

DIN EN 9300-005



ICS 01.110; 35.240.30; 35.240.60; 49.020

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; Deutsche und Englische Fassung EN 9300-005:2017**

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;
German and English version EN 9300-005:2017

Série aérospatiale –

LOTAR –

Archivage long terme et récupération des données techniques produits numériques telles que CAD 3D et PDM – Partie 005: Authentification et Vérification;
Version allemande et anglaise EN 9300-005:2017

Gesamtumfang 38 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Der Verband der Europäischen Luft-, Raumfahrt- und Verteidigungsindustrie — Normung (ASD-STAN) ist vom Europäischen Komitee für Normung (CEN) für zuständig erklärt worden, Europäische Normen (EN) für das Gebiet der Luft- und Raumfahrt auszuarbeiten. Durch die Vereinbarung vom 3. Oktober 1986 wurde ASD Assoziierte Organisation (ASB) des CEN.

Das vorliegende Dokument (EN 9300-005:2017) wurde von ASD-STAN, Fachbereich Allgemein, veröffentlicht.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-05-01 AA „Grundlagen und Managementverfahren“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Entsprechend Beschluss 57/9 des Technischen Ausschusses des Beirats des DIN-Normenausschusses Luft- und Raumfahrt (NL) sind die europäischen Luft- und Raumfahrt-Normungsergebnisse zweisprachig, in Deutsch und Englisch, in das Deutsche Normenwerk zu überführen. Aus diesem Grund wurde der Deutschen Fassung dieses Dokumentes die Englische Fassung hinzugefügt.

Deutsche Fassung

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

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

Diese Europäische Norm wurde vom CEN am 16. Juli 2017 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Europäisches Vorwort	3
1 Anwendungsbereich	4
2 Normative Verweisungen	4
3 Begriffe und Abkürzungen	4
4 Anwendbarkeit	6
5 Authentifizierung	6
5.1 Authentifizierung des Nutzers	6
5.1.1 Authentifizierung mittels einer Infrastruktur mit öffentlichem Schlüssel (PKI, en: Public Key Infrastructure)	7
5.1.2 Authentifizierung durch Nutzerschlüssel und Passwort	7
5.2 Authentifizierung von Dokument und Inhalt	7
5.2.1 Anforderungen an Hash-Codes	7
5.2.2 Nutzbare Hash-Funktionen	8
6 Qualifikationsverfahren	9
6.1 Verifizierung	9
6.1.1 Spezifikation für Verifizierungsstufen	9
6.2 Validierung	10
6.2.1 Validierungseigenschaften	10
6.2.2 Spezifikation für Validierungsstufen	10
6.3 Fehlerbehandlung	11
6.3.1 Reparatur von Daten	11
7 Elektronische Signatur	12
7.1 Engineering-Signatur	12
7.2 Zeitsignatur	13
7.3 Ziel zur Anwendung elektronischer Signaturen	13
7.4 Erstellung und Prüfung elektronischer Signaturen	14
7.4.1 Gültigkeit elektronischer Signaturen	14
Anhang A (informativ) Anwendungsfälle und empfohlene Lösungen bei Problemen mit Authentifizierung und Verifizierung	16
Literaturhinweise	18
 Bilder	
Bild 1 — Signaturdokument prüfen und erneuern	8
Bild 2 — Konzept zur Reparatur im Datenvorbereitungs-/Aufnahmeprozess und im Bereitstellungsprozess	12
Bild 3 — Erstellung und Prüfung elektronischer Signaturen	14
Bild 4 — Gültigkeit elektronischer Signaturen	15
Bild 5 — Verifizierungszeitraum elektronischer Signaturen	15

Europäisches Vorwort

Dieses Dokument (EN 9300-005:2017) wurde vom Verband der Europäischen Luft-, Raumfahrt- und Verteidigungsindustrie – Normung (ASD-STAN) erstellt.

