

# Datensicherheit in heutigen Gesundheitsanwendungen

---

Peter Pharow  
Bernd Blobel  
Kjeld Engel

eHealth Competence Center Regensburg  
<http://www.ehealth-cc.de>

GMDS-AG „Datenschutz in  
Gesundheitsinformationssystemen (DGI)“  
<http://www.ehealth-cc.de/agdgi>



# Wachsende Anforderungen an Datensicherheit

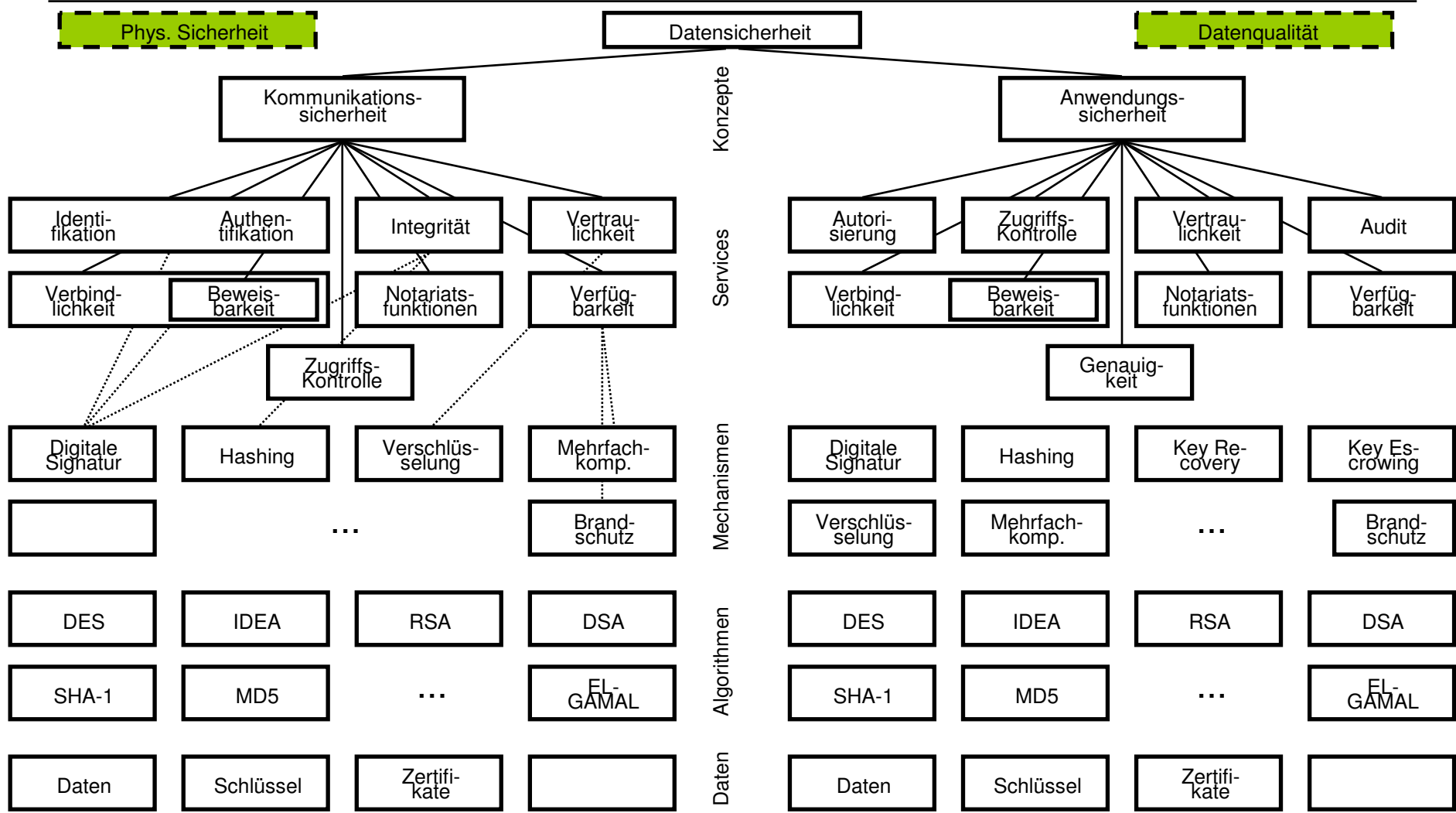
- Vielschichtige Landschaft im Bereich eHealth mit sehr vielen unterschiedlichen Providern, Nutzern und Organisationen (Workflow)
- Wachsende Durchdringung der Domäne eHealth mit nicht-text-basierten Lösungen (MR, CT, Audio, Video usw.)
- Industrieorientierung stark auf globale Standards (Markt)
- Wachsende Anforderungen an sicherer Langzeitspeicherung und Verfügbarkeit digitalisierter (multimedialer) Informationsquellen
- EHR als Zukunftsziel beinhaltet alle Arten und Formen von Daten bzw. Datensammlungen
- Sicherheit, Datenschutz, Datensicherheit, IT-Sicherheit als Herausforderung bei gleichzeitiger leichter Handhabbarkeit der Datensammlungen (GUI)



