



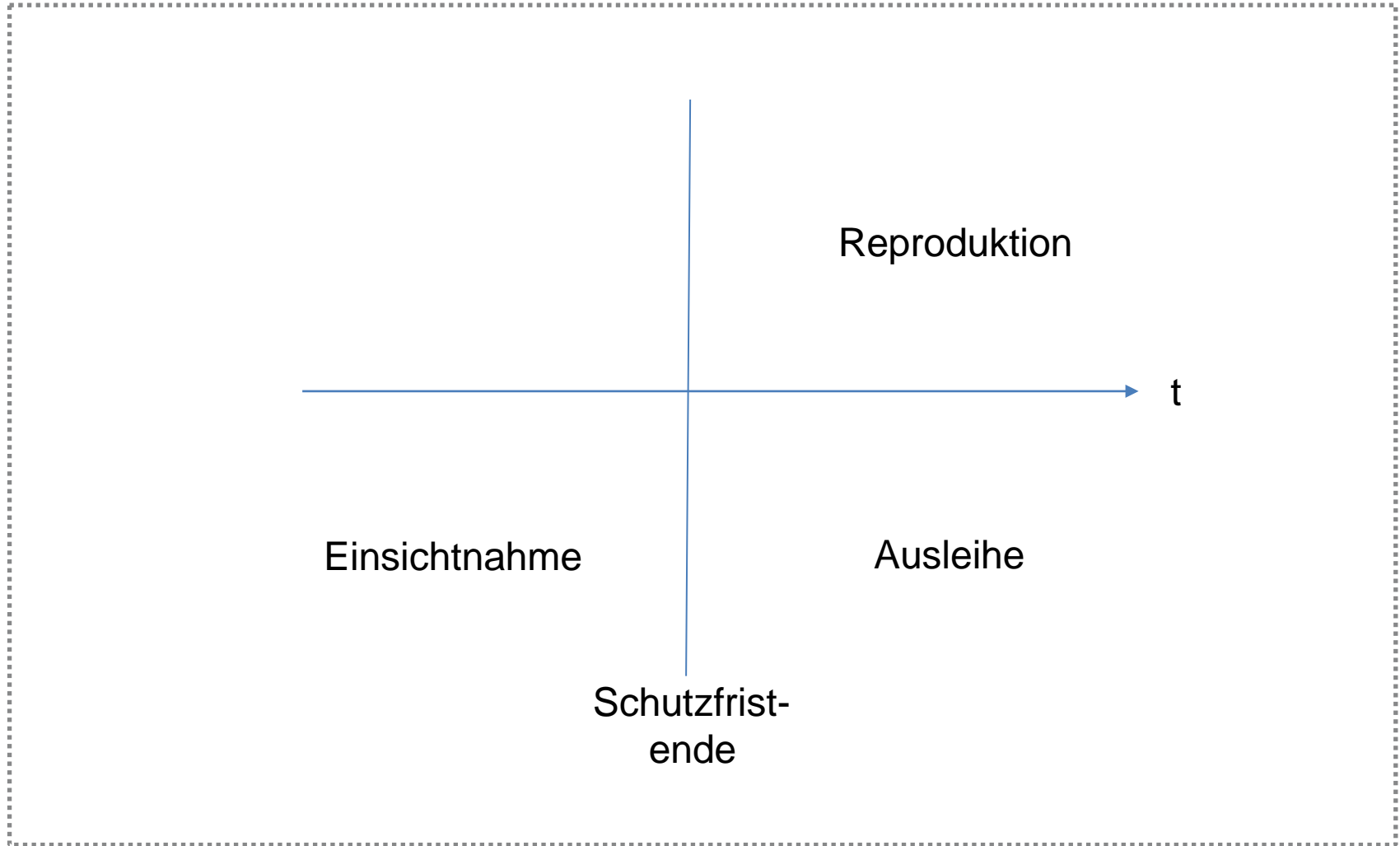
**scope**

Informatiklösungen für das  
Archivmanagement. Beratung  
im Records Management.