Nachdem Umfragen und Abstimmungen entsprechend den Regeln dieses Verbandes durchgeführt wurden, hat diese Norm die Zustimmung der nationalen Verbände und offiziellen Behörden der Mitgliedsländer der ASD erhalten, bevor sie CEN vorgelegt wurde.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2018, und etwaige entgegenstehende nationale Normen müssen bis April 2018 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

1 Anwendungsbereich

In EN 9300-005 werden die Grundlagen und Konzepte der Authentifizierung und Verifizierung der Integrität digitaler Dokumente und ihrer Inhalte während der Archivierungs- und Bereitstellungsprozesse beschrieben. Die datentypspezifischen Teile EN 9300-x00 enthalten Vorgaben für Qualifikationsmaßnahmen für den Inhalt des Dokuments. Die in diesem Dokument vermittelten Grundlagen decken Anforderungen, Verfahren und Empfehlungen für deren Umsetzung innerhalb eines Archivierungssystems ab.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 9300 (alle Teile), *Luft- und Raumfahrt — LOTAR — Langzeit-Archivierung und -Bereitstellung digitaler technischer Produktdokumentationen, wie zum Beispiel von 3D-, CAD- und PDM-Daten*

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe und Abkürzungen nach EN 9300-003 und EN 9300-007 und die folgenden Begriffe.

3.1

Authentifizierung

Authentifizierung muss Folgendes nachweisen:

- die *Echtheit* und *Integrität* eines Dokuments und seiner Inhalte;
- die Identität eines Nutzers.

Durch die Authentifizierung eines elektronischen Dokuments wird festgestellt, dass der Inhalt gegenüber den Originalinformationen unverändert ist. Informationen gelten als *echt*, wenn nachweisbar ist, dass die Information dem angeblichen Autor zugeordnet werden kann.

Die Authentifizierung kann von einem oder mehreren Authentifizierungsfaktoren abhängen.

Anders als bei Verifizierung und Validierung wird bei einer Authentifizierung keine Aussage über die Qualität der Daten in Bezug auf die Gebrauchstauglichkeit bei z. B. Konvertierung oder Wiederverwendung in der Prozesskette der Archivierung getroffen.

3.2

asymmetrischer Schlüssel

in einem einzigen Schritt erstelltes Schlüsselpaar; sie können in beide Richtungen verwendet werden. Mit dem öffentlichen Schlüssel vorgenommene Verschlüsselung kann nur mit dem privaten Schlüssel wieder entschlüsselt werden; wird die Verschlüsselung mit dem privaten Schlüssel vorgenommen, so kann die Entschlüsselung nur mit dem öffentlichen Schlüssel erfolgen; ein solches Schlüsselpaar kann für Verschlüsselung und zur Unterzeichnung verwendet werden

3.2.1

öffentlicher Schlüssel

in der Öffentlichkeit bekannter Teil des asymmetrischen Schlüsselpaars

3.2.2**privater Schlüssel**

Teil des asymmetrischen Schlüsselpaars, der nur dem Eigentümer des asymmetrischen Schlüsselpaars bekannt ist

3.3**elektronisches Dokument**

digitale Darstellung einer festgelegten und strukturierten Menge von Informationen, die als Einheit verwaltet und zwischen Anwendern und Systemen ausgetauscht werden kann; jede Überarbeitung eines Dokuments ist ein neues elektronisches Dokument

[Übernommen und modifiziert von ISO-IEC 82045]

3.4**elektronische Signatur**

definiertes Verfahren zur Unterzeichnung eines Objekts in elektronischen Umgebungen; sie bietet Mittel zur Authentifizierung des Unterzeichners und des unterzeichneten Objekts auf eindeutige und sichere Weise durch Beifügung von Daten in elektronischer Form an oder durch logische Zuordnung zu anderen elektronischen Objekten

In EN 9300 ist sie definiert als ein verschlüsselter Hash-Code mit zusätzlichen Informationen, wie der Zeit der Erstellung und dem Eigentümer der Signatur.

ASD-STAN LOTAR unterscheidet zwischen:

- Engineering-Signatur;
- Zeitsignatur.

