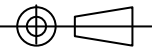


NAS9300-005

Long Term Archiving and Retrieval
of digital technical product documentation
such as 3D, CAD and PDM data

PART 005: Authentication and Verification

THIRD ANGLE PROJECTION 	CUSTODIAN ENGINEERING MANAGEMENT COMMITTEE	REVISION NEW
PROCUREMENT SPECIFICATION NONE	TITLE LONG TERM ARCHIVING AND RETRIEVAL OF DIGITAL TECHNICAL PRODUCT DOCUMENTATION SUCH AS 3D, CAD AND PDM DATA PART 005: AUTHENTICATION AND VERIFICATION	CLASSIFICATION STANDARD PRACTICE NAS9300-005 SHEET 1 OF 17

FOREWORD

1. This standard was prepared jointly by AIA, ASD-STAN, PDES Inc and the PROSTEP iViP Association.
2. The PROSTEP iViP Association is an international non-profit association in Europe. For establishing leadership in IT-based engineering it offers a moderated platform to its nearly 200 members from leading industries, system vendors and research institutions. Its product and process data standardization activities at European and worldwide levels are well known and accepted. The PROSTEP iViP Association sees this standard and the related parts as a milestone of product data technology.
3. PDES Inc is an international non-profit association in USA. The mission of PDES Inc is to accelerate the development and implementation of ISO 10303, enabling enterprise integration and PLM interoperability for member companies. PDES Inc gathers members from leading manufacturers, national government agencies, PLM vendors and research organizations. PDES Inc. supports this standard as an industry resource to sustain the interoperability of digital product information, ensuring and maintaining authentic longevity throughout their product lifecycle.
4. Readers of this standard should note that all standards undergo periodic revisions and that any reference made herein to any other standard implies its latest edition, unless otherwise stated.
5. The Standards will be published under two different standards organizations using different prefixes. ASD-STAN will publish the standard under the number EN9300-xxx. AIA will publish the standard under the number NAS9300-xxx. The content in the EN9300 and NAS9300 documents will be the same. The differences will be noted in the reference documentation (i.e. for EN9300 Geometric Dimensioning & Tolerancing will be referenced in ISO 1101 and ISO 16792, and for NAS9300 the same information will be referenced in ASME Y14.5M and Y 14.41). The document formatting etc., will follow that of the respective editorial rules of ASD-STAN and AIA.

REVISION

NEW

NAS9300-005

SHEET 2



Documents

Document Sharing Hub

USE OF OR RELIANCE UPON THIS DOCUMENT OR ANY NATIONAL AEROSPACE STANDARD IS ENTIRELY VOLUNTARY. AIA DOES NOT QUALIFY SUPPLIERS OR CERTIFY

Copyright Aerospace Industries Association of America Inc. ALL RIGHTS RESERVED. AIA MAKES NO REPRESENTATION OR CLAIM RESPECTING (1) THE SUITABILITY OF
Provided by IHS under license with AIA/NAS. ANY PARTICULAR APPLICATION OR (2) THE EXISTENCE OF OR APPLICABLE LAWS, REGULATIONS, ORDINANCES, DECREES, OR OTHER LEGISLATION.
No reproduction or networking permitted without license from IHS. Licensee= www.sepana.ir/5991803002, User=sam, albert
Not for Resale, 01/04/2016 11:32:00 MST TRADEMARKS RIGHTS.

CONTENTS

1	Scope	4
2	Normative references	4
3	Terms, definitions and abbreviations	4
3.1	Authentication.....	4
3.2	Asymmetric keys	4
3.3	Electronic document	4
3.4	Electronic signatures	4
3.5	Hash code	5
3.6	Signer	5
3.7	Verifier	5
3.8	Trust center	5
3.9	Verification levels	6
4	Applicability	6
5	Authentication	6
5.1	Authentication of user	6
5.2	Authentication of document and content	6
6	Qualification methods.....	8
6.1	Verification	8
6.2	Validation	8
6.3	Error handling.....	9
7	Electronic signature.....	11
7.1	Engineering signature.....	11
7.2	Time signature.....	11
7.3	Target for applying electronic signatures	11
7.4	Creation and check of electronic signatures	12

FIGURES

Figure 1 – Check and renew signature document	7
Figure 2 – Concept of repair in data preparation / ingest process and retrieval process	10
Figure 3 – Creation and check of electronic signatures	12
Figure 4 – Validity of electronic signatures	13
Figure 5 – Verification period of electronic signatures	14

ANNEXES

ANNEX A – Use cases and recommended solutions for issues of authentication and verification	15
ANNEX B – Bibliography	17

REVISION

NEW

NAS9300-005

SHEET 3



Documents

Document Sharing Hub

1 Scope

NAS9300-005 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 NAS9300-xxx 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 Standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

NAS9300 Aerospace series – LOTAR – Long Term Archiving and Retrieval of digital technical and product documentation such as 3D CAD and PDM data. Other parts are applicable as required.

3 Terms, definitions and abbreviations

For the purpose of this standard, the terms, definitions and abbreviations given in NAS9300 – 003 and 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

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

3.2.2 Private key

The 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

An electronic document is a 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.

3.4 Electronic signatures

An electronic signature is a defined method to singe 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.

REVISION

NEW

NAS9300-005

SHEET 4



Documents

Document Sharing Hub

In NAS9300 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 NAS9300, 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: This definition complies with that given by:

- US Electronic Signatures in Global and National Commerce Act (ESIGN) Pub Law 106-229 2000-06-30
- US Government Paperwork Elimination Act (GPEA) Pub Law 105-277 1999-10-21
- 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

The engineering signature expresses and fixes 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

The engineering signature can be fixed using different methods. Within NAS9300 the recommended method is usage of methods of electronic signatures.

3.4.2 Time signature

A 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

A 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

A 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

A verifier is an entity that verifies evidence. Within the context of this document this is an entity that validates an electronic signature.

3.8 Trust center

A 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.

REVISION

NEW

NAS9300-005

SHEET 5

3.9 Verification levels

In the context of NAS9300 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 NAS9300-001, paragraph 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 authorized 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

NAS9300 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 fulfill 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 possible to find a file that generates a given hash code.

Note: From a theoretical point of view collisions are inevitable.

REVISION

NEW

NAS9300-005

SHEET 6



Documents

Document Sharing Hub