# Anforderungen an und Praxisbeispiele für das Rechtmanagement beim Access in der digitalen Archivierung

**12.03.2014**

# «Klasische» Vermittlungsarten



# Arten der «klassischen Ausleihe» (Ungarn)

- Accession (Übernahme)
  - Temporary Loan (zeitweilige Ausleihe)
  - Permanent Loan (dauerhafte Ausleihe)
  - Reproduction (dauerhafte Ausleihe als Kopie)
  - De-Accession (Kassierung)
- 
- Loan to public (öffentliche Ausleihe)
  - Loan to Administration (Ausleihe an abliefernde Stelle oder an interne Stelle mit erhöhten Zugriffsrechten)
  - Loan with special permission (Ausleihe mit Bewilligung)

# «klassische» ↔ «digitale» Ausleihe

- Ausleiharten sind grundsätzlich für beide Ausleihtypen gültig
- Digitale Ausleihe ist per Definition eine Kopie
  - Original geht mit jeder Übertragung verloren
  - Authentizität wird i.d.R. über Hashwerte sichergestellt
  - «Echte» Ausleihen von digitalen Objekten können nur über den Schutz vor weiterer Vervielfältigung sichergestellt werden

Gängige Mittel zum Schutz vor Vervielfältigung digitaler Objekte sind:

- Digital Right Management (DRM)
- «Sandboxes» (technische Umgebungen zum Schutz der darin angezeigten Informationen)

- Digital Right Management schützt heute primär copyright geschützte Inhalte
- Die Standards sind permanenten Angriffen ausgesetzt
- Sie unterliegen einer sehr hohen Veränderungsquote, welche durch die Industrie zum Schutz der Rechteinhaber fortwährend auf den neusten Stand der Technik gebracht werden
- Die Unterstützung zur Anzeige von DRM ist insb. eine Forderung der Bibliotheken an die digitale Archivierung
- DRM beeinflusst die Datenhaltung nach OAIS in der Form von AIP direkt
- Das OAIS konforme Preservation DRM-geschützter Inhalte ist weitgehend ungelöst

Fazit: DRM ist aufgrund der hohen Änderungsquote der Standards für die digitale Archivierung ungeeignet

- Als Alternative zum DRM bieten sich Sandboxes an
- Auch Sandboxes benötigen der stetigen Pflege, diese Pflege findet jedoch ausserhalb der Datenhaltung / ausserhalb des AIP statt
- Sandboxes bieten insb. im Lesesaal eine gute Lösung, da dort die Möglichkeit zum Kopieren mittels geeigneter Soft- und Hardwarekombination weitgehend unterbunden werden kann

Fazit: Sandboxes sind aus archivischer Sicht empfehlenswert, da sie im Rahmen des Access situativ angewendet werden können, ohne das Preservation zu tangieren.

# Öffentlich zugängliche Records



# Sandbox - Beispiel NRAA Oman

- Die National Records & Archiving Authority of Oman betreibt einen digitalen Lesesaal
- Öffentlich zugängliche Records ausserhalb der Schutzfrist sind direkt übers Internet zugänglich (PDF, Video, Audio, Digitalisate)
- Die Reproduzierbarkeit der öffentlich zugänglichen Records wird über geeignete «Sandbox Viewer» eingeschränkt.
- Die «Sandbox» Viewer können die Reproduktion nicht verhindern. Ziel ist, die «Kosten» für die Reproduktion so hoch wie möglich anzusetzen, das heisst die Aufwände, den «Sandbox Viewer» zu umgehen für «Angreifer» so weit wie möglich nach oben zu treiben
- Für Records mit hohem Schutzbedürfnis bildet ein Besuch im physischen Lesesaal die Voraussetzung
- Die digitale Ausleihe im physischen Lesesaal erfolgt auf Basis von thin clients
- Die Möglichkeit zur Kopie wird auf das Abfotographieren des Bildschirms eingeschränkt
- Andere Schnittstellen für die Reproduktion sind unterbunden

Nicht öffentlich zugängige Records

- Nutzer mit vordefinierter Zugriffsberechtigung
  - Zugriff aufgrund vordefinierter Rollen
  - (I.d.R.) Zugriff auf komplettes AIP (Erhaltung der granularen Entität)
  - Rollen auf Stufe Datenmanagement oder attributbasiert in den Metadaten des AIP festgelegt
  - Entscheid über Freigabe erfolgt zum Such- bzw. Zugriffszeitpunkt mittels Rollenmatching Partner  $\leftrightarrow$  Record
  - Möglicher Bedarf, den Zugriff im System zu Loggen
  - Zugriff remote i.d.R. möglich, jedoch nur innerhalb derselben Systemgrenzen (z.B. innerhalb des gleichen LANs)
- Archivnutzer mit temporärer Berechtigung
  - Zugriff i.d.R. durch manuelle Freigabe des Archivs (kein automatischer Zugriff über vordefinierte Rollen möglich)
  - Freigabe erfolgt mittels Transfer der gewünschten Records in eine «Sandbox»
  - Records müssen vor Bereitstellung durch das Archiv gesichtet werden
  - Physischer Besuch im Archiv nötig

- DIP Viewer Anwender
  - Darstellung der logischen DIP Struktur im Browser
  - Anzeige in Sandboxumgebung im physischen Lesesaal
  - Zugriff auf und Anzeige von Primärdaten im Browser oder mittels separatem Viewer durch einfachem Klick auf den entsprechenden Eintrag in der logischen Struktur
- DIP Editor Archivar
  - Erweiterter DIP Viewer mit Editorfunktionen
  - Erlaubt die Sichtung und Aufbereitung von DIP vor der Ausleihe
  - Möglichkeit, Primärdaten aus der Struktur zu entfernen
  - Möglichkeit, Metadaten zu verändern
  - Möglichkeit, Zweige in der logischen Struktur zu löschen
  - Möglichkeit, Zweige in der logischen Struktur zu verschieben
  - Möglichkeit, Zweige in der logischen Struktur einzufügen
  - Erhalt der DIP Schemadefinition über alle Manipulationen

# Die Frage der Entität

- Die kleinste Bestelleinheit in der klassischen Archivierung ist i.d.R. die Archivschachtel (Container)
- Eine weitere Aussonderung zum Zeitpunkt der Ausleihe wird vermieden (Ausnahme: bewilligungsbasierte Einsichtnahme)
- Schutzfristen beziehen sich auf Verzeichnungseinheiten (VE)
- Bei VE-übergreifenden Containern wird auf eine gleichwertige Schutzfrist der darin enthaltenen VE geachtet

# AIP versus Archivschachtel

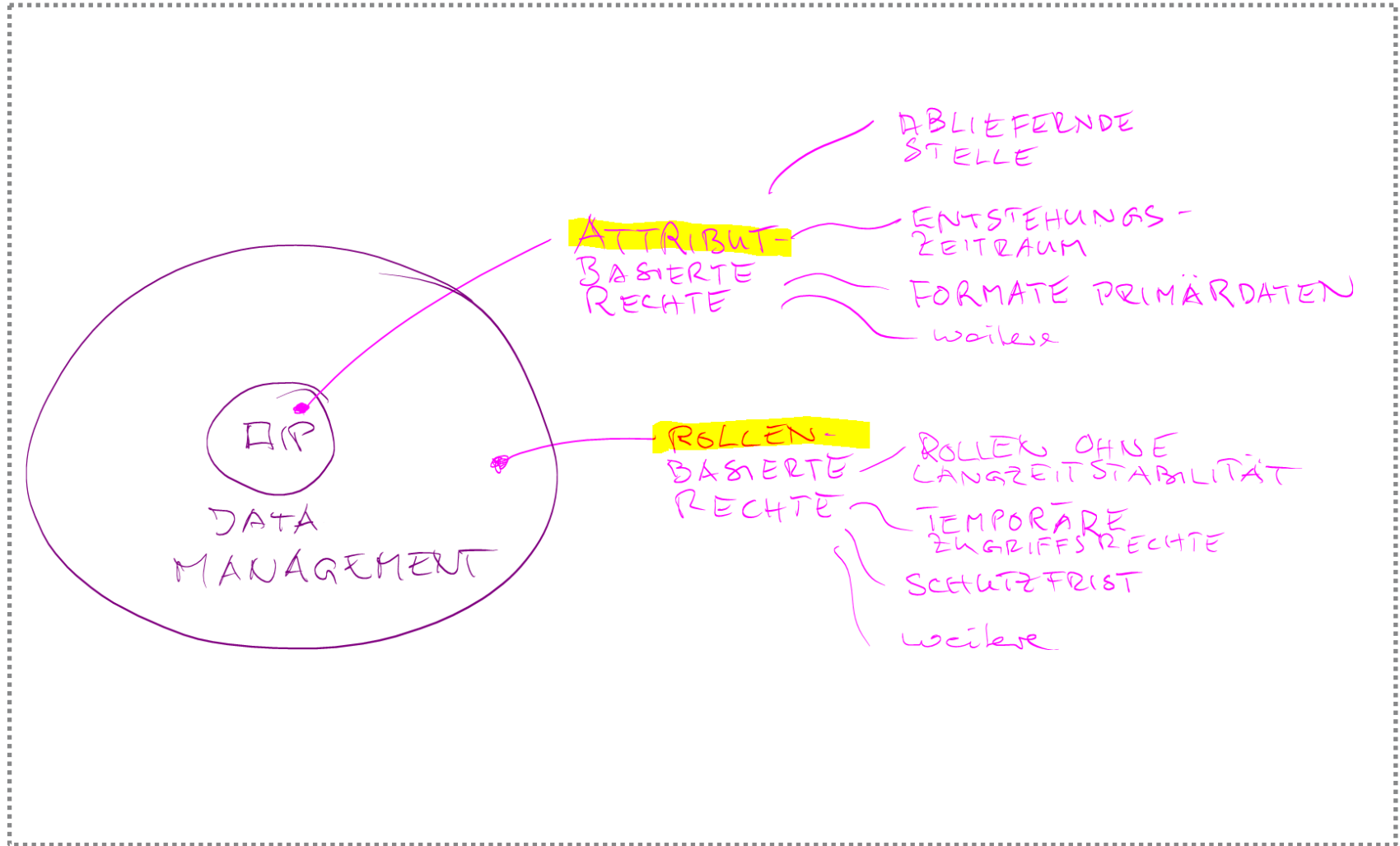
Wendet man das Entitätsprinzip der klassischen Archivierung auf die digitale Archivierung an, dann gilt:

- Das AIP ist die Archivschachtel der digitalen Archivierung (Container)
- Der elektronische Speicher ist das Magazin der digitalen Archivierung (Location)

Logische Konsequenz:

- Der Archivplan befindet sich ausserhalb des AIP
- Er ist stattdessen Teil des Data Managements.
- Hauptgrund: Falls die Archivplanposition ins AIP eingraviert ist, muss z.B. beim Verschieben von AIPs innerhalb des Archivplans zwingend ein Preservation Action durchgeführt werden

# Attribut versus Rollenbasiert





## Fazit:

- Die Erfahrungen aus dem Rechtenmanagement für die klassische Archivierung sollte als Grundsatz auch für die digitale Archivierung gelten.
- Die einfachste Rechtstufe ist die Schutzfrist öffentlicher Records. Diese erfolgt als Teil des Data Managements
- Einzelnen Rechteinhabern können permanent rollenbasierte Rechte eingeräumt werden.
- Rollenbasierte Rechte sollten ausserhalb des AIP (=Container) gepflegt werden (Grund: Notwendigkeit zur AIP Preservation bei Wechsel der recordsseitigen Zurgriffsrollen)
- Die im AIP enthaltenen Metadaten können für das attributbasierte Rechtenmanagement verwendet werden (z.B. abliefernde Stelle, Copyrightvermerk, Copyrightschutzfrist etc.)
- Temporäre Zugriffsrechte (z.B. bewilligungspflichtige Zugriffe) bedürfen der Sichtung der ausgehändigten Records über einen geeigneten DIP Editor