Im Kontext von EN 9300 muss eine elektronische Signatur:

- ausschließlich dem Unterzeichner zugeordnet sein;
- in der Lage sein, den Unterzeichner zu identifizieren;
- durch Mittel erstellt worden sein, die der Unterzeichner aufrechterhalten kann:
 - unter seiner alleinigen Kontrolle.
- so mit den Daten verknüpft sein, auf die sie sich bezieht, dass
 - jede nachfolgende Änderung der Daten erkannt werden kann.

Anmerkung 1 zum Begriff: Diese Definition deckt sich mit der Definition, die von:

- der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vorgegeben wird.

3.4.1**Engineering-Signatur**

die Engineering-Signatur drückt eine Absicht des Unterzeichners aus und fixiert diese; sie gilt als Nachweis für Folgendes:

- den Prozess der Bezeugung der Qualität von Daten gegenüber Prozess-/Qualitätsanforderungen durch Verknüpfung des Eigentümers der Signatur mit den Daten;

- die Identität des Unterzeichners durch Verwendung der angemessenen Authentifizierungsverfahren;
- die Integrität der Daten durch Verwendung der angemessenen Verfahren, die das unterzeichnete Objekt vor unautorisierten Änderungen schützen.

3.4.2

Zeitsignatur

eine Zeitsignatur wird automatisch als Teil eines zertifizierten Prozesses erstellt und erfordert zertifizierte Hardware; sie bietet eine rechtskräftige Garantie von Zeit und Eigentümer der Daten

3.5

Hash-Code

Zahl, die mittels einer Einweg-Hash-Funktion errechnet wurde; sie repräsentiert das elektronische Dokument auf eine eindeutige Weise

3.6

Unterzeichner

Instanz, die zuerst eine elektronische Signatur erstellt; wenn der Unterzeichner Daten mit dem vorgeschriebenen Format digital unterzeichnet, stellt dies eine Verpflichtung seitens der unterzeichnenden Instanz auf die unterzeichneten Daten dar

3.7

Verifizierer

Instanz, die einen Nachweis verifiziert (ISO/IEC 13888-1); im Kontext dieses Dokuments ist das eine Instanz, die eine elektronische Signatur validiert

3.8

Trust-Center

Instanz /en, die dazu beiträgt / beitragen, ein Vertrauensverhältnis zwischen Unterzeichner und Verifizierer aufzubauen; die Nutzung einiger spezifischer Leistungen technischer Dienstanbieter (TSP, en: Technical Service Provider) DARF von der Signaturpolitik vorgeschrieben werden. Die unterstützenden Dienste von TSP können die folgenden Informationen liefern: Nutzerzertifikate, Cross-Zertifikate, Zeitstempel-Tokens

3.9

Verifizierungsstufe

im Kontext von EN 9300 zeigen Verifizierungsstufen eine Risikoanalyse an; hier zeigen Verifizierungsstufen das zulässige Höchstisiko für einen spezifischen Prozess an

4 Anwendbarkeit

Siehe Anwendbarkeit in EN 9300-001, 4.

5 Authentifizierung

Die Notwendigkeit von Authentifizierung und Verifizierung digitaler Informationen ergibt sich aus der rechtlichen Anforderung, die Authentizität (*Echtheit* und *Integrität*) gespeicherter Daten sicherzustellen.

5.1 Authentifizierung des Nutzers

Die Authentifizierung des Nutzers ist erforderlich, um sicherzustellen, dass nur autorisierte Personen kontrollierte Prozesse einleiten.

Der rechtliche Status einer Engineering-Signatur wird durch Mittel der Authentifizierung erweitert.

5.1.1 Authentifizierung mittels einer Infrastruktur mit öffentlichem Schlüssel (PKI, en: Public Key Infrastructure)

Die Anwendung einer PKI wird empfohlen, um die Qualität einer Engineering-Signatur zu garantieren.

Vorteil:

- bietet höheren Beweiswert.

Nachteile:

- Erfordernis der Erstellung einer Infrastruktur (PKI) mit Schlüsselbundverwaltung;
- jedes Release eines Dokuments erstellt elektronische Signaturen mit zu steuernden Metadaten.

