



# **Authentizität bewahren – Trans- formationen in der Archivpraxis**

Fachkonferenz „Rechtssichere elektronische  
Archivierung“ im Bundesministerium für Wirt-  
schaft und Technologie in Berlin am 13.12.2007

**Dr. Bernd Kappelhoff**  
**Präsident des Niedersächsischen Landesarchivs**  
**Am Archiv 1**  
**30169 Hannover**  
**Tel: 0511 / 120-6682**  
**e-mail: [bernd.kappelhoff@nla.niedersachsen.de](mailto:bernd.kappelhoff@nla.niedersachsen.de)**



## Zwei Schlüsselbegriffe:

### „Archiv“ und „Authentizität“

- Definition Archiv:

wörtlich „Schatzkammer“; Heimstatt von u.a. rechtlich erheblichen Unterlagen von **bleibendem Wert**, die deshalb auf Dauer aufbewahrt werden müssen

- Zweck von Archiven:

Gewährleistung von langfristiger Rechtssicherheit und Kontinuität in Recht und Verwaltung



## Basis archivischer Zweckerfüllung:

- Unzweifelhafte Authentizität und Beweiskraft des Archivguts (ergibt sich aus diesem selbst)
- Voraussetzung: Ununterbrochene und gegen unberechtigten Zugriff geschützte Überlieferungskette von der Entstehung über alle Phasen der zwischenzeitlichen Verwahrung bis zur Abgabe ins Archiv
- „Ius Archivi“ jahrhundertlang als spezifisches Rechtsinstitut dieser Gegebenheiten



## Authentizität (1)

- Ist bei ungestörter Überlieferungskette für papierne Unterlagen als Folge des „Ius Archivi“ per se gegeben.
- Beweiskraft und Beweiswert stehen bei herkömmlichem Archivgut in der Regel nicht in Frage.



## Authentizität (2)

- Muss bei elektronischen Unterlagen mit technischen Mitteln erreicht und nachvollziehbar unter Beweis gestellt werden durch
  - zuverlässiges Erzeugungssystem (DMS) mit vollständiger Dokumentation aller Bearbeitungsschritte
  - klar definierte und nicht manipulierbare Metadaten zur Herstellung von größeren Sachzusammenhängen (Vorgangs- und Aktenbildung)

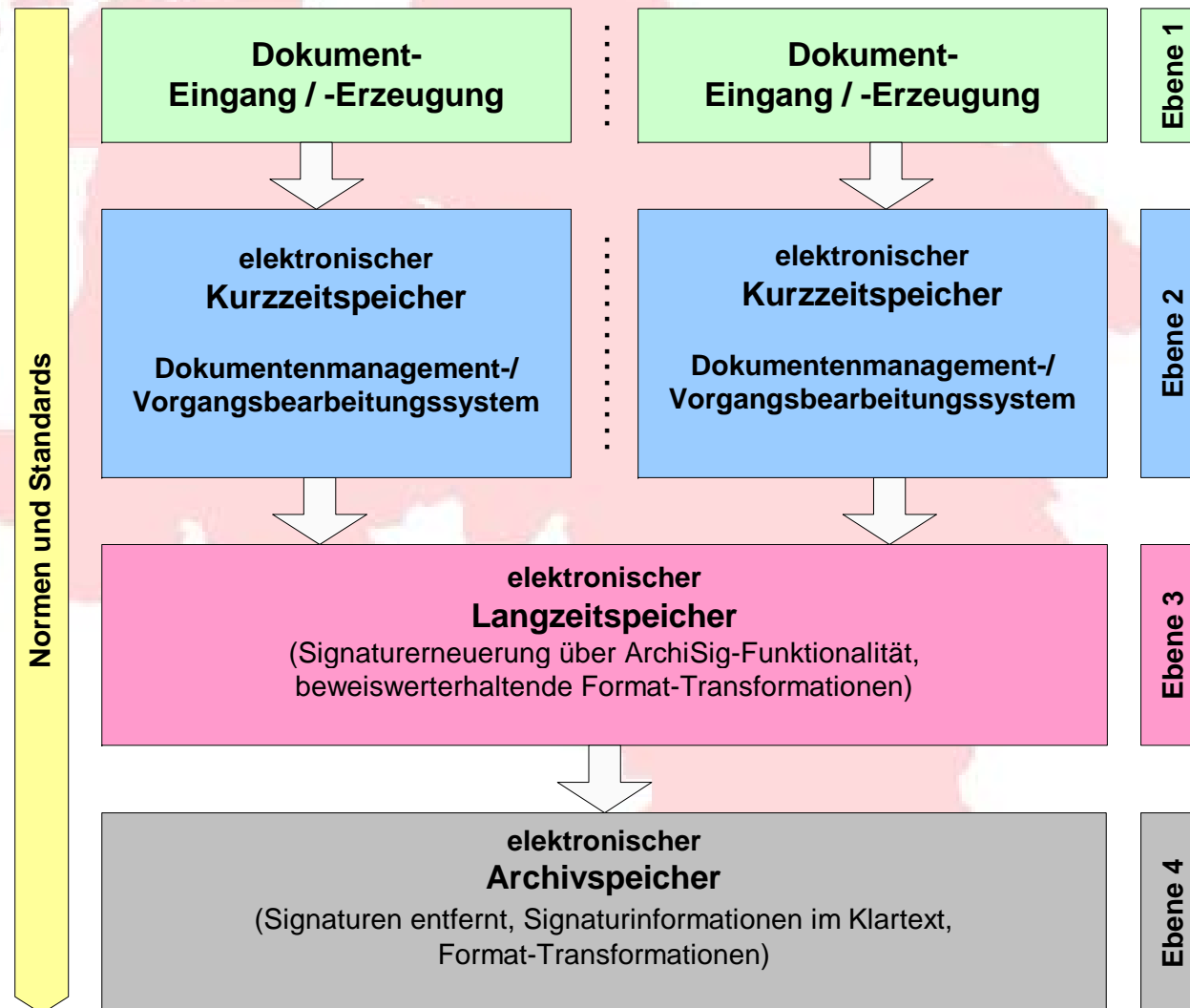


## Authentizität (3)

- bei Bedarf Einsatz elektronischer Signaturen
- kurze Verweildauer der Unterlagen im DMS bzw. sonstigen VORSYSTEM und klar definierter Übergang von diesem in einen gesicherten Langzeitspeicher mit ArchiSig-Funktionalität und dem dazugehörigen Instrumentarium (Signaturprüfung und ggf. Signaturerneuerung)



# Architekturmodell





## Verfahrensschritte (1)

- gemäß Lyfecycleprinzip Einbindung der Archive möglichst bereits bei der Konzeption von elektronischen Arbeitsverfahren sowie bei der Auswahl von DMS und der Entscheidung über deren Konfiguration
- XML-Schnittstelle zur Überführung in den Langzeitspeicher, dabei ggf. Transformation in ein archivtaugliches Format („Containerbildung aus Primär- und Metadaten“)



## Verfahrensschritte (2)

-Klar definierter Übergang vom Langzeit-  
speicher bzw. von Vorsystemen ins Archiv

**Beispiel:** StandardArchivierungsModul  
(SAM) für den Übergang von Daten und  
Unterlagen aus unterschiedlichen Erstsyste-  
men der Bundesverwaltung ins Bundes-  
archiv

-Vollständige Dokumentation etwaiger  
Transformationen



## Elektronische Signaturen (1)

- Sind erforderlich, solange **unmittelbare Rechtswirkung** anhält (i. d. R. 30 Jahre)
- Prüfung ihres korrekten Zustands und ihrer ordnungsgemäßen Genese im Zeitpunkt des Übergangs ins Archiv
- Genaue Dokumentation ihres ordnungsgemäßen Zustands und ihres vollständigen Inhalts



## Elektronische Signaturen (2)

-Nach Ablauf der unmittelbaren Rechtswirkung weitere Erneuerung elektronischer Signaturen im Archiv nicht erforderlich; es reicht die Dokumentation ihres korrekten Endzustands als Metadatum.

-Weiterer Beweiswert auch ohne Signaturen gegeben bei ordnungsgemäßer Überlieferungskette bis ins Archiv



## Elektronische Signaturen (3)

- Versuch zur (faktischen) Erneuerung des „Ius Archivi“ in § 371a ZPO bei den Beratungen des JKomG 2004
- Archivgesetze begründen ausreichendes Vertrauen in öffentliche Archive (Konzept „trusted custodian“)
- Beweiskraft öffentlicher Urkunden bleibt auch nach Konvertierung und Signaturentfernung erhalten, wenn alle genannten Schritte korrekt durchgeführt wurden