

# ArchSafe

**Rechts- und revisionssichere  
Langzeitspeicherung elektronischer Dokumente**

**Dipl. Wirt.-Inform. Tobias Schäfer, PTB  
KoopA Erfahrungsaustausch  
Dresden 26. März 2007**

# ArchiSafe Record Keeping Strategy (ARS)

Die elektronische Archivstrategie der öffentlichen Verwaltung

## Agenda

Fakten & Ziele

Die Problemlage und die Ziele von ArchiSafe

Rahmenbedingungen

Rechtliche und technische Rahmenbedingungen

Initiativen

Initiativen, Konzepte und Standards

Konzept & Lösung

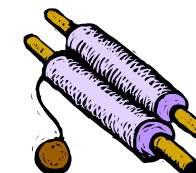
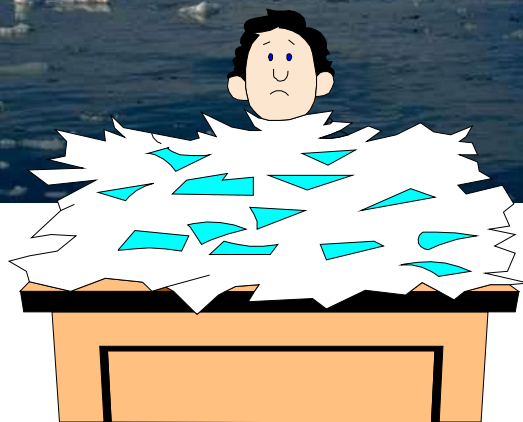
Das ArchiSafe Konzept und die ArchiSafe Referenzarchitektur

„Lessons learned“

... und die nächsten Schritte

Hallo Berlin...  
Wir haben ein  
Problem!

In den letzten 10 Jahren  
wurden mehr Akten  
produziert,  
als in der gesamten  
Menschheitsgeschichte  
ZUVOR.

