



ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente

# Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente

## Ergebnisse des Forschungsvorhabens „ArchiSig“

**Prof. Dr. Paul Schmücker**

Hochschule Mannheim, Fachbereich Informatik

**1. Nutzerbeiratssitzung des Projektes „ArchiSafe“  
am 02. Februar 2005**

**in der Physikalisch-Technischen Bundesanstalt,  
Braunschweig**



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNIKASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
1



# Gliederung

1. Historie digitaler Medien im Bereich Langzeitarchivierung
2. Problemstellungen bei der Einführung digitaler Signaturen zur Langzeitarchivierung
3. Verbundprojekt „ArchiSig“: Zielsetzungen und Partner
4. Ergebnisse des Verbundprojektes „ArchiSig“
5. Resümee und Fazit

2000

2010

2020

2030



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDIGES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
2



# 1. Historie digitaler Medien im Bereich Langzeitarchivierung

80'er Jahre: große Euphorie nach Einführung digitaler Medien wie die WORM ==> Visionen vom papierlosen Krankenhaus + vom papierlosen Büro

Zertifikate der Firmen PHILIPS (30 Jahre) und SONY (100 Jahre) zur Haltbarkeit von WORM-Medien

2000 ----- 2010 ----- 2020 ----- 2030 -----



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

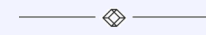
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
3



## Problematik:

These 1: Es gibt bisher kein digitales Archivmedium, lediglich digitale Speichermedien.

These 2: Digitale Dokumente genügen bisher in der Regel nicht den Anforderungen der Ordnungsmäßigkeit, Revisionssicherheit und rechtlichen Anerkennung.

2000

2010

2020

2030



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
4

## Aktivitäten der 90'er Jahre:

Das Bundesjustizministerium reagiert nicht zufriedenstellend auf Forderungen nach einer Gesetzesinitiative zur rechtlichen Anerkennung digitaler Dokumente.

Der Verband Organisations- und Informationssysteme e. V. (VOI) erarbeitet organisatorische Grundsätze für die Ordnungsmäßigkeit, Revisionssicherheit und rechtliche Anerkennung digital erzeugter Dokumente.

1997: Verabschiedung des Deutschen Signaturgesetzes, allerdings ohne Bezug auf die sonstige Gesetzgebung



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
5

## Fazit im Jahr 2001:

Wir sind häufig noch weit vom papierlosen Büro und papierlosen Krankenhaus entfernt.

## Lösungsansätze zur Sicherstellung der Rechtsicherheit:

Vereinbarung mit dem Haftpflichtversicherer

hybride Archivierung (gleichzeitige Ablage von Mikrofilm und digitalem Medium)

Grundsätze der Ordnungsmäßigkeit und Revisionsicherheit digitaler Archive (VOI e.V.)

Anwendung digitaler Signaturen



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
6



## Neuer Lösungsansatz seit 2001:

2001: Novellierung des Deutschen Signaturgesetzes, Anpassung des Bürgerlichen Gesetzbuches (BGB) und der Zivilprozessordnung (ZPO)

==> Integration digitaler Signaturen in Dokumentations- und Archivierungssysteme

2000

2010

2020

2030



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie

7

## 2. Problemstellungen bei der Einführung digitaler Signaturen zur Langzeitarchivierung

- Kryptographische Algorithmen können mit der Zeit ihre Sicherheitseignung verlieren.
- Zeitlich begrenzte Prüfbarkeit und Verfügbarkeit von qualifizierten Zertifikaten
  - 5 Jahre bei nicht akkreditierten Zertifizierungsdiensteanbietern
  - 30 Jahre bei akkreditierten Zertifizierungsdiensteanbietern
- Informationen zur Sicherheitseignung der Algorithmen liegen nicht in digitaler Form vor.
- Transformation in andere Dokumentenformate oder -träger führt zur Ungültigkeit der ursprünglichen Signaturen

↳ Elektronisch signierte Dokumente können im Laufe der Zeit an Beweiswert verlieren



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

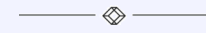
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie

8



## Problemstellungen (2)

kaum Erfahrungen mit einer benutzer- und prozessgerechten performanten und kostengünstigen Integration digitaler Signaturkomponenten in beliebig komplexe Informationssysteme

wenig Bereitschaft zur Einführung der digitalen Signatur und der digitalen Langzeitarchivierung

Unsicherheiten bezüglich der Umsetzung der neuen Gesetzgebungen



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

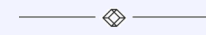
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
9