ANMERKUNG Aktuell bestehen unterschiedliche nationale Gesetze und/oder Normen, die unterschiedliche Sicherheitsstufen für PKI definieren. Durch Anwendung dieser Stufen können sich unterschiedliche rechtliche Eigenschaften von Dokumenten ergeben.

5.1.2 Authentifizierung durch Nutzerschlüssel und Passwort

EN 9300 empfiehlt Authentifizierungsrichtlinien basierend auf aktuellen Geschäftspraktiken für Nutzerschlüssel und -passwörter als anfängliche Qualitätsstufe für die Nutzerauthentifizierung.

Vorteile:

- gesetzliche Empfehlungen für die Dokumentation der Release-Prozesse werden erfüllt;
- kein Bedarf für eine PKI; zusätzliche Hardware für die Identifikation ist nicht erforderlich.

Nachteil:

- die Validität im Kontext von Gerichtsverfahren ist geringer als mit PKI.

5.2 Authentifizierung von Dokument und Inhalt

Die Anwendung einer Authentifizierung auf ein Dokument und seinen Inhalt verbessert dessen Beweiskraft in Rechtsverfahren. Die Authentifizierung eines digitalen Dokuments kann mittels des Hash-Codes des Dokuments nachgewiesen werden. Wenn der Inhalt verändert wurde, muss ein neues elektronisches Dokument erstellt und authentifiziert werden.

5.2.1 Anforderungen an Hash-Codes

Zur Unterzeichnung und Verifizierung wird ein Hash-Code als digitaler Fingerabdruck verwendet. Um Sicherheitslücken auszuschließen, muss der Hash-Code die folgenden Kriterien erfüllen:

- *es sollte praktisch unmöglich sein, eine Kollision zu finden* (bei der zwei oder mehr digitale Dokumente einen identischen Hash-Code generieren);
- *die Generierung eines Hash-Code muss eine Einweg-Funktion sein*. Es sollte nicht möglich sein, eine Datei zu finden, die einen vorhandenen Hash-Code generiert.

ANMERKUNG Aus theoretischer Sicht sind Kollisionen unvermeidbar.

5.2.2 Nutzbare Hash-Funktionen

Es wird empfohlen, dass die angewendete Praxis die höchste Sicherheitsstufe aufweist. Ihre Validität ist abhängig von der technischen Entwicklung in Bezug auf Hardware, Kryptographie und Netzwerke. Zudem wird empfohlen, Hash-Codes die maximale Lebensdauer zu geben, damit der Hash-Code nicht nach einem kurzen Zeitraum bereits erneuert werden muss.

ANMERKUNG 1 Siehe beispielsweise die Empfehlungen der Bundesnetzagentur (für Strom, Gas, Telekommunikation, Post und Eisenbahnen) aus dem Jahr 2006.

ANMERKUNG 2 Eine Analyse von Hash-Funktionen zeigt, dass die folgenden 160-bit-Funktionen bis Ende 2009 als sicher angesehen werden dürfen:

- RIPEMD-160;
- SHA-1.

ANMERKUNG 3 Die folgenden Hash-Funktionen mit unterschiedlicher Hash-Code-Länge (SHA-224 ist eine 224-bit-Hash-Funktion usw.) sind voraussichtlich für die Langzeitarchivierung sicher:

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

Die eigentliche Zulassung muss nach den höchsten anwendbaren Anforderungen innerhalb eines festgelegten und angemessenen Zeitrahmens erneuert werden. Siehe Bild unten.

