

DIN 31647:2015-05 (D)

Information und Dokumentation - Beweiswerterhaltung kryptographisch signierter Dokumente

| Inhalt | Seite |
|---|-------|
| Vorwort | 3 |
| Einleitung | 4 |
| 1 Anwendungsbereich | 6 |
| 2 Normative Verweisungen | 6 |
| 3 Begriffe | 7 |
| 4 Abkürzungen..... | 16 |
| 5 Funktionale Anforderungen an ein System zur Beweiswerterhaltung | 17 |
| 5.1 Anforderungen..... | 17 |
| 5.1.1 Art und Weise der Erzeugung von Hashwerten | 17 |
| 5.1.2 Nachvollziehbarkeit..... | 18 |
| 5.1.3 Fähigkeit zum ungehinderten Datenaustausch | 18 |
| 5.2 Funktionen | 19 |
| 5.2.1 Allgemeines | 19 |
| 5.2.2 Funktion 1: Einholung und Prüfung der beweisrelevanten Daten des SIP/Version..... | 19 |
| 5.2.3 Funktion 2: Erzeugen von technischen Beweisdaten des AIP | 19 |
| 5.2.4 Funktion 3: Abruf des AIP mit den technischen Beweisdaten zum Zweck der externen Integritäts- und Authentizitätsprüfung..... | 19 |
| 5.2.5 Funktion 4: Prüfung der technischen Beweisdaten | 20 |
| 5.2.6 Funktion 5: Erhaltung durch Erneuerung der technischen Beweisdaten des AIP..... | 20 |
| Anhang A (informativ) Archivpakete mit kryptographischen Beweismitteln..... | 22 |
| Anhang B (informativ) Anwendungsbeispiele..... | 25 |
| Literaturhinweise..... | 26 |
| | |
| Bilder | |
| Bild A.1 — Struktur eines Archivpaketes mit kryptografischen Sicherungsmitteln | 23 |