### 3. Verbundprojekt „ArchiSig“: Zielsetzungen und Partner

Im Projekt „ArchiSig“ wurden gesetzeskonforme technische Lösungen und organisatorische Konzepte zur beweiskräftigen und sicheren Langzeitarchivierung digital erzeugter und signierter Dokumente erarbeitet und auf ihre praktische Einsetzbarkeit und Beweiseignung überprüft.

gefördert vom Bundesministerium für Wirtschaft und Arbeit (BMWA)



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
10



# Zielsetzungen

Erarbeitung organisatorischer Konzepte und technischer Lösungen, die eine sichere und beweiskräftige Langzeitarchivierung digital erzeugter und signierter Dokumente über 30 Jahre und mehr ermöglichen

Prototypische Umsetzung und Evaluation

Nachweis der Rechtskonformität, Praktikabilität und Wirtschaftlichkeit

Nachweis der Rechtsgültigkeit durch Beweisgutachten anhand fiktiver Rechtsfälle



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
11



# ArchiSig

Beweiskräftige und sichere  
Langzeitarchivierung digital  
signierter Dokumente



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)



SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
12

# ArchiSig-Projektpartner

interdisziplinäres Team aus Wissenschaft, Industrie und Anwendern

- Universitätsklinikum Heidelberg: Abt. Medizinische Informatik + Abt. Innere Medizin II
- PERGIS Systemhaus GmbH in Ludwigshafen (Konsortialführer)
- Niedersächsische Staatskanzlei: Staatliche Archivverwaltung in Hannover
- SECUDE Sicherheitstechnologie Informationssysteme GmbH in Darmstadt
- CEYONIQ AG in Bielefeld (im Frühjahr ausgeschieden)
- IXOS Software AG in Grasbrunn / München (ab 01.11.2002)
- Fraunhofer-Institut für sichere Telekooperation SIT in Darmstadt
- Universität Kassel: Projektgruppe Verfassungsverträgliche Technikgestaltung (provet)
- DATEV eG in Nürnberg (nicht geförderter Partner ab Frühjahr 2002)
- sonstige Partner: Informatik-Zentrum Niedersachsen, Hochschule Mannheim, T-Systems incl. SAP-Gruppe Gesundheitswesen



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDE  
e-security for e-business

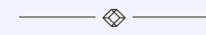
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
13



## 4. Ergebnisse des Verbundprojektes „ArchiSig“

- ArchiSig-Anforderungskatalog
- ArchiSig-Grobspezifikation
- Stellungnahme zur Erneuerung qualifizierter elektronischer Signaturen nach § 17 SigV
- Grundsätze zur Langzeitsicherung elektronisch signierter Dokumente
- ArchiSig-Prototypen
- ArchiSig-Gerichtssimulation (Simulationsstudie)
- Standardisierungsinitiative



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH  
SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
14



# Analysen

- Dokumenten- und Geschäftsprozessanalysen zum Unterschriftsverhalten im Gesundheitswesen
  - **Medizinische Universitätsklinik und Poliklinik Heidelberg (335 Betten)**
  - **Krankenhaus Wetter (60 Betten)**
  - **Niedergelassene Ärzte aus der Region Heidelberg / Mannheim**
- Untersuchung von Standards
- rechtliche Analysen
- Markt- und Systemanalysen im Bereich von Dokumentenmanagement- und Archivierungssystemen sowie von PKI-Komponenten
- Analysen von Nutz- und Signaturdatenformaten
- Sicherheits- und Beweiswertanalysen



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

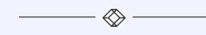
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
15



# Medizinische Dokumentation

ca. 60 % der Dokumente unterschriftsrelevant



- Universitätskliniken
  - Anzahl: ca. 40
  - Dokumente/Jahr: ca. 6.000.000
- Krankenhäuser
  - Anzahl: ca. 2.200
  - Dokumente/Jahr: > 30.000
- Arzt- und Zahnarztpraxen
  - Anzahl: ca. 125.000
  - Dokumente/Jahr: < 10.000



- Aufbewahrungsfristen von 30 Jahren und mehr



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDIDNES  
e-security for e-business

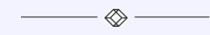
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