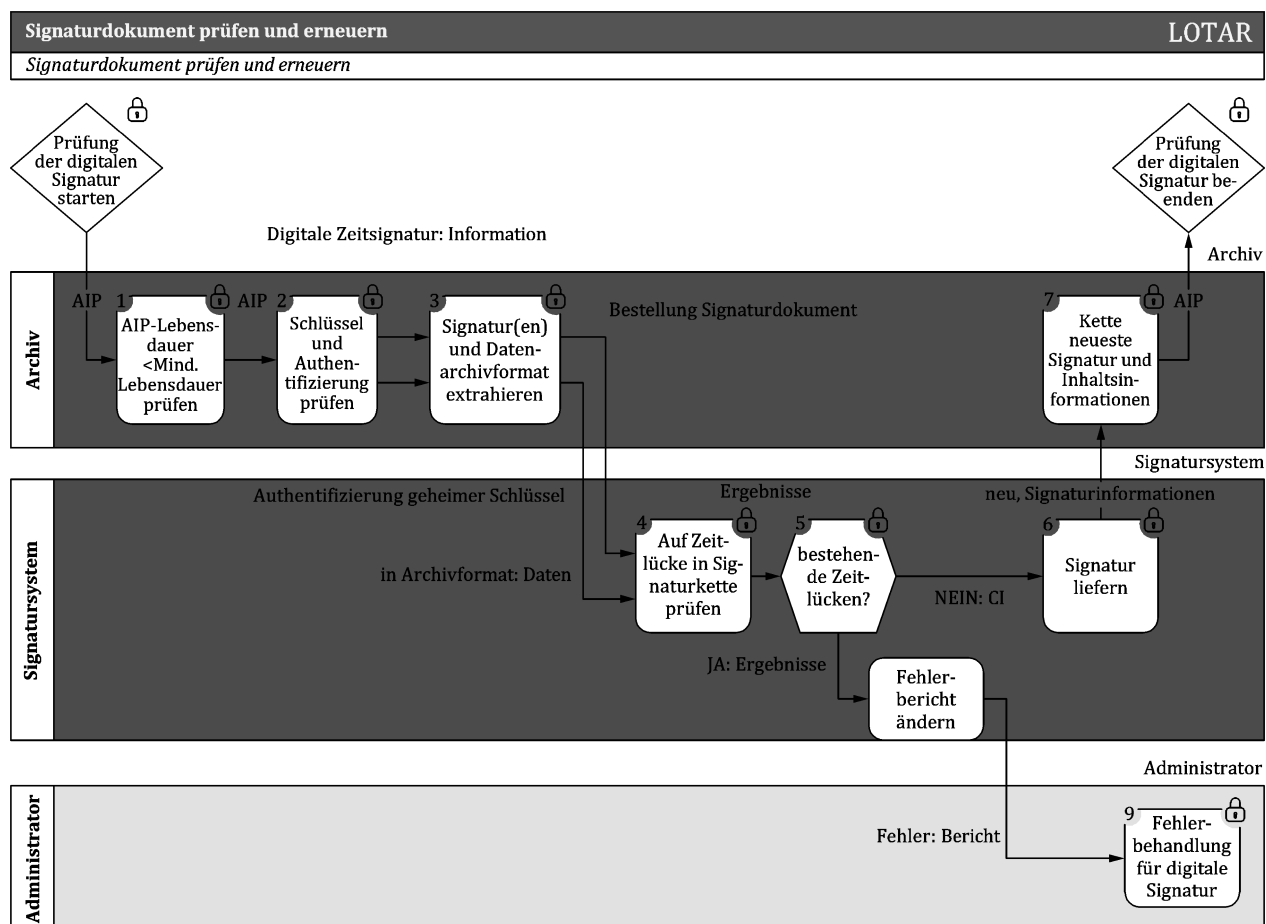


Bild 1 — Signaturdokument prüfen und erneuern

6 Qualifikationsverfahren

Qualifikationsverfahren bieten Verfahren zur Angabe der Qualität von Prozessen, Daten und/oder Informationen innerhalb des Rahmens von LOTAR.

Es werden zwei grundlegende Verfahren gegeben:

- Verifizierung;
- Validierung;
- das Ergebnis von Verifizierung und Validierung ist als Statusinformation im System zu halten. Das Ergebnis unterscheidet zwischen „bestanden“, „nicht bestanden“ und „nicht durchgeführt“. „Nicht durchgeführt“ bedeutet, dass im Verifizierungs- oder Validierungsprozess kein Ergebnis erstellt wurde.

6.1 Verifizierung

Eine Verifizierung der Authentizität bewertet Informationen gegenüber Regeln zur rechtlichen Zulässigkeit, vorzugsweise solchen, die durch Normen oder Gesetze definiert sind.

