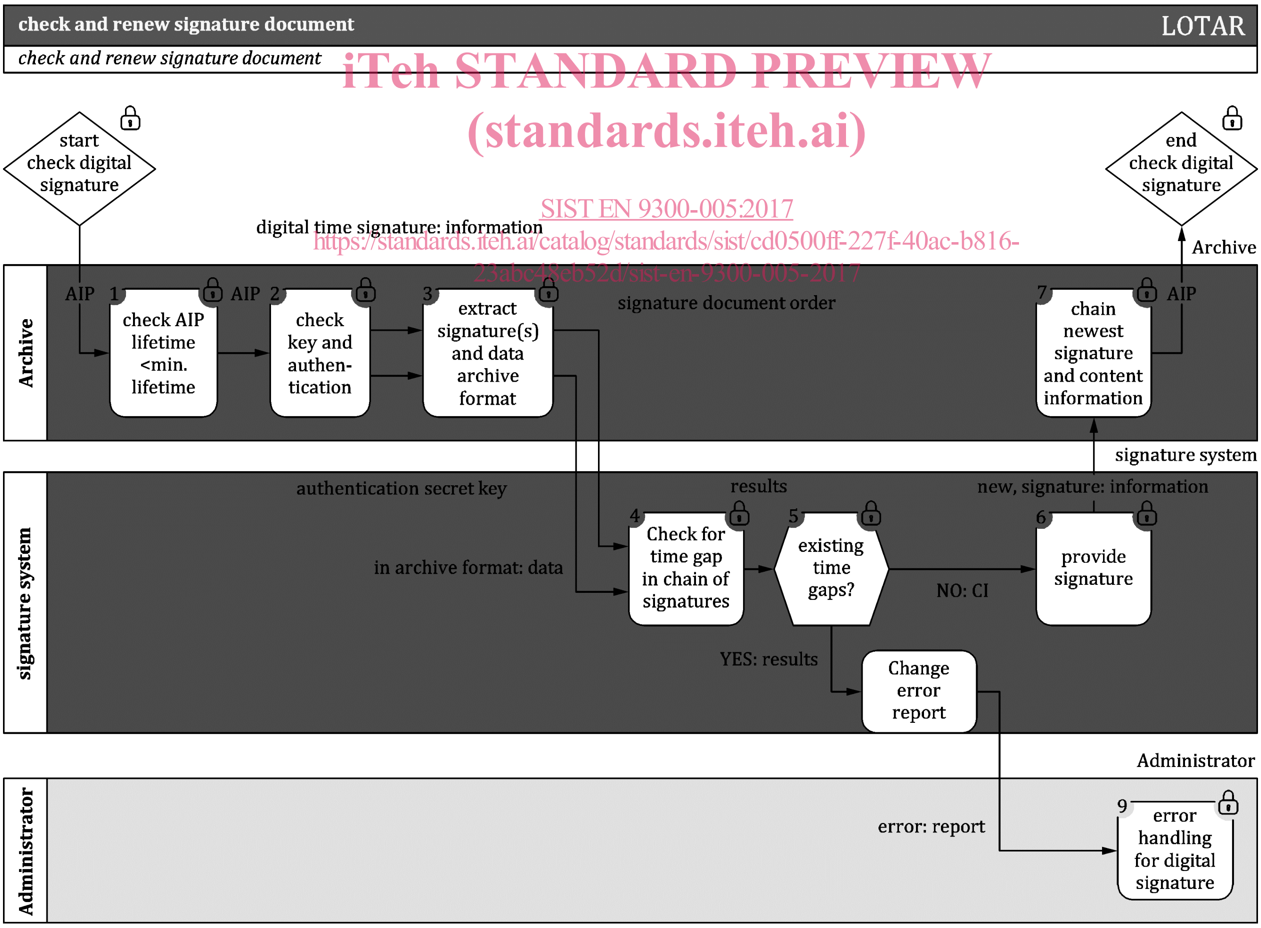
check and renew signature document
LOTAR
check and renew signature document
start check digital signature
end check digital signature
digital time signature: information
Archive
Archive
AIP
1
check AIP lifetime <min. lifetime
AIP
2
check key and authen-tication
3
extract signature(s) and data archive format
signature document order
7
chain newest signature and content information
AIP
signature system
signature system
authentication secret key
results
new, signature: information
4
Check for time gap in chain of signatures
5
existing time gaps?
6
provide signature
in archive format: data
NO: CI
YES: results
Change error report
Administrator
Administrator
error: report
9
error handling for digital signature

Figure 1 — Check and renew signature document

6 Qualification methods

Qualification methods provide procedures to indicate the quality of processes, data and or information within the LOTAR framework.

Two basic procedures are given:

— verification;

— validation;

— the result of verification and validation shall be kept in the system as status information. The result will distinguish between “passed”, “failed” or “not performed”. “Not performed” means that there is no result created in the verification or validation process.

6.1 Verification

A verification of authenticity judges information against rules for legal admissibility, preferably those defined in standards or laws.

Verification of the consistency of the information shall be applied throughout the throughout the Long Term Archiving (LTA) process. The initial verification takes place during the data preparation process. In case of data conversion, the verification is executed on the converted data. The EN 9300 introduces the verification of information on different levels.

A verification of processes should guarantee that all parts of the process finished without errors. If required, the results of the process should be stored and archived into a process protocol (log file).

The objectives of Verification in the LOTAR context are:

— managing the risk of loss of information after a period of LTA;

— re-interpretable information based on a stable data format;

— avoiding efforts of quality control and corrective methods (e.g. repair) in following processes of the archive chain.

6.1.1 Specification of Verification Levels

In order to manage the risk of data or information loss during the LTA, LOTAR introduces a concept of verification levels. These levels are:

Verification Level	Method	Risk
0	No rules applied	Maximum
1	Mandatory rules	Calculated risk
2	Mandatory plus optional rules	Minimized risk

The rules and their categorization into “mandatory” and “optional” will be given within the Data Domain Specific Parts of LOTAR.