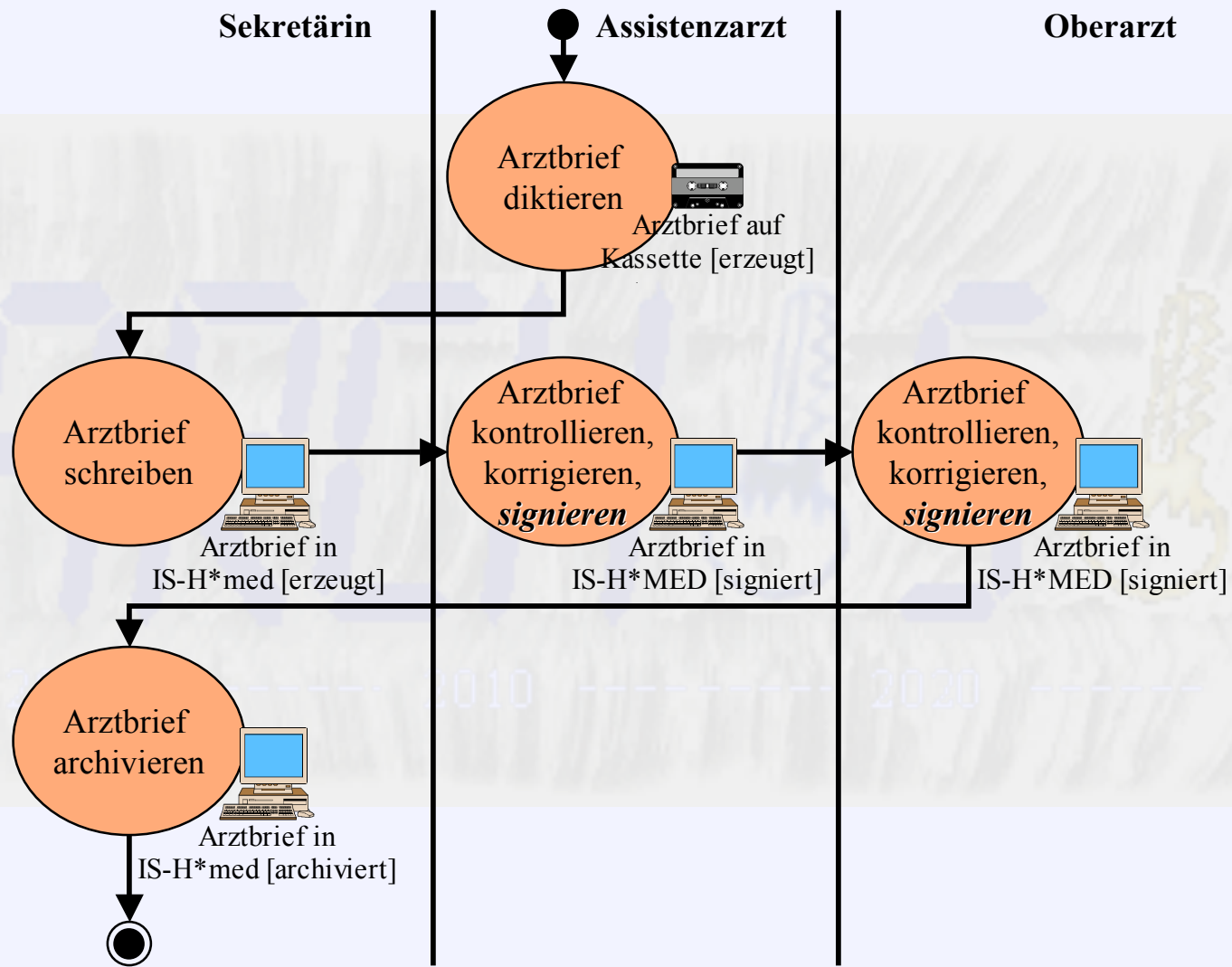


PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
16



# Geschäftsprozeß der Arztbriefschreibung mit digitaler Signatur



Universitätsklinikum Heidelberg



Fraunhofer Gesellschaft, SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische Staatskanzlei



IXOS Software AG, Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie Informationssysteme GmbH, Darmstadt



DATEV eG, Nürnberg

PERGIS

PERGIS Systemhaus GmbH, Ludwigshafen

Folie 17

# Konkrete Anforderungen (1)

- Verifikationsdatenbeschaffung und -sicherung
- Signaturerneuerung: rechtzeitige, automatische Signaturerneuerung durch qualifizierte Zeitstempel vor dem Sicherheitsverlust von Signatur- und Hashverfahren
- Berücksichtigung der amtlichen Sicherheitseignungsbestätigungen für Algorithmen
- Transformation: Gewährleistung der Integrität und Authentizität bei der Transformation (P-to-E, E-to-P, E-to-E)



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCES  
e-security for e-business

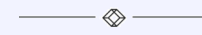
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
18



## Konkrete Anforderungen (2)

- Migration: Übernahme der Dokumente mit allen Verifikationsdaten und erneuten Signaturen von anderen Dokumentenmanagement- und Archivierungssystemen oder Langzeitspeichermedien ohne Beweiswertverlust
- Anwendungsintegration unter Berücksichtigung des Lifecycle der Dokumente