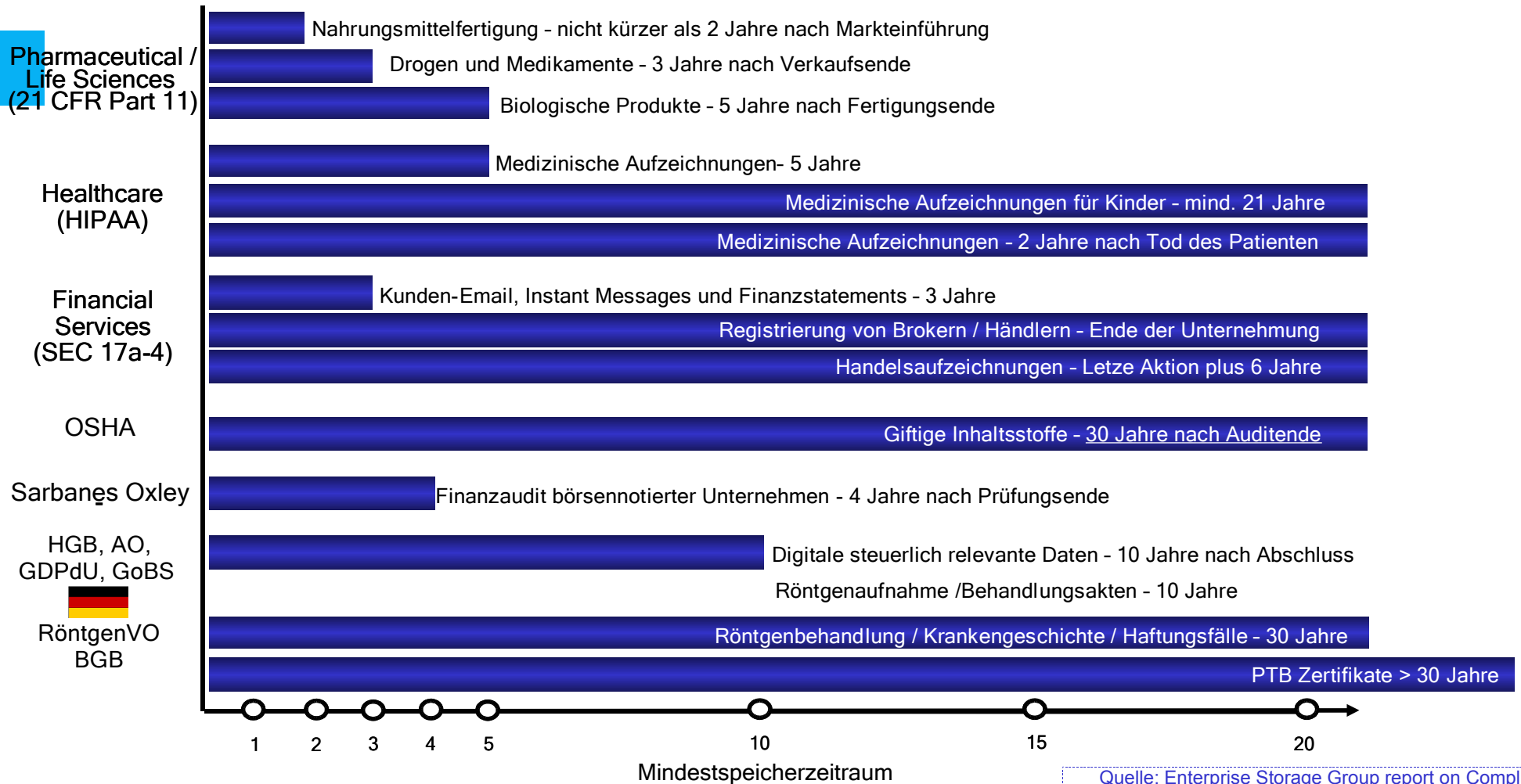


30 Jahre ?

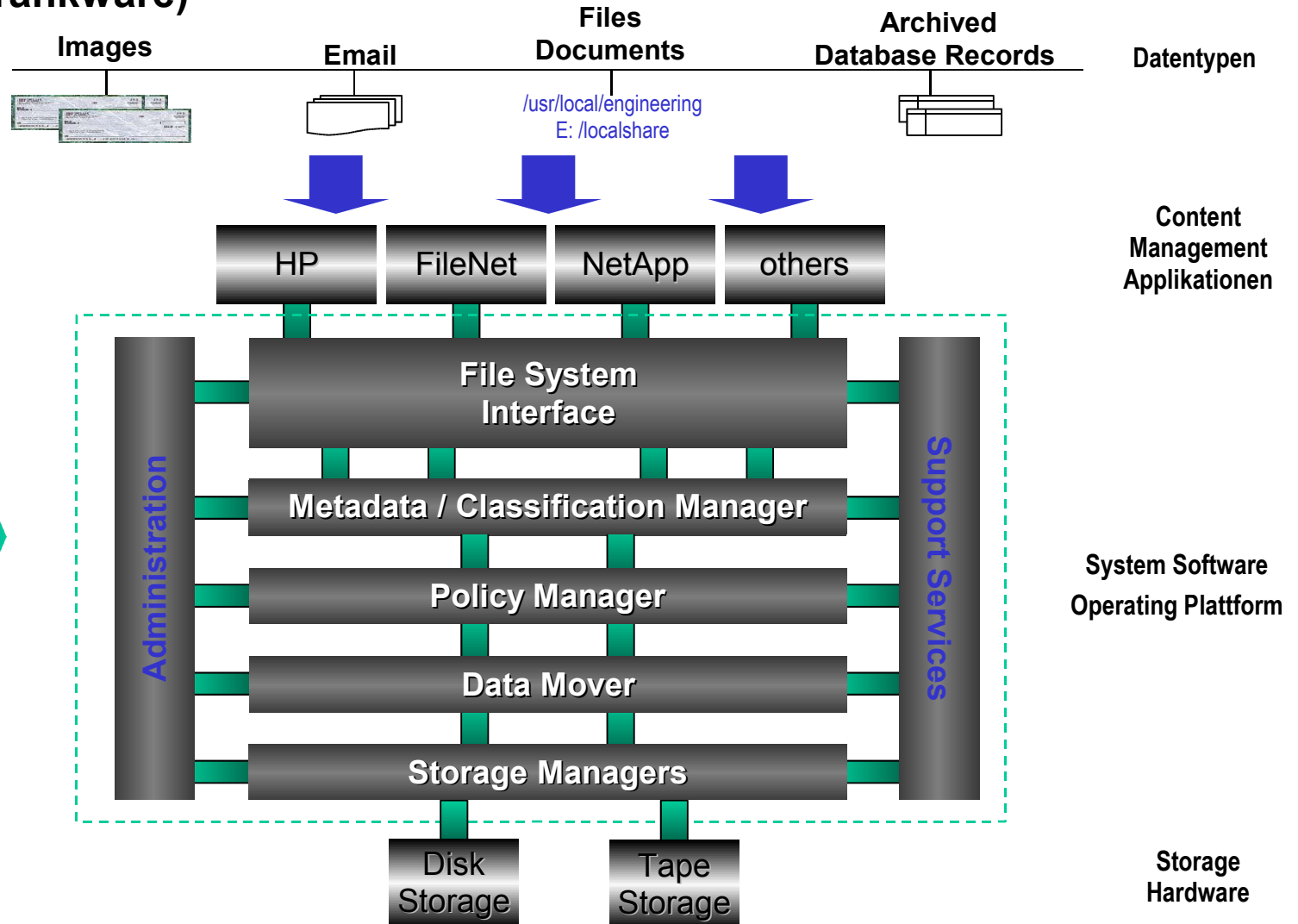
## Elektronisches Dokument

|            |                             |
|------------|-----------------------------|
| 256 LONG   | 2720 ImageWidth             |
| 257 LONG   | 3636 ImageLength            |
| 258 SHORT  | 1 BitsPerSample             |
| 259 SHORT  | 4 Compression               |
| ...        | ...                         |
| ...        | ...                         |
| 50571 BYTE | 30 82 03 04 06 09 2m 86 ... |
|            | 62 03 75 30 82 03 71 02 ... |
|            | 2b 24 03 02 01 05 00 ...    |
|            | ...                         |
|            | ...                         |
|            | 07 02 82 06 01 0m 07 01..   |

## ... Aufbewahrungspflichten für (elektronische) Dokumente



## ... viel Technik (Schrankware)



**Die „Botschaft“: ... machen Sie sich keine Sorgen, unsere IT wird's richten...**

## Studie des BMWI zu Anforderungen und Trends der langfristigen Aufbewahrung (Entwurf)

Uni Kassel, Projektgruppe verfassungsgemäße Technikgestaltung, Mai 2006

### ATLAS

#### Recht

- Das Recht bietet ausreichende Lösungen für die Rechts- und Beweissicherheit elektronischer Dokumente ... aber nicht in jedem Fall klare Regelungen

#### Anwender

- nach wie vor: Heterogenität in den Ansätzen und Lösungen
- Unklarheiten und Unsicherheiten über die rechtlichen Vorgaben und die Vor- und Nachteile vorhandener technischer Sicherungsmittel

#### Hersteller

- Angebote der Hersteller derzeit nicht darauf ausgerichtet, eine größere Homogenität herzustellen.
- obwohl Richtung klar und einheitlich ist:  
**Authentizität – Integrität – Lesbarkeit – Vollständigkeit – Verkehrsfähigkeit...**

## ArchiSafe

**Einen „Archiv-Dienst“ und eine Archiv-Schnittstelle als „Basisdienst“ für alle Fachanwendungen**

**Eine lose Kopplung zwischen dem Archiv und den Fachanwendungen,**  
so dass Änderungen im Archivsystem (Herstellerwechsel/Migration) ohne Auswirkungen auf die Fachverfahren bleiben und umgekehrt Änderungen in den Fachverfahren nicht aufwendige Nacharbeiten im Archiv benötigen

**Ein einheitliches und dauerhaftes Archivformat,**  
so dass archivierte Objekte auch nach langer Zeit noch verfügbar und lesbar sind

**Rechts- und Revisionssicherheit zum Nachweis der Ordnungsmäßigkeit des Verwaltungshandelns und Erhalt der Beweiskraft für die archivierten Dokumente**

auch und gerade für elektronisch signierte Dokumente

**Eine flexible und erweiterbare Abbildung der Papierakte auf die elektronische Akte**

So dass jederzeit auch von Dritten eine Rekonstruktion des Verwaltungsvorgangs möglich ist, auch dann, wenn die Fachanwendung nicht mehr zur Verfügung steht





**Ein „Einer-Für-Alle“ Projekt  
der Physikalisch-Technischen Bundesanstalt  
im Rahmen der E-Government Initiative BundOnline 2005**

Ziel: Konzept und Referenzarchitektur (proof-of-concept) für die rechts- und revisionssichere Langzeitspeicherung elektronischer Dokumente in der öffentlichen Verwaltung

**Start: 12-2004**

**Mehr als 25 Bundes- und Landesbehörden im Nutzerbeirat aktiv beteiligt, darunter: BSI, BNetzA, KBSt, Bundesarchiv, AA, BAFin, ...**