# Anforderungen an vertrauenswürdige Informations- und Kommunikationssysteme

- Sicherung einer vertrauenswürdigen Kommunikation zwischen authentischen (authentisierten) Principals in vertraulicher Weise zur Gewährleistung der **Kommunikationssicherheit**
- Gewährung nur der erlaubten funktionellen und Datenzugriffsrechte für die autorisierten Nutzer zur Gewährleistung der **Anwendungssicherheit**



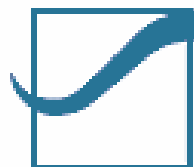
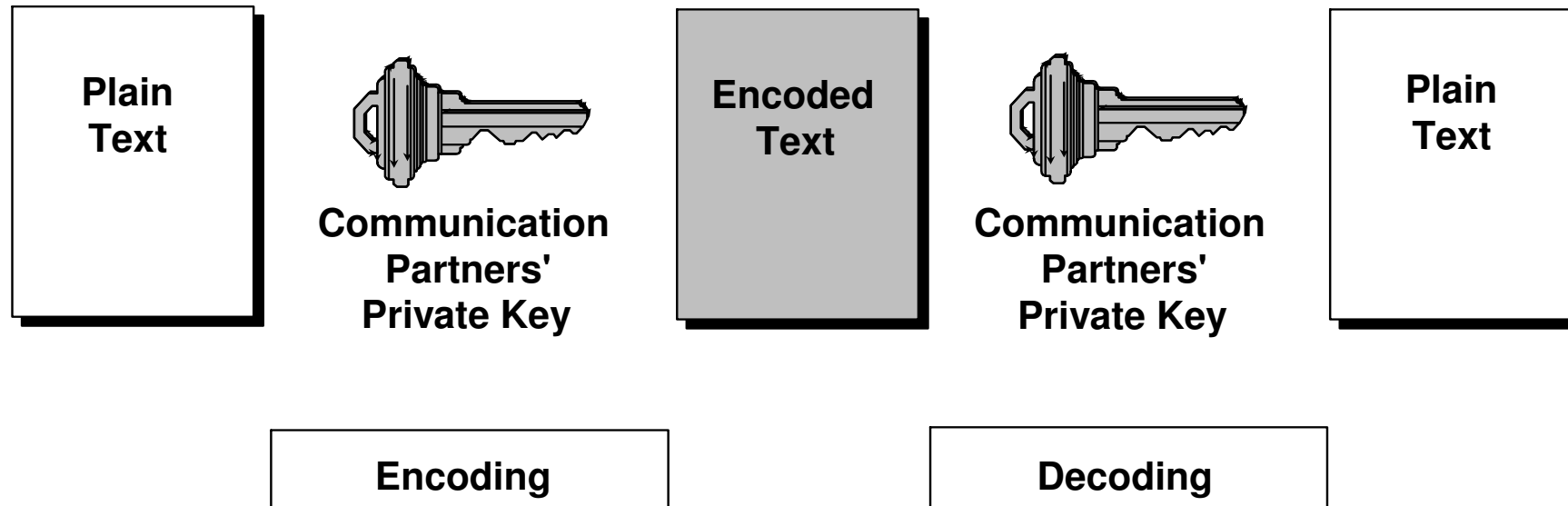


Sender



# Prinzip der symmetrischen Verschlüsselung (Symmetric Key )

Recipient

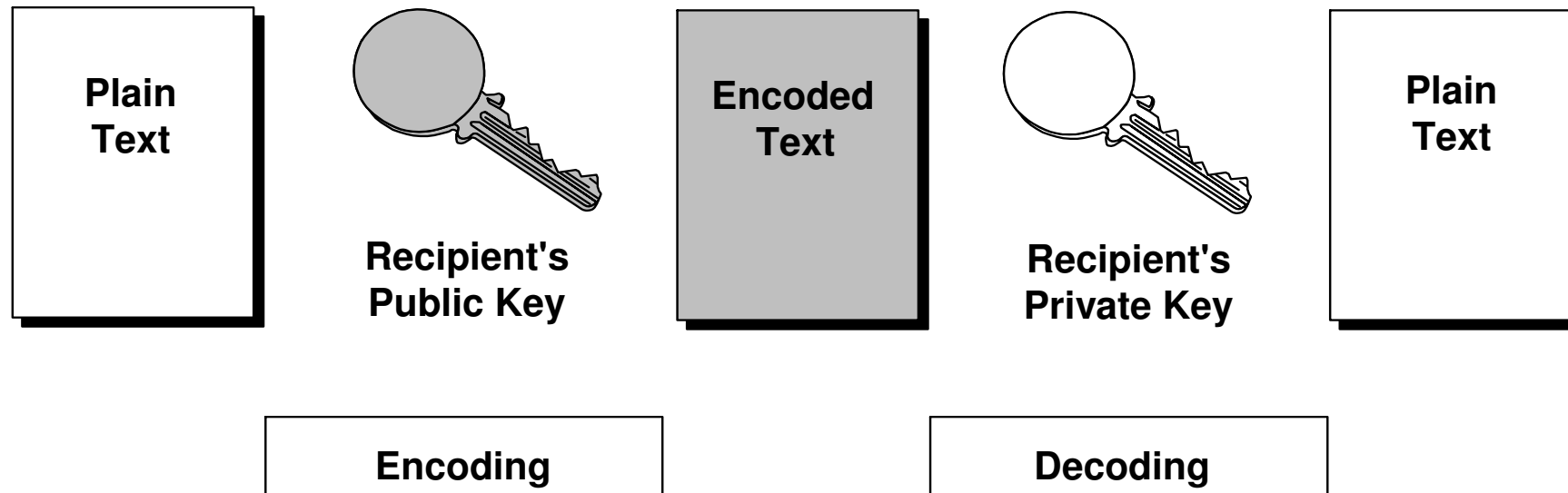


Sender

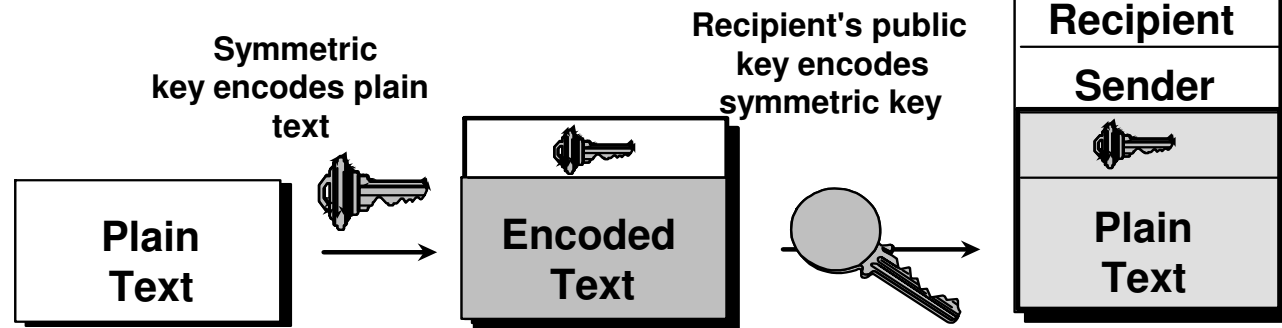


# Prinzip der asymmetrischen Verschlüsselung ( Asymmetric Key)

Recipient

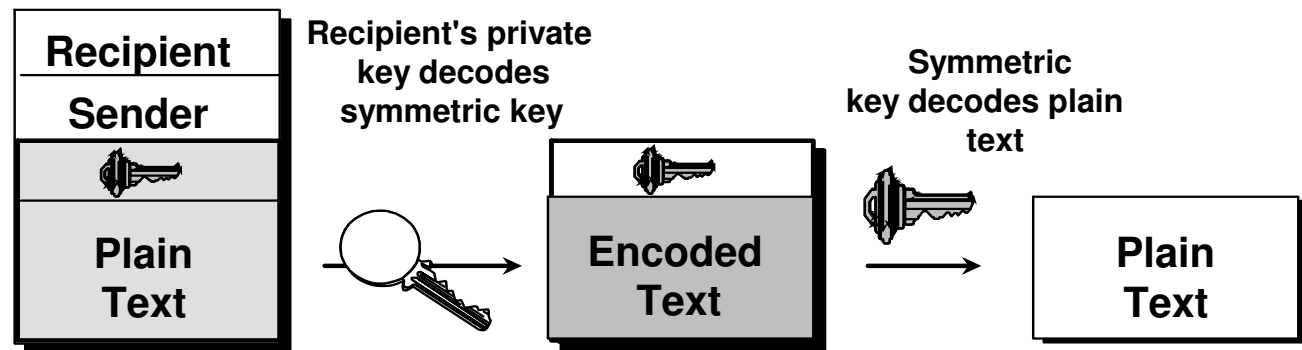


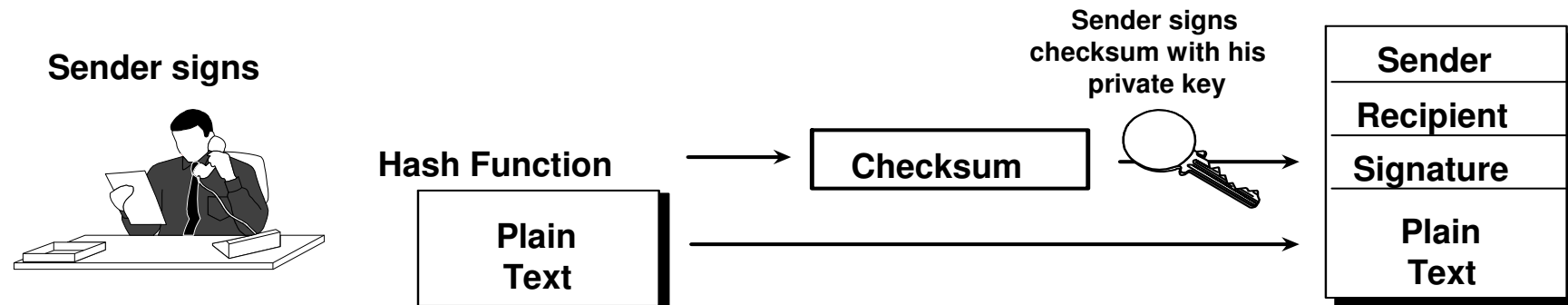
**Sender encodes**



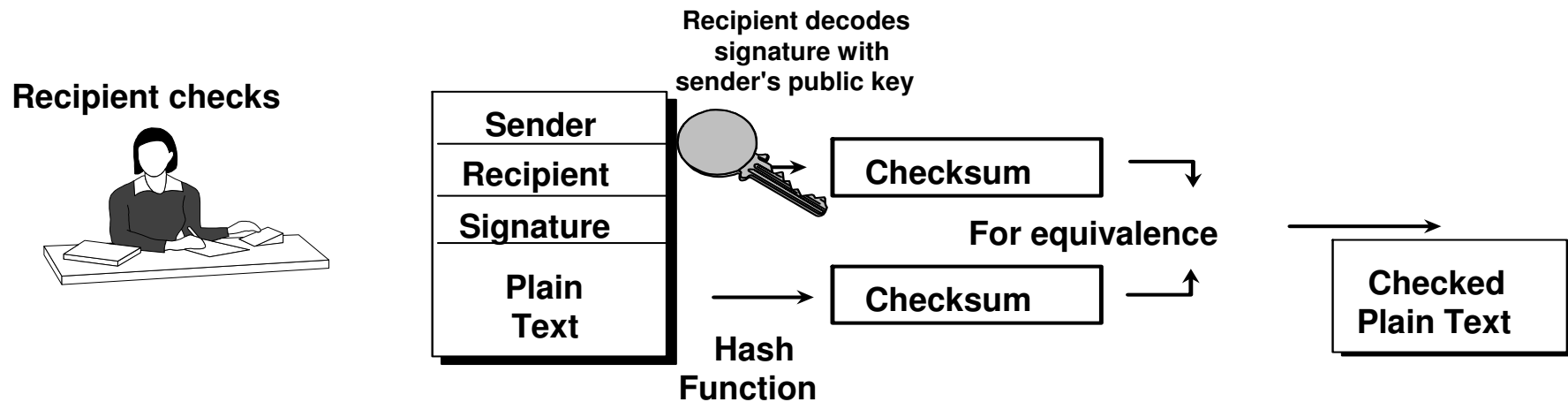
**Hybrid Encryption**

**Recipient decodes**





## Digital Signature



# Authentifikation und andere Dienste

- Wissen
    - Passwort
  - Besitz
    - Chipkarte und PIN
  - Charakteristische Eigenschaften
    - Biometrische Merkmale
- 
- Die Digitale Signaturen sichert die Integrität, Authentizität und Verbindlichkeit von Information
  - Verschlüsselung sichert die Vertraulichkeit von Information
  - Die Kombination beider Dienste sichert Datensicherheit und Datenschutz



# Medizinische Dokumentation

- Elektronische Signaturen (spezifischer: digitale Signaturen), Zeitstempel und Zeit-Signaturen für elektronische Archive einschließlich EHR
- Nachsignieren für technische Integrität und Gültigkeit, nicht für medizinischen Inhalt (Administratoren, TTP, Notare)
- „Re-stamping“ statt „Re-signing“ (qualifizierte Zeit-Signaturen)
- Massen-Signaturen wenn angebracht, auf Grund von gleichen Kontexten, Abhängigkeiten (Delta-Signatur: Gruppe von Items oder Dokumenten)
- Technologische Lösungen, Standards sowie nationale und europäische Gesetze sind verfügbar