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

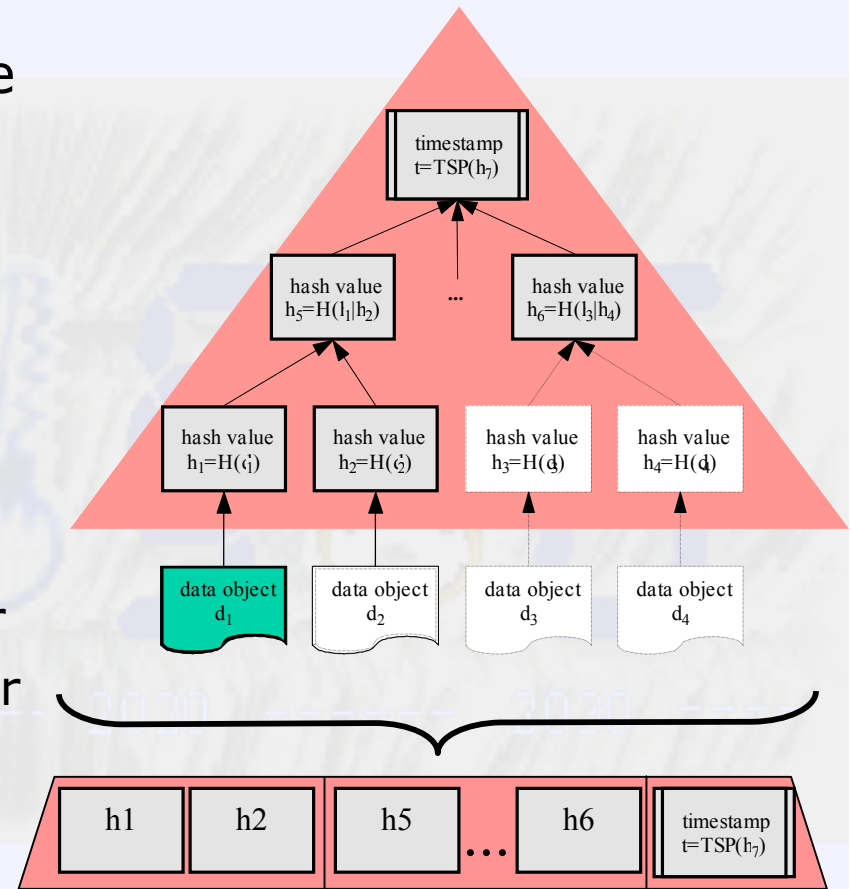
PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
19



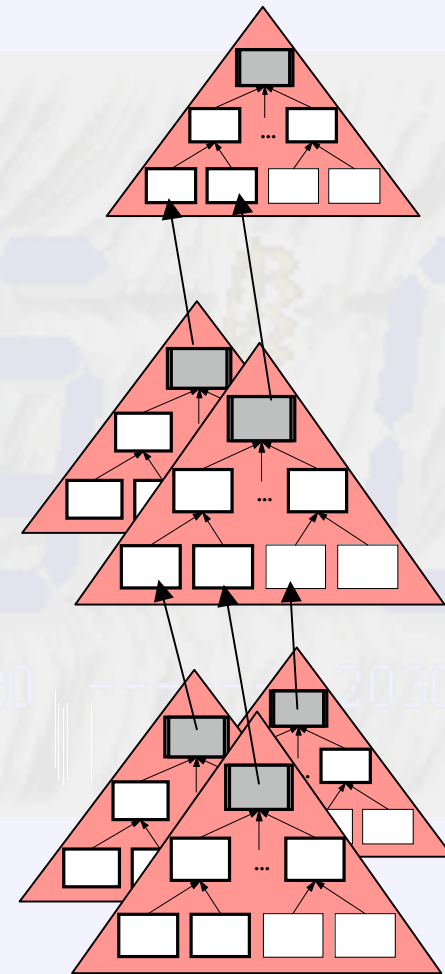
# ArchiSig – Archivzeitstempel

- Zeitstempel für viele Datenobjekte
  - Hashtree (Merkle) + akkreditierter Zeitstempel
  - reduzierbar zu Liste = erneute Signatur
- Eigenschaften
  - signaturgesetzkonform: Zeitstempel mit akkred. Signatur
  - wirtschaftlich: ein Zeitstempel für viele Datenobjekte
  - datenschutzkonform: Löschung von Datenobjekten möglich