**Partner: CSC, BearingPoint, MICUS, SECUNET, IBM, OpenText (iXOS)**

**Proof-of-concept: 12-2005**

**Alle Ergebnisse unter: <http://www.archisafe.de>**





**Prinzip der Aktenmäßigkeit des behördlichen Handelns**

**§ 29 VerwVfG → Verpflichtung zum Führen von Akten**

- Gebot der Vollständigkeit
- Gebot zur Führung wahrheitsgetreuer Akten (Unversehrtheit)

**Unstrittig gültig auch für die elektronische Vorgangsbearbeitung / Kommunikation**

**§ 12 Gemeinsame Geschäftsordnung (der Bundesregierung)**

**„Stand und Entwicklung der Vorgangsbearbeitung müssen aus den elektronischen oder in Papierform geführten Akten nachvollziehbar sein“**

**§ 18 Abs. 1 S. 2 Registraturrichtlinie Bundesministerien (RegR)**

**„Bei elektronisch gespeichertem Schriftgut sind die Vollständigkeit, Integrität, Authentizität und Lesbarkeit durch geeignete Maßnahmen zu gewährleisten.“**



## Rechtswirkung elektronischer Dokumente (grundsätzlich geregelt)

- ✓ *SigG und SigV ( 2001)*
- ✓ *Änderungen Formvorschriften (BGB ,§ 126a)*
- ✓ *die Erleichterungen der Beweisführung (ZPO)*
- ✓ *Anpassung Verwaltungsverfahrenrecht*

## Handlungsbedarf: Erhalt der Rechtswirkung elektronischer Dokumente

> 10 ... 50 Jahre

- Sicherung des Ursprungs (Authentizität)*
- Sicherung der Unversehrtheit (Integrität)*
- Sicherung der Verkehrsfähigkeit*
  - der Daten und*
  - der „Beweismittel“*



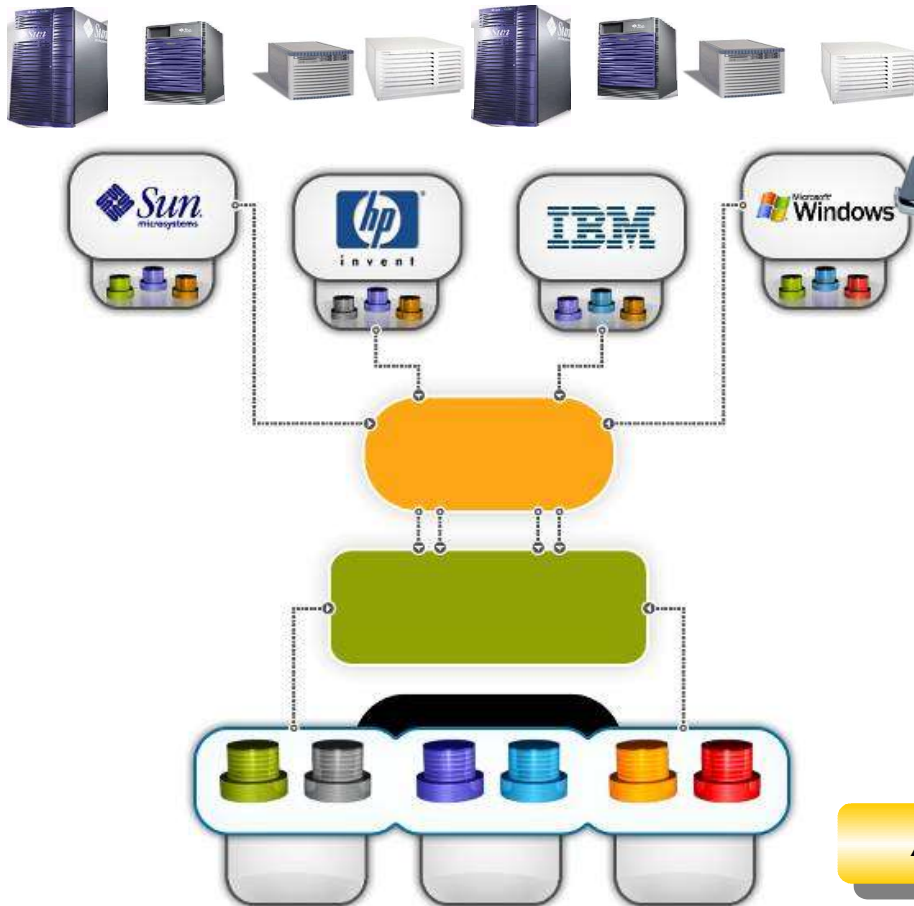
| Konzepte, Standards   | Inhalte / Funktionen  |
|---|---|
| DOMEA Organisationskonzept, Aussonderung, Archivierung - KBSt   | Einführung von DMS Lösungen in der öffentlichen Verwaltung  |
| DOMEA Organisationskonzept, Technische Aspekte der Archivierung elektronischer Akten - KBSt             | Anforderungen an Softwareprodukte (DOMEA Anforderungsprofil) für die Aufbewahrung elektronischer Dokumente  |
| MoReq (Model Requirements for the Management of Electronic Records - EU                                 | Modellspezifikation zu funktionalen Anforderungen an Schriftgutverwaltungssysteme   |
| Open Archival Information System OAI (ISO 14721) – Referenzmodell zur Archivierung digitaler Unterlagen | Referenzmodell für ein Archiv als Organisation, in dem Menschen und Systeme mit der Aufgabenstellung zusammenwirken, Informationen zu erhalten und einer definierten Nutzerschaft verfügbar zu machen |



