



ICS:

Descriptors:

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
Langzeitarchivierung und Bereitstellung
digitaler technischer Produktdokumentationen,
beispielsweise 3D CAD und PDM Daten
Teil 005: Authentifizierung und Verifikation**

This "Aerospace Series" Prestandard has been drawn up under the responsibility of ASD-STAN (The AeroSpace and Defence Industries Association of Europe - Standardization). It is published for the needs of the European Aerospace Industry. It has been technically approved by the experts of the concerned Domain following member comments.

Subsequent to the publication of this Prestandard, the technical content shall not be changed to an extent that interchangeability is affected, physically or functionally, without re-identification of the standard.

After examination and review by users and formal agreement of ASD-STAN, it will be submitted as a draft European Standard (prEN) to CEN (European Committee for Standardization) for formal vote and transformation to full European Standard (EN).

The CEN national members have then to implement the EN at national level by giving the EN the status of a national standard and by withdrawing any national standards conflicting with the EN.

Edition approved for publication

30 April 2012

Comments should be sent within six months
after the date of publication to
ASD-STAN

**Engineering Procedures and
Processes Domain**

Contents

Page

Foreword	2
1 Scope	5
2 Normative references	5
3 Terms, definitions and abbreviations.....	5
3.1 Authentication	5
3.2 Asymmetric keys	5
3.2.1 Public key	5
3.2.2 Private key.....	5
3.3 Electronic document	6
3.4 Electronic signatures	6
3.4.1 Engineering Signature	6
3.4.2 Time Signature.....	6
3.5 Hash Code	7
3.6 Signer.....	7
3.7 Verifier	7
3.8 Trust Center	7
3.9 Verification levels	7
4 Applicability	7
5 Authentication	7
5.1 Authentication of User	7
5.1.1 Authentication by means of a PKI (Public Key Infrastructure).....	7
5.1.2 Authentication by User Key and Password	8
5.2 Authentication of Document and Content	8
5.2.1 Requirements to Hash Codes	8
5.2.2 Usable Hash Functions.....	8
6 Qualification methods.....	9
6.1 Verification	9
6.1.1 Specification of Verification Levels	10
6.2 Validation.....	10
6.2.1 Validation Properties.....	10
6.2.2 Specification of Validation Levels	11
6.3 Error Handling	11
6.3.1 Repair of data.....	11
7 Electronic signature	12

7.1	Engineering Signature	12
7.2	Time Signature	13
7.3	Target for Applying Electronic Signatures	13
7.4	Creation and check of electronic signatures	13
7.4.1	Validity of electronic signatures	14
Annex A (informative) Use cases and recommended solutions for issues of authentication and verification		16
Bibliography		18

Figures

Page

Figure 1 — Check and renew signature document	9
Figure 2 — Concept of repair in data preparation / ingest process and retrieval process	12
Figure 3 — Creation and check of electronic signatures	13
Figure 4 — Validity of electronic signatures	14
Figure 5 — Verification period of electronic signatures	15