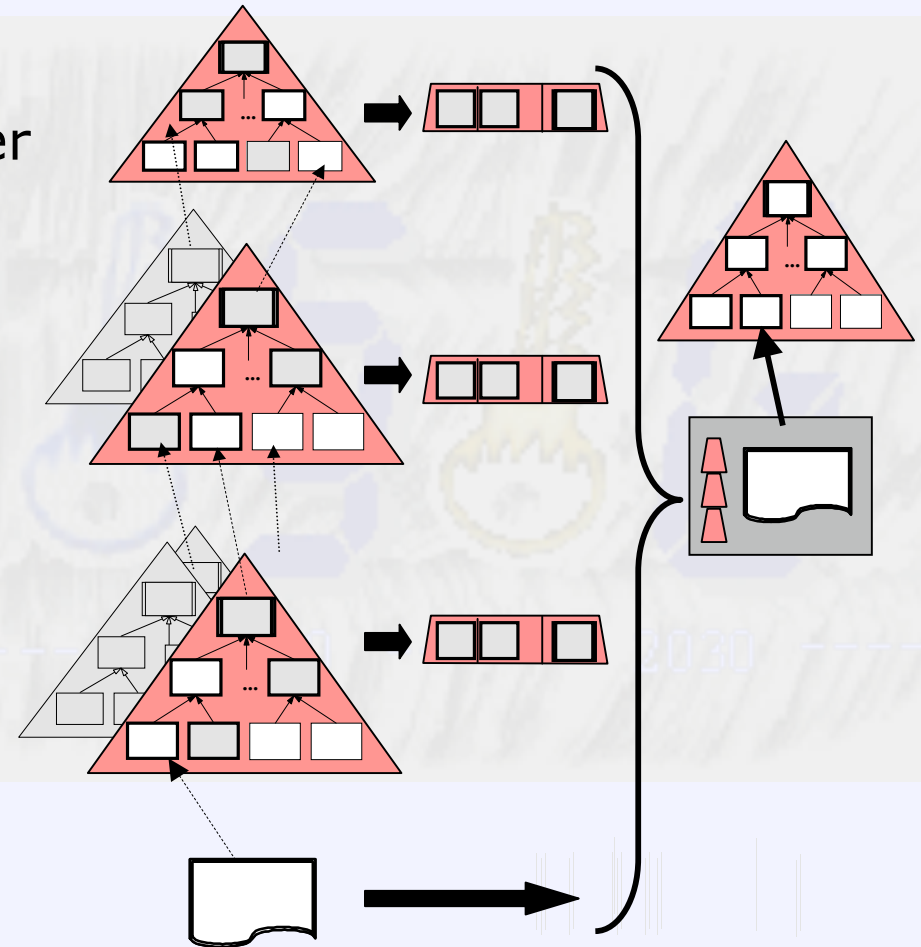
# Zeitstempelerneuerung

- Notwendig, bevor
  - Algorithmus in Zeitstempel unsicher
  - und Zeitstempel ungültig (z.B. USA)
- Für betroffene Archivzeitstempel
  - Zeitstempel erneut archivstempeln
- Kein Zugriff auf Dokumente
  - nur ein neuer Zeitstempel
- Unzureichend nur, wenn Hash-Algorithmus in Baum unsicher



# Hashbaumerneuerung

- Notwendig, wenn Hash-Algorithmus in Baum unsicher
- Für jedes Dokument
  - Archivstempelkette bilden
  - Archivstempel reduzieren
  - mit Dokument in eine Hülle
  - erneut archivstempeln
- Dokumentzugriff erforderlich
  - aber mutmaßlich selten



# ArchiSig-Prototyp

- Erarbeitung von technischen und organisatorischen Konzepten zur
  - Signaturerzeugung
  - Signaturerneuerung
  - Sicherheitseignung kryptographischer Algorithmen
  - langfristigen Sicherung von Verifikationsdaten
  - vertrauenswürdigen Transformation

unter Berücksichtigung des gesamten Lifecycles der digitalen Dokumente (Erzeugung, Signaturerzeugung, Präsentation, Kommunikation, Archivierung, Verwendung)

- Prototypische Umsetzung im Universitätsklinikum Heidelberg durch Entwicklung und Evaluation eines Prototypen
- Integration von ArchiSig-Konzepten in das eGovernment-Projekt des Landes Niedersachsen



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDE  
e-security for e-business

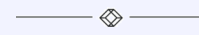
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