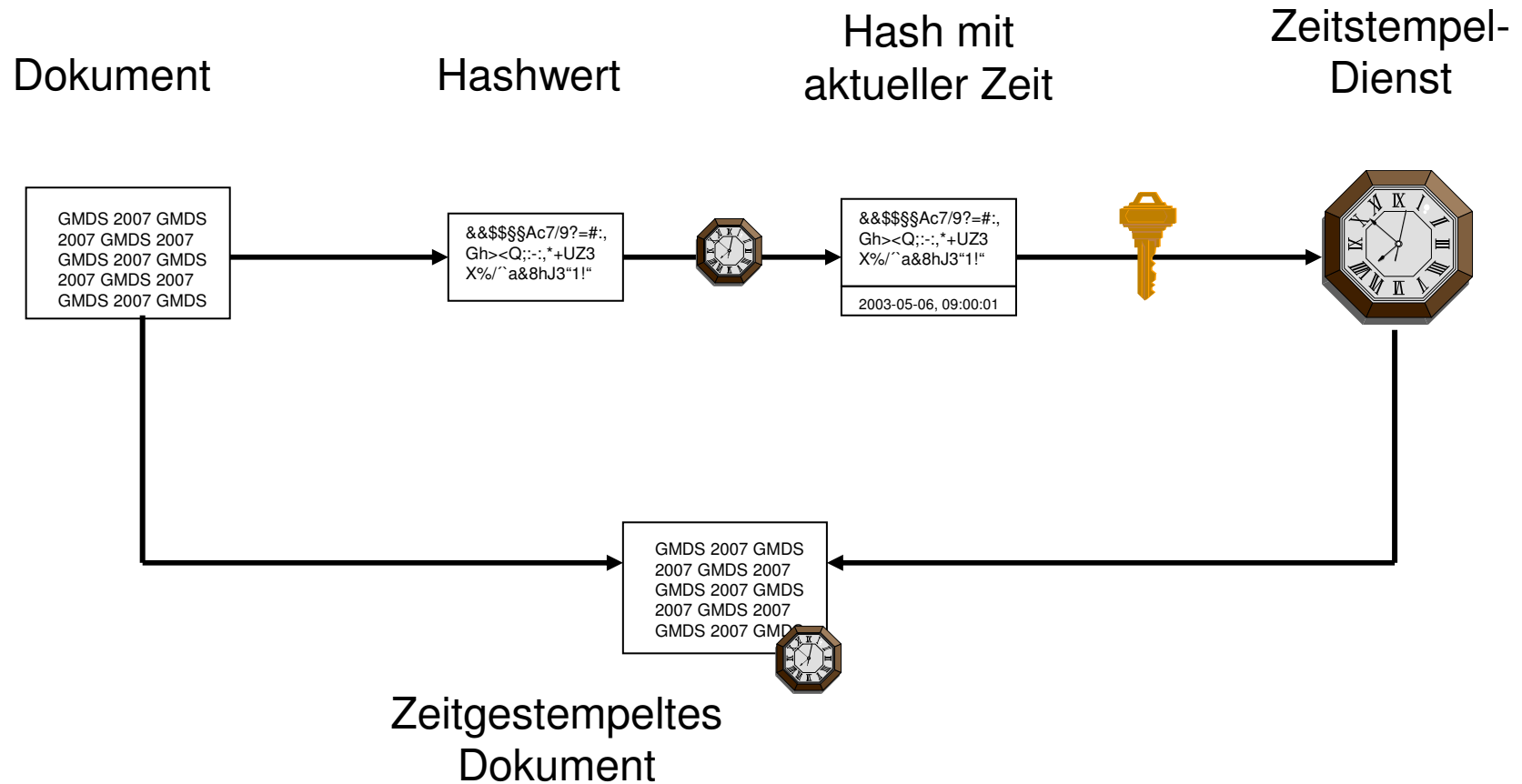
## Zweck elektronischer Signaturen

- Nachweis, dass eine Datei oder ein Record durch eine bestimmte Person erzeugt wurde und unverändert geblieben ist (Hashwert)
  - Verbindlichkeit, Unbestreitbarkeit, Integrität
  - Gleicher rechtlicher Wert wie eine handgeschriebene Unterschrift
  - Nachweis der Absicht, Nachweis der Bereitwilligkeit
  - “Sicherheit” von Kryptologie und Kryptographie im Allgemeinen
  - “Unsicherheit” bzgl. technischer Mittel und deren Parameter
  - Bestimmte Einschränkungen bzgl. der Lebensdauer von Algorithmen
  - Sichere Algorithmen, sichere Zeitstempel, sichere Dienste
  - Langjährige Archiv-Anforderungen, z.B. Bildarchive und EHR bzw. EPA, EFA usw.
- 
- ***Sicherung durch RE-SIGNING: Wer und Wie ??***

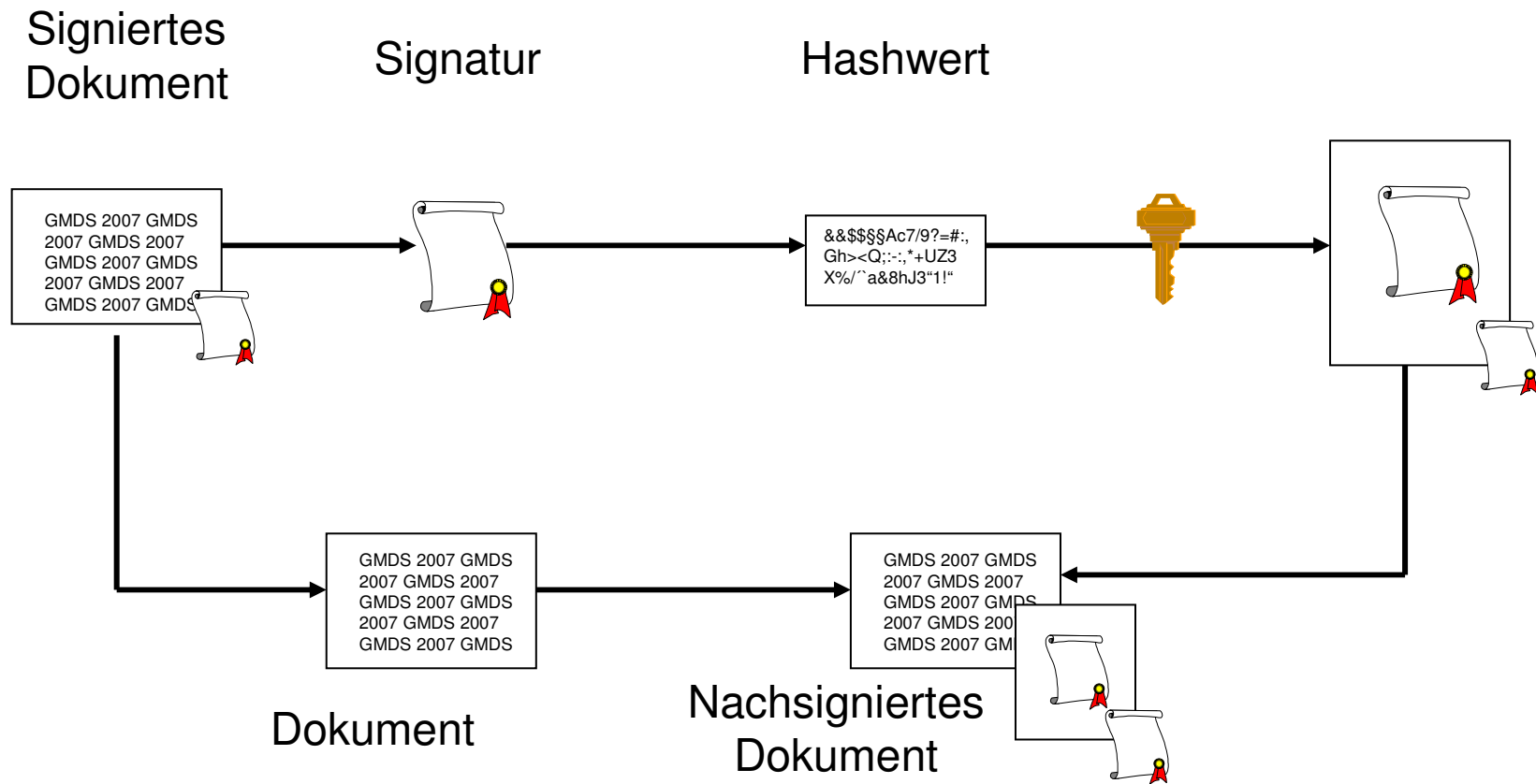




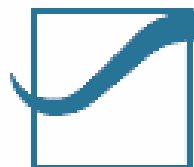
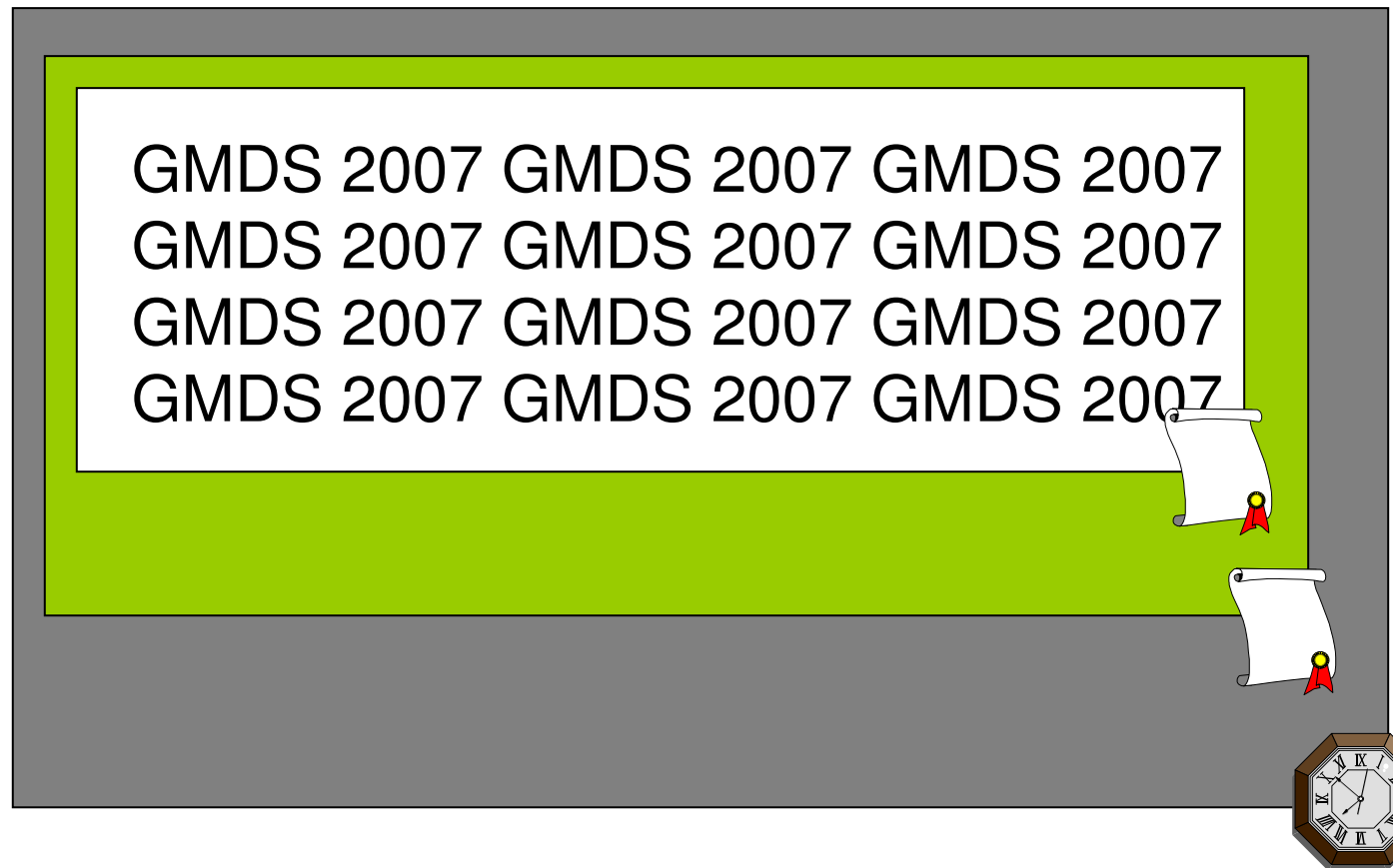
# Zeitstempeln eines gültigen Dokuments



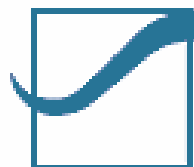
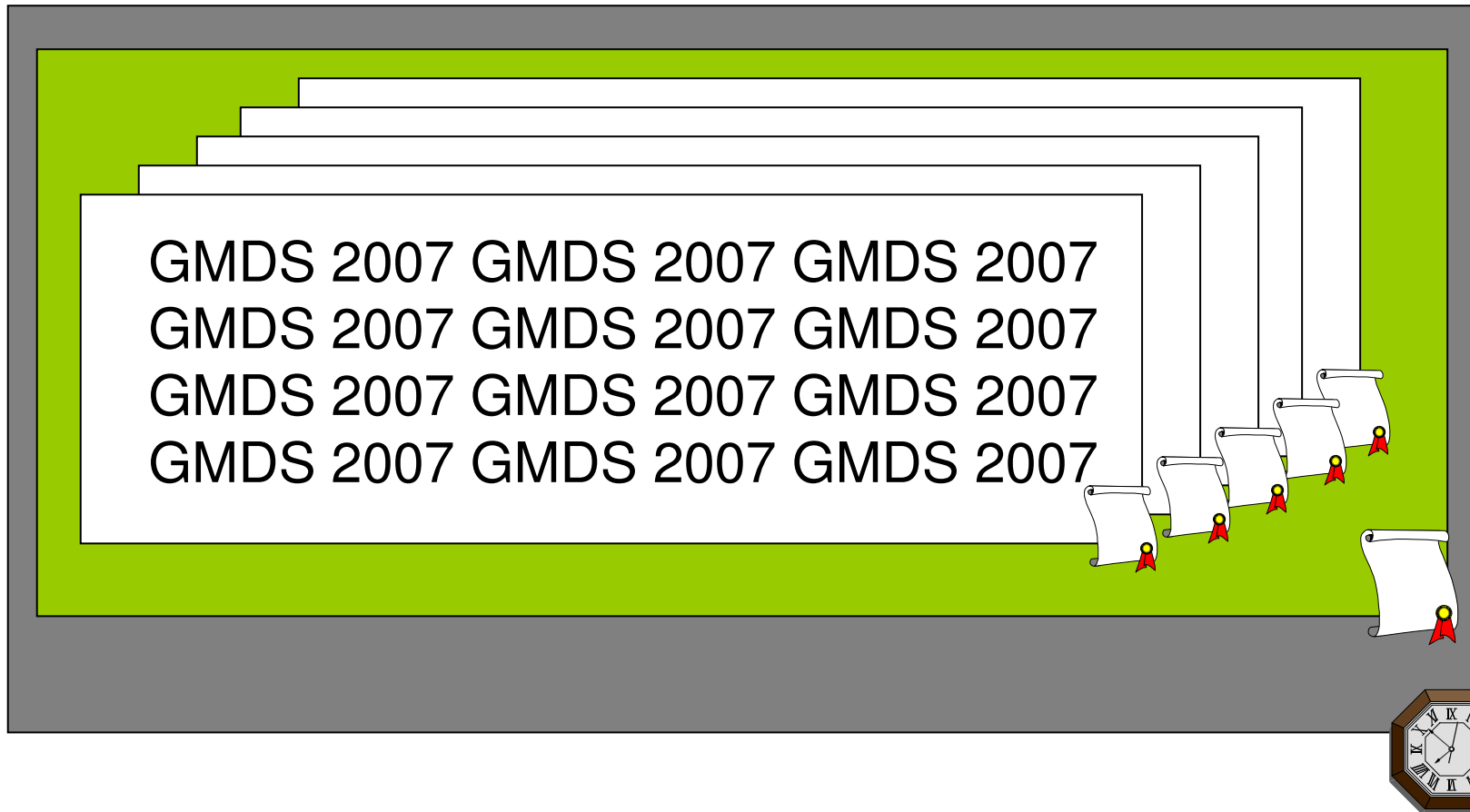
# Nachsignieren eines gültigen Dokuments



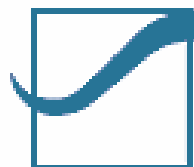
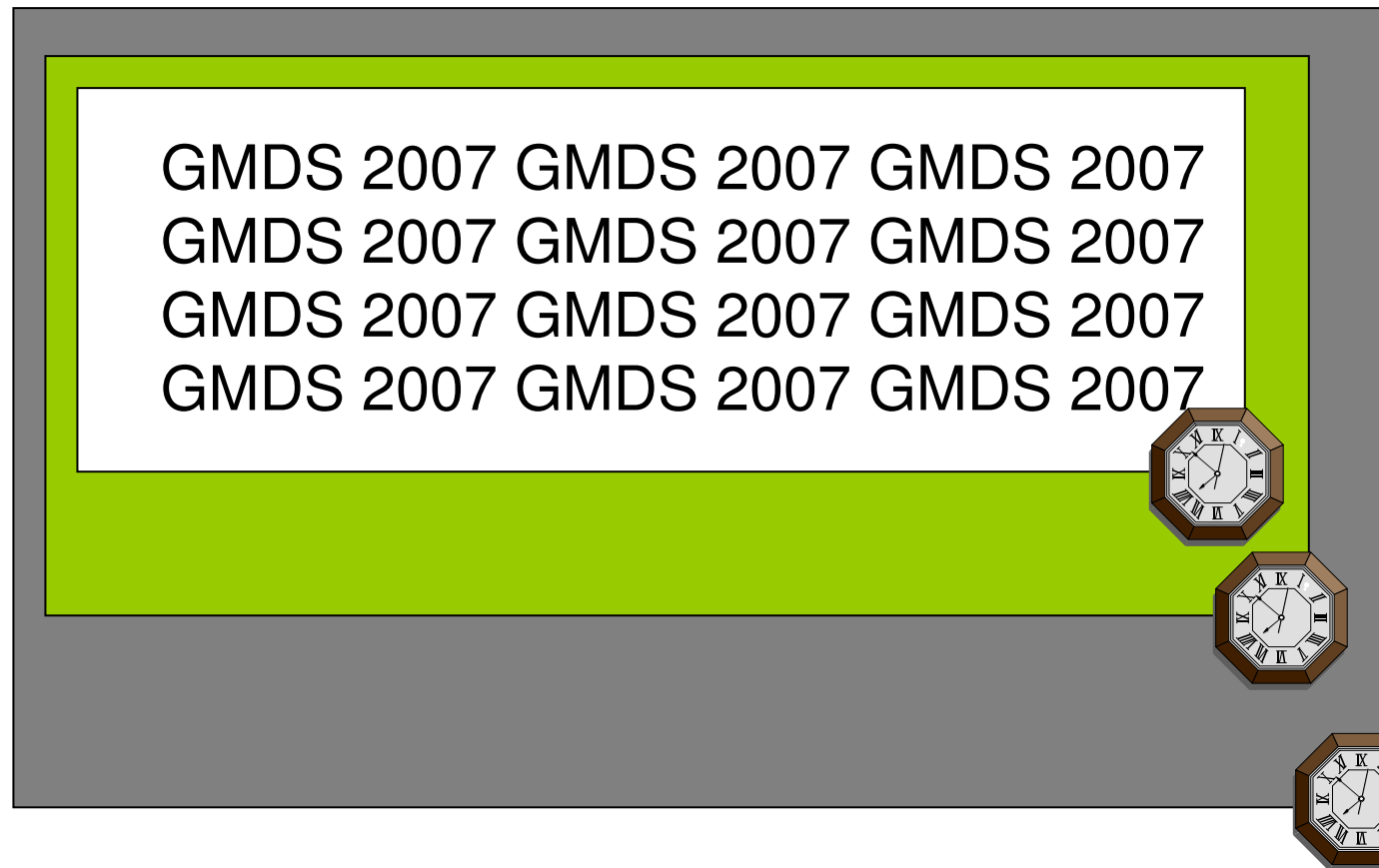
# Nachsignieren gültiger Dokumente



# Massen-Signaturen