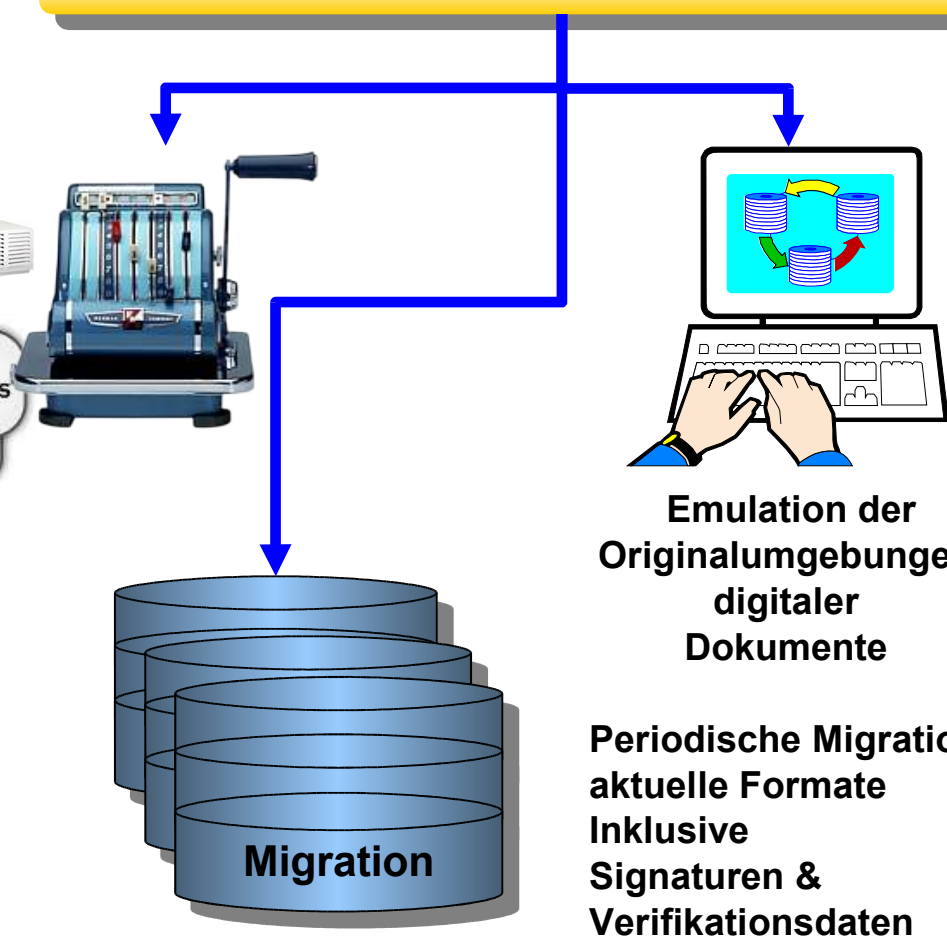
| Projektname  | Schwerpunkte  |
|--|---|
| <p>Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente (ArchiSig).</p> <p><a href="http://www.archisig.de">www.archisig.de</a></p>   | <p>(1) die Verifikation &amp; Erhalt des Beweiswertes qualifizierter elektronischer Signaturen,<br/>           (2) automatische Neusignierung durch qualifizierte Zeitstempel,</p> <p>Prototypen wurden in der Routine und die Konzepte im Rahmen der „Simulationsstudie AchiSig“ evaluiert.<br/>           Eine technische Standardisierung wurde eingeleitet.</p> |
| <p>ArchiSafe<br/>           EfA Projekt der PTB im Rahmen von BundOnline 2005</p> <p><a href="http://www.archisafe.de">www.archisafe.de</a></p>  | <p>Definition von Grundlagen für eine kostengünstige und skalierbare, rechts- und revisionssichere elektronische Archivlösung</p> <ul style="list-style-type: none"> <li>• Definition und Offenlegung von Formaten und Schnittstellen zu vorgelagerten Funktionen im Backoffice-Bereich</li> <li>• Realisierung in Form eines Pilotsystems.</li> </ul>              |
| <p>Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit digitaler Ressourcen in Deutschland (Nestor)</p> <p><a href="http://www.langzeitarchivierung.de">www.langzeitarchivierung.de</a></p> | <p>Kompetenzen und Informationen zu technischen, organisatorischen und rechtlichen Aspekten der digitalen Langzeitarchivierung verfügbar zu machen,<br/>           Kooperationen zwischen Bibliotheken, Archive, Museen, Datenzentren und anderen zu ermöglichen</p>  |
| <p>transidoc<br/>           Gefördert durch BMWi</p> <p><a href="http://www.trasidoc.de">www.trasidoc.de</a></p>   | <p>Anforderungen an &amp; Regeln für rechtssichere Transformationen, die Schaffung einer technischen Infrastruktur für rechtssichere Transformationen</p>   |

**Innovationszyklen werden immer kürzer...**

**Hard- und Software „Museum“**



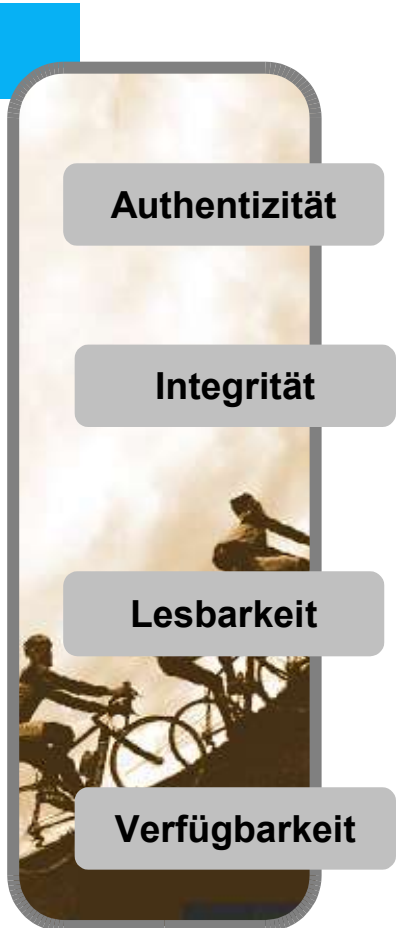
**Alternativen?**



**Emulation der Originalumgebungen digitaler Dokumente**

**Periodische Migration auf aktuelle Formate  
Inklusive Signaturen & Verifikationsdaten**

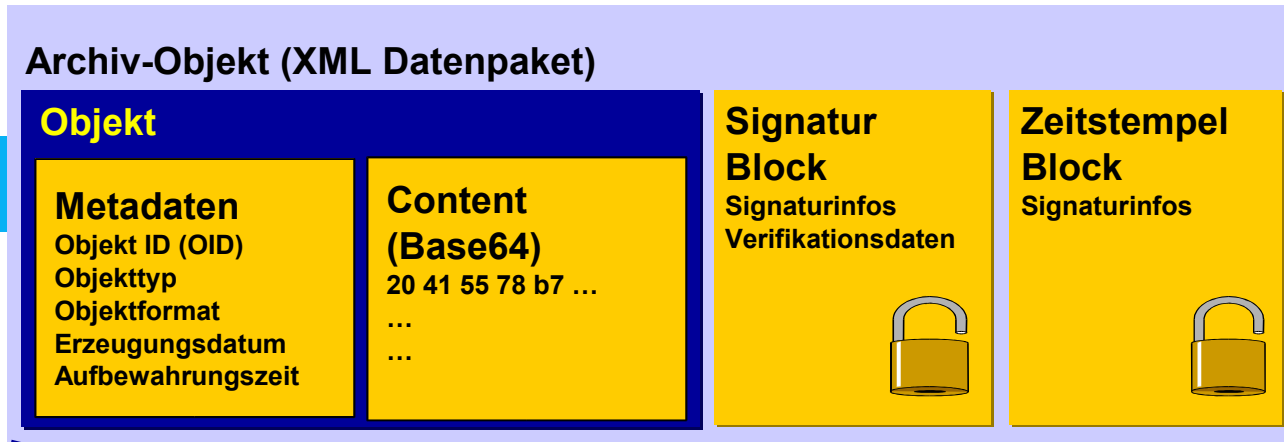
**Ausweg: Abhängigkeit von Technik reduzieren?**