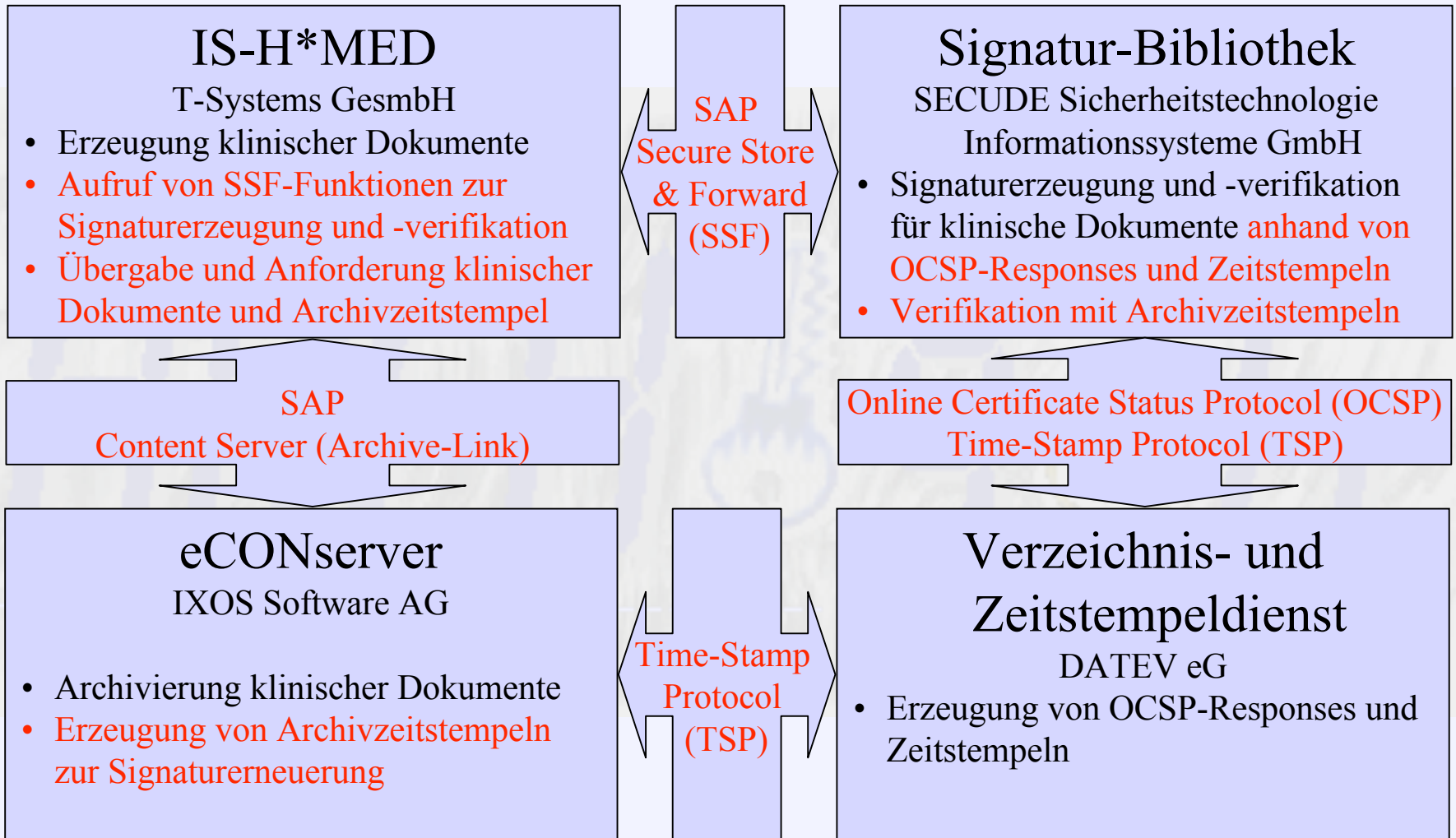


PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
23



# Systemarchitektur für die Lösung des Universitätsklinikums Heidelberg

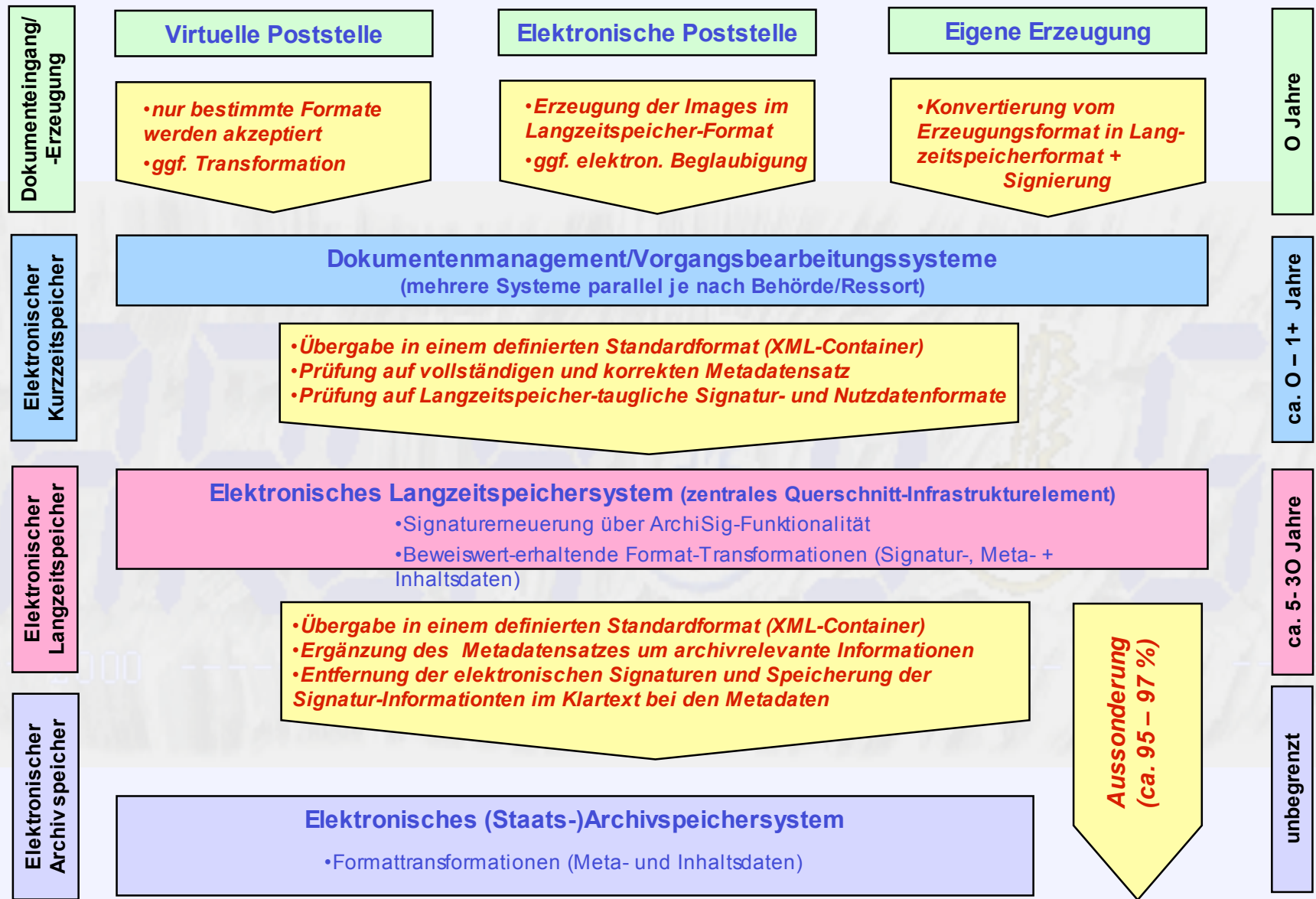




# Architekturmodell des Landes Niedersachsen im Überblick



# Architekturmodell des Landes Niedersachsen



# Zeitstempel und das Geld

- Universitätsklinik Heidelberg
  - 7'000'000 Dokumente pro Jahr
  - 60% sind unterschriftsrelevant → 4'200'000 Dokumente
- Staatskanzlei Niedersachsen
  - 200'000'000 Dokumente pro Jahr
  - 1 % unterschriftsrelevant → 2'000'000 Dokumente
- Signatur-Erneuerung ohne ArchiSig
  - Heidelberg: 4'200'000 Dok. \* 0,30 € → 1'260'000 €
  - Niedersachsen: 2'000'000 Dok. \* 0,30 € → 600'000 €
- Signatur-Erneuerung mit ArchiSig\*
  - Heidelberg (1 ZS pro 1'000 Dok.) 4200 \* 0,30 € → 1260 €
  - Niedersachsen (1x pro Tag): 360 Zeit-Stmp \* 0,30 € → 108 €



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
27

# Evaluation

- Durchführung einer Evaluation anhand des ArchiSig-Prototypen
  - Machbarkeitsstudie
  - Integrations- und Feldtest
  - E-Government-Projekte des Landes Niedersachsen
  - Simulationsstudie zur Prozess- und Beweiseignung



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
28



# Ergebnisse der ArchiSig-Simulationsstudie

- realitätsnahe Gerichtssimulation mit aufbewahrten elektronisch signierten Dokumenten anhand 12 zivil-, straf- und verwaltungsrechtlicher Fälle
- Ziel: Untersuchung elektronisch signierter Dokumente auf ihre Beweiseignung vor Gericht
- ArchiSig-Dokumente erhalten Anscheinsbeweis des § 292a ZPO für Echtheit des Dokuments
- Ohne ordentliche Erneuerung der Signatur freie Beweiswürdigung des Dokuments mit Hilfe von Indizien – unterschiedliche Ergebnisse, keine Rechtssicherheit