Die Verifizierung der Konsistenz von Informationen ist den Prozess der Langzeitarchivierung (LTA, en: Long-Term Archiving) hindurch anzuwenden. Die Erstverifizierung findet während des Prozesses der Datenvorbereitung statt. Im Falle einer Datenkonvertierung wird die Verifizierung an den konvertierten Daten durchgeführt. EN 9300 führt die Verifizierung von Informationen auf verschiedenen Stufen ein.

Eine Verifizierung von Prozessen sollte gewährleisten, dass alle Teile des Prozesses ohne Fehler abschließen. Falls erforderlich, sollten die Ergebnisse des Prozesses in einem Prozessprotokoll gespeichert und archiviert werden (Logdatei).

Die Ziele der Verifizierung im Kontext von LOTAR sind:

- die Steuerung des Risikos von Informationsverlusten nach einem Zeitraum der LTA;
- re-interpretierbare Informationen basierend auf einem stabilen Datenformat;
- die Vermeidung von Aufwand bei der Qualitätskontrolle und bei Korrekturmaßnahmen (z. B. Reparatur) bei nachfolgenden Prozessen in der Archivkette.

6.1.1 Spezifikation für Verifizierungsstufen

Um das Risiko von Daten- oder Informationsverlusten während der LTA zu steuern, führt LOTAR ein Konzept von Verifizierungsstufen ein. Diese Stufen lauten:

Verifizierungsstufe	Verfahren	Risiko
0	Keine Regeln angewendet	Maximum
1	Obligatorische Regeln	Kalkuliertes Risiko
2	Obligatorische plus optionale Regeln	Minimiertes Risiko

Die Regeln und ihre Zuordnung zu „obligatorisch“ und „optional“ sind in den datentypspezifischen Teilen von LOTAR angegeben.

6.2 Validierung

Validierung wird angewendet, um die Integrität des Inhalts eines Dokuments während des gesamten LTA-Prozesses zu gewährleisten. Im Kontext von LOTAR wird die Validierung durch die Berechnung und den Vergleich von Validierungseigenschaften durchgeführt.

6.2.1 Validierungseigenschaften

Validierungseigenschaften sind signifikante Informationen, die berechnet werden mit den Daten:

- innerhalb des Absendersystems;
- nach jeder Konvertierung innerhalb des LTA-Prozesses.

Ein Satz Validierungseigenschaften ist wie ein Fingerabdruck für den Inhalt des Dokuments. Jede Änderung des Inhalts ändert ein oder mehrere Attribute der Validierungseigenschaften. Validierungseigenschaften sollten unabhängig vom System sein, und die Darstellung sollte innerhalb bestimmter Abweichungen bleiben.

Jeder Dokumententyp hat spezifische Validierungseigenschaften. Diese werden als Metadaten und optional in der LOTAR-Format-Datei gespeichert.

Zum automatischen Vergleich von Validierungseigenschaften kann eine vordefinierte Matrix verwendet werden. In dieser Matrix können Werte für Validierungseigenschaften und zulässige Abweichungen von diesen Werten gespeichert werden, um die automatische Verarbeitung zu erleichtern. Die zulässigen Abweichungen können je nach den definierten Anwendungsfällen (z. B. Produkthaftung oder Wiederverwendung von Designs) variieren und sind festzulegen.

Die detaillierten Informationen zu Validierungseigenschaften sind in den datentypspezifischen Teilen enthalten.

6.2.2 Spezifikation für Validierungsstufen

Um die Integrität des Inhalts und das Risiko von Daten- oder Informationsverlusten während der LTA zu steuern, führt LOTAR ein Konzept von Validierungsstufen ein. Diese Stufen lauten:

Validierungsstufe	Verfahren	Risiko
0	Keine Validierungseigenschaften angewendet	Maximum
1	Obligatorische Validierungseigenschaften	Kalkuliertes Risiko
2	Obligatorische plus optionale Eigenschaften	Minimiertes Risiko

Die Validierungseigenschaften und ihre Zuordnung zu „obligatorisch“ und „optional“ sind in den datentypspezifischen Teilen angegeben.