| Physikalische Ebene   | Logische Ebene  | Dokument-Ebene   |
|---|---|--|
| <b>Integrität Bitstream</b>   | Dokumentation / Nachweis über Verfahrenswege (Zugriffsprotokolle)             | <b>Nachweis z.B. über elektronische Signaturen</b>   |
| Veränderungsschutz bspw. auf Ebene der Speichermedien mittels WORM-Technologien | Schutz / Nachweis über Verfahrenswege (Zugriffsschutz und Zugriffsprotokolle) | <b>Nachweis z.B. über elektronische Signaturen und/oder Zeitstempel</b>  |
| Bereitstellung von Technologien zum „Lesen“ elektronischer Speichermedien       | Gewährleistung der Verkehrsfähigkeit der Index-Verwaltung                     | <b>Gewährleistung der Lesbarkeit der Dokumentformate und Metadaten</b>   |
| Physische Redundanz von Speichermedien und Systemen                             | Anforderungsgerechte Gestaltung von Suchkriterien und Zugriffsmechanismen     | <b>Gewährleistung der Lesbarkeit gespeicherter Dokumentformate und Metadaten, Verfügbarkeit &amp; Integrität des Bitstream</b> |

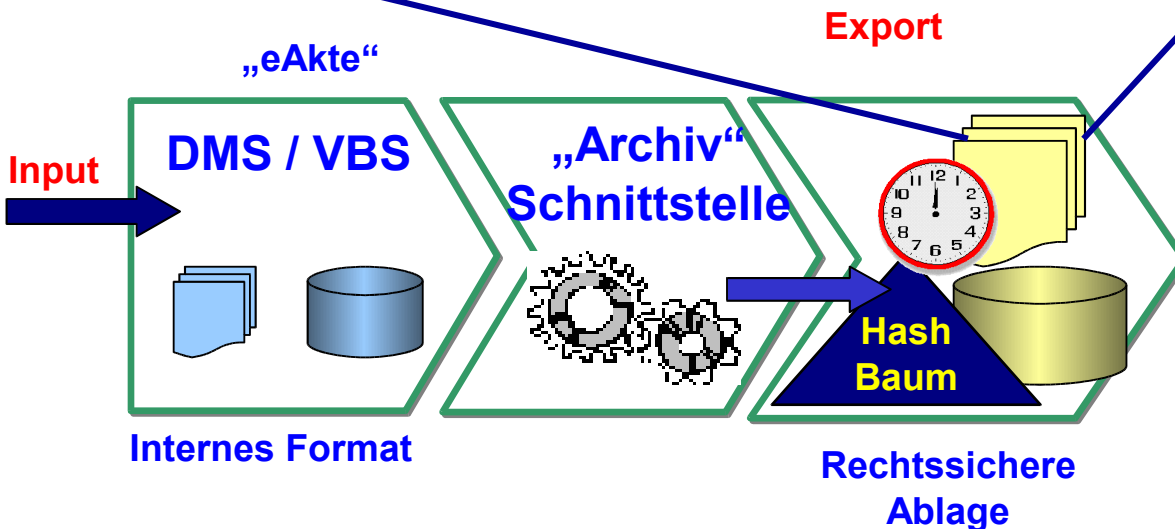
**... durch Erhalt ...**

| <b>Ziel</b>  | <b>Maßnahme</b>   |
|--|---|
| <b>Unversehrtheit (Integrität)</b>   | elektronischer Zeitstempel , elektronische Signatur<br>→ Manipulationen bleiben nicht unbemerkt   |
| <b>Ursprungs (Authentizität)</b> <ul style="list-style-type: none"> <li>▪ Bildl. &amp; inhaltliche Übereinstimmung</li> <li>▪ Autorschaft</li> </ul> | Datenformate : Text + Grafik → PDF-A / TIFF<br><br>elektronische Signatur = elektronische Unterschrift                                    |
| <b>Verkehrsfähigkeit</b>   | Dauerhaft wiedergabefähige Datenformate<br>→ Offene Standards: ASCII, PDF-A, TIFF   |
| <b>Verfügbarkeit</b>   | Migrationsstrategien (z.B. bei Technikwechsel)  |
| <b>Nachvollziehbarkeit des Verwaltungshandelns</b>   | Dokument + Bearbeitungsinformation → Archivobjekt<br>(Selbstbeschreibende d. h. aus sich selbst verständliche „elektronische Dokumente“ ) |



## Systemanforderungen:

- eindeutig interpretierbare, langfristig stabile & veröffentlichte **Nutzdatenformate**
- eindeutig interpretierbare, langfristig stabile & standardisierte **Signaturdatenformate**
- Verwendung elektronischer **Signaturen mit ausreichend hohem Sicherheitsniveau**
- **Archivierung** erforderlicher **Verifikationsdaten** in verkehrsfähiger Form
- **rechtzeitige** und **beweiskräftige** **Signaturerneuerung**
- Kosteneffizienz durch **Nachnutzbarkeit & Einsatz standardisierter, wirtschaftlicher Technologien**



XML-Datei (Dokument) →

Archiv Objekt

Archiv Objekt : z. B. „Akte“

„Garderobenmarke“  
Objekttyp = „Akte“

Metadaten zur „Akte“

Dokument 1

Dokument 2

Dokument  
Spezifische  
Metadaten

Dokument  
Spezifische  
Metadaten

Dokument  
Inhalt  
Abcabcab  
Abcabcab  
Abcabcab

Dokument  
Inhalt  
Abcabcab  
Abcabcab  
Abcabcab

Garderobenmarke = ObjectID

Objektbeschreibung: „Akte“

Aktentitel

...

Löschdatum

Löschverfügung

Gehört zu: ...Aktenkennzeichen

Dokumenttyp: Antrag

Betreff

...

Löschdatum



## Sicherung der Unversehrtheit (Integrität)

- Hashverfahren / Signaturverfahren / Schutz des Signaturschlüssels

**Problem:**

Zeitbedingtes Nachlassen der Sicherheit kryptographischer Algorithmen und Parameter

➡ Erneute Signatur nach § 17 SigV

## Sicherung des Ursprungs (Authentizität)

- Zertifikate (Identifizierung und Übergabe) / Dokumentation
- Verzeichnis- und Sperrdienste / Gültigkeitsabfragen / Algorithmen und zugehörige Parameter

**Problem:** Zeitlich begrenzte Prüfbarkeit der Zertifikate  
max. 5 Jahren bei qualifizierten ZDA  
max. 30 Jahren bei akkreditierten ZDA

➡ Erneute Signatur nach § 17 SigV

➡ Rechtzeitige Sicherung der Verifikationsdaten und Integration

## Projekt ArchiSig BMWA (2003)

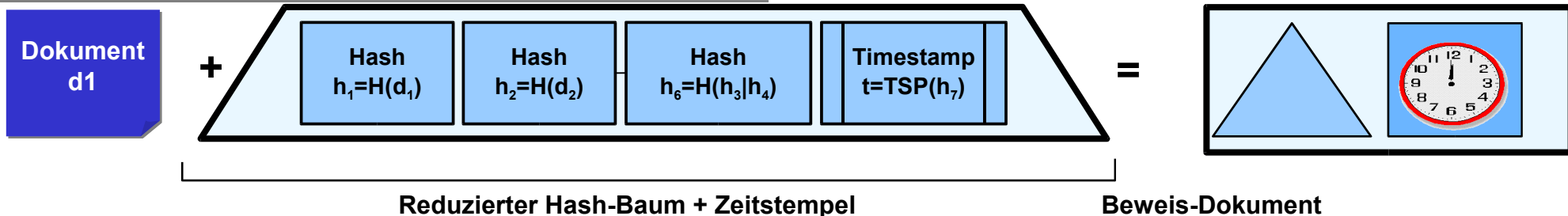
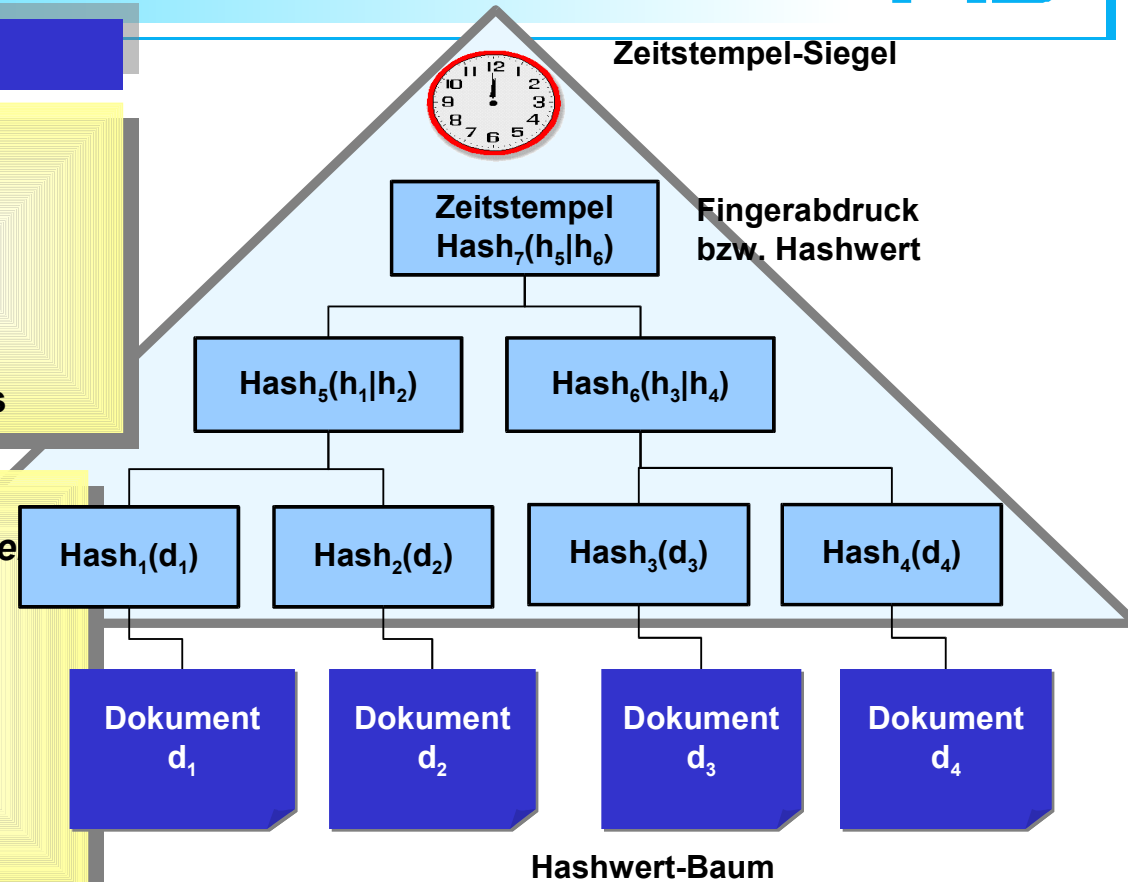
### Technologie

- **Akkreditierte Zeitstempel**
- **Merkle-Hashbäume**
- **Resultat**
  - Erhaltung der elektronischen Form
  - Bewahrung des hohen Beweiswerts

■ **Verifikationsdaten bei Verifikation im Anwendungssystem einholen und im Dokument vervollständigen**

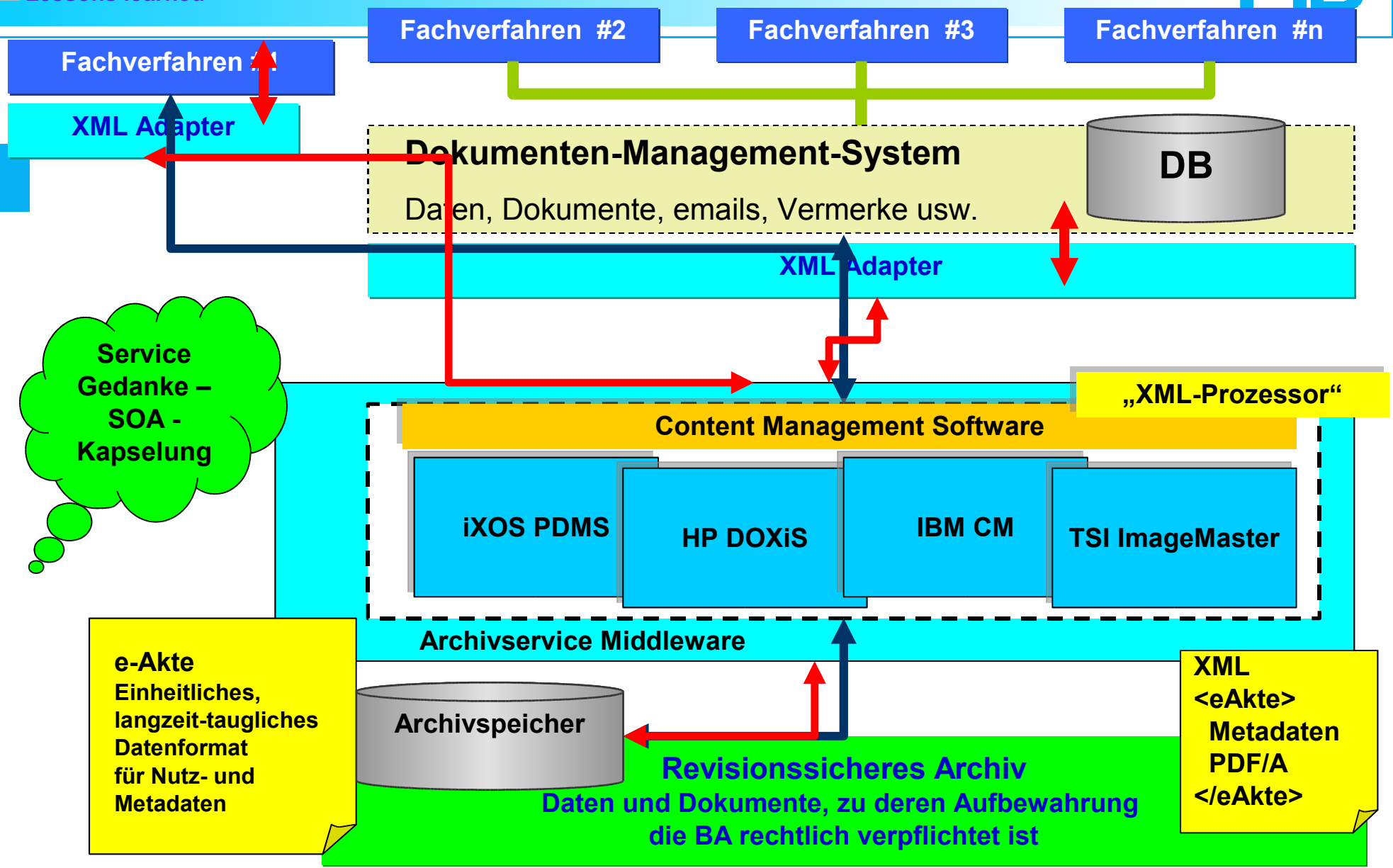
■ **Dokument archivieren und wiederholt zeit-stempeln**

■ **Dokument mit integrierten Verifikationsdaten und Archivzeitstempeln später abrufen**



- Fakten & Ziele
- Rahmen
- Initiativen
- Konzept & Lösung
- Lessons learned

# ArchiSafe: Architekturidee

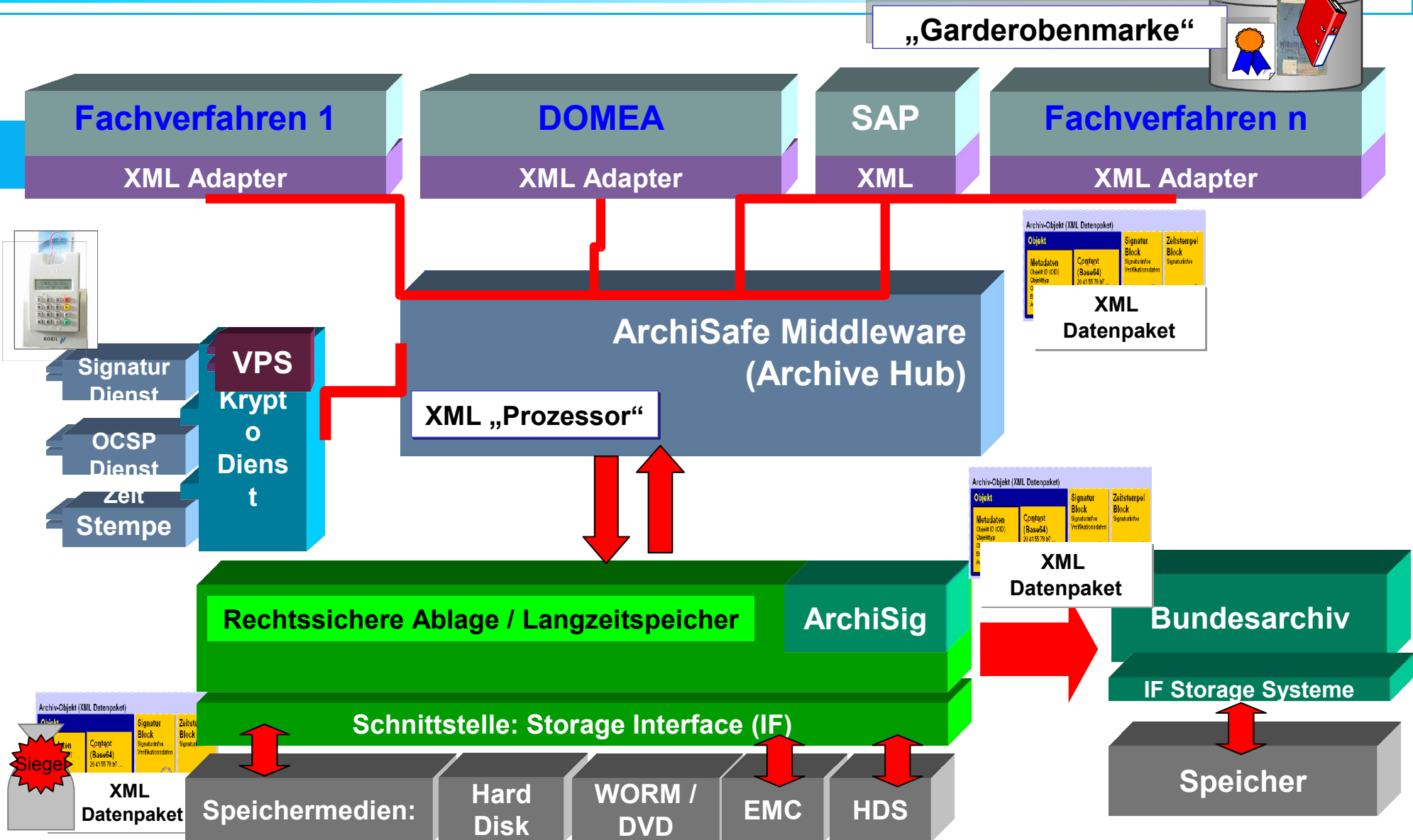


- Fakten & Ziele
- Rahmen
- Initiativen
- Konzept & Lösung
- Lessons learned

# ArchiSafe: Zielarchitektur



„Garderobenmarke“



Archi-Objekt (XML Datenpaket)

|   |                                       |   |
|---|---------------------------------------|---|
| Objekt                                    | Signatur Block                        | Zeitstempel Block                                   |
| Metadaten<br>Objekt ID (OID)<br>Objekttyp | Content<br>(Base64)<br>30 41 55 78 67 | Signatur Block<br>Signaturdaten<br>Verifikatordaten |

XML Datenpaket

Archi-Objekt (XML Datenpaket)

|   |                                       |   |
|---|---------------------------------------|---|
| Objekt                                    | Signatur Block                        | Zeitstempel Block                                   |
| Metadaten<br>Objekt ID (OID)<br>Objekttyp | Content<br>(Base64)<br>30 41 55 78 67 | Signatur Block<br>Signaturdaten<br>Verifikatordaten |

XML Datenpaket

Siegel

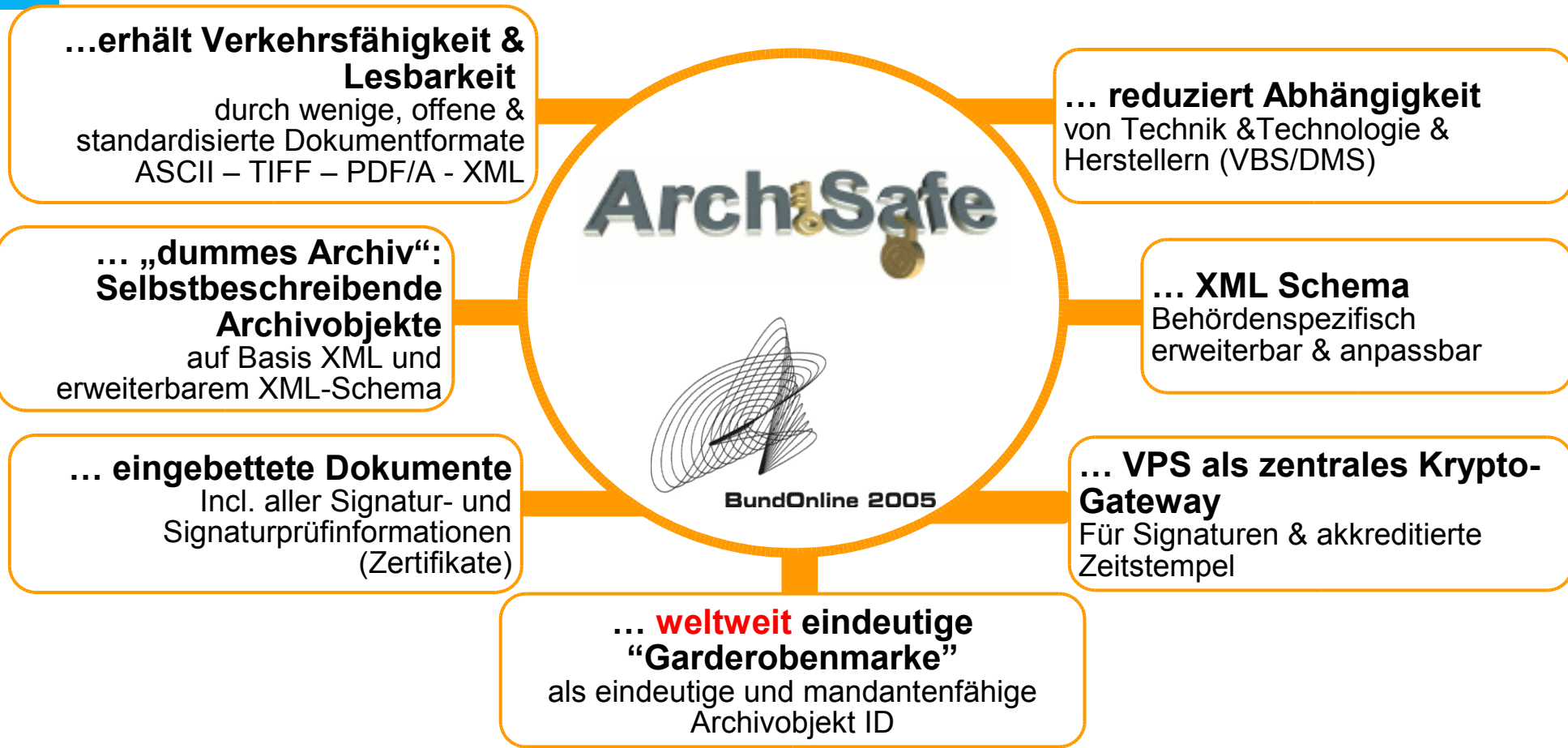
Archi-Objekt (XML Datenpaket)

|   |                                       |   |
|---|---------------------------------------|---|
| Objekt                                    | Signatur Block                        | Zeitstempel Block                                   |
| Metadaten<br>Objekt ID (OID)<br>Objekttyp | Content<br>(Base64)<br>30 41 55 78 67 | Signatur Block<br>Signaturdaten<br>Verifikatordaten |

XML Datenpaket



## ARS ArchiSafe Record Keeping Strategy – ein pragmatischer Ansatz





## ARS Spezifikationen

- ✓ ARS Fachkonzept (funkt. Anforderungen)
- ✓ ARS Metadatendefinition & XML Schema
- ✓ ARS Dokumentformate
- ✓ ARS Signaturformate
- ✓ ARS Schnittstellen

Alles unter: [www.archisafe.de](http://www.archisafe.de)

## Standardisierung

- ✓ Standardisierung des ARS-XML-Schema im KoopA
- ✓ Erstellung eines Schutzprofiles nach CC-Anforderungen
- ✓ Aufnahme in das DOMEA-Konzept

**Fazit: ArchiSafe** ist ein **realisiertes Konzept** = geeignet als **Basis & Standard** (Referenz) für Ausschreibungen & Aufträge der öffentlichen Hand in Bund – Ländern – Kommunen  
**Nicht zuletzt aus wettbewerbsrechtlichen Gründen kein Produkt**

**Dir. u. Prof. Dr. Siegfried Hackel**

**Physikalisch-Technische Bundesanstalt (PTB)  
Fachbereich Q.4 Informationstechnologie  
Bundesallee 100  
D-38116 Braunschweig  
Tel.: +49 (531) 592-8400  
Fax.: +49 (531) 592-8406  
Mailto:siegfried.hackel@ptb.de**

**...und**

**Dipl. Wirt.-Inform. Tobias Schäfer  
ArchiSafe Projektleiter  
Arbeitsgruppe Q.43 Datenbanken  
Bundesallee 100  
D-38116 Braunschweig  
Tel.: +49 (531) 592-2456  
Fax.: +49 (531) 592-692456  
Mailto: tobias.schaefer@ptb.de**

**Vielen Dank für Ihre Aufmerksamkeit**