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDIGES  
e-security for e-business

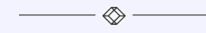
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
29



# Standardisierungsinitiative für Spezifikationen zur Langzeitsicherung qualifizierter elektronischer Signaturen

- Spezifikationen
  - zur Integration erforderlicher Verifikationsdaten in signierte Dokumente
  - zur Signaturerneuerung
  - für die Bestätigung der Sicherheitseignung kryptographischer Algorithmen
- nationale Standardisierungsinitiative mit Unterstützung des ISIS-MTT-Boards
- internationale Standardisierungsinitiative: IETF - Internet Engineering Task Force



## 5. Resümee und Fazit

1. Nachweis erbracht, dass elektronische Langzeitarchive gesetzeskonform, effizient und kostengünstig betrieben werden können, wenn man das ArchiSig-Konzept anwendet.
2. Die prototypischen Lösungen werden in Produkte übernommen und am Markt angeboten.
3. Erste Einsätze der Verfahren in Heidelberg und Hannover.
4. Erfolge bei der Standardisierung.
5. Gewinnung neuer Erkenntnisse, Umsetzung in Folgeprojekten (z. B. E-to-E Transformation: Projekt TransiDoc).



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

UNI KASSEL  
VERSITÄT

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

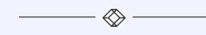
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS



PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
31



# Ausblick

- Überführung der Ergebnisse in Produktentwicklungen und Routineanwendungen verschiedener Branchen und Prozesse
- Fortsetzung der Aktivitäten zur Standardisierung
- Herausgabe des ArchiSig-Buches mit allen Ergebnissen des Verbundprojektes

weitere Informationen: [www.archisig.de](http://www.archisig.de)

Nachfolgeprojekt TransiDoc: [www.transidoc.de](http://www.transidoc.de)



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCSES  
e-security for e-business

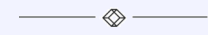
SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

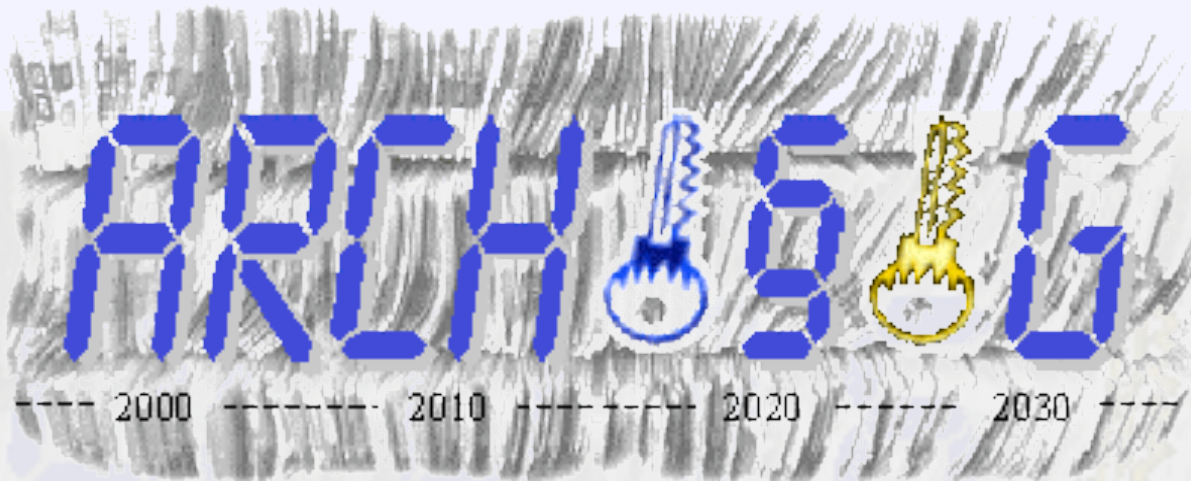


PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
32







**Vielen Dank für Ihre Aufmerksamkeit!**



Universitätsklinikum  
Heidelberg



Fraunhofer Gesellschaft,  
SIT, Darmstadt

U N I K A S S E L  
V E R S I T Ä T

Universität Kassel



Niedersächsische  
Staatskanzlei



IXOS Software AG,  
Grasbrunn (München)

SECUDOCES  
e-security for e-business

SICHERHEITSTECHNOLOGIE  
INFORMATIONSSYSTEME GMBH

SECUDE Sicherheitstechnologie  
Informationssysteme GmbH, Darmstadt



DATEV eG,  
Nürnberg

PERGIS

PERGIS Systemhaus GmbH,  
Ludwigshafen

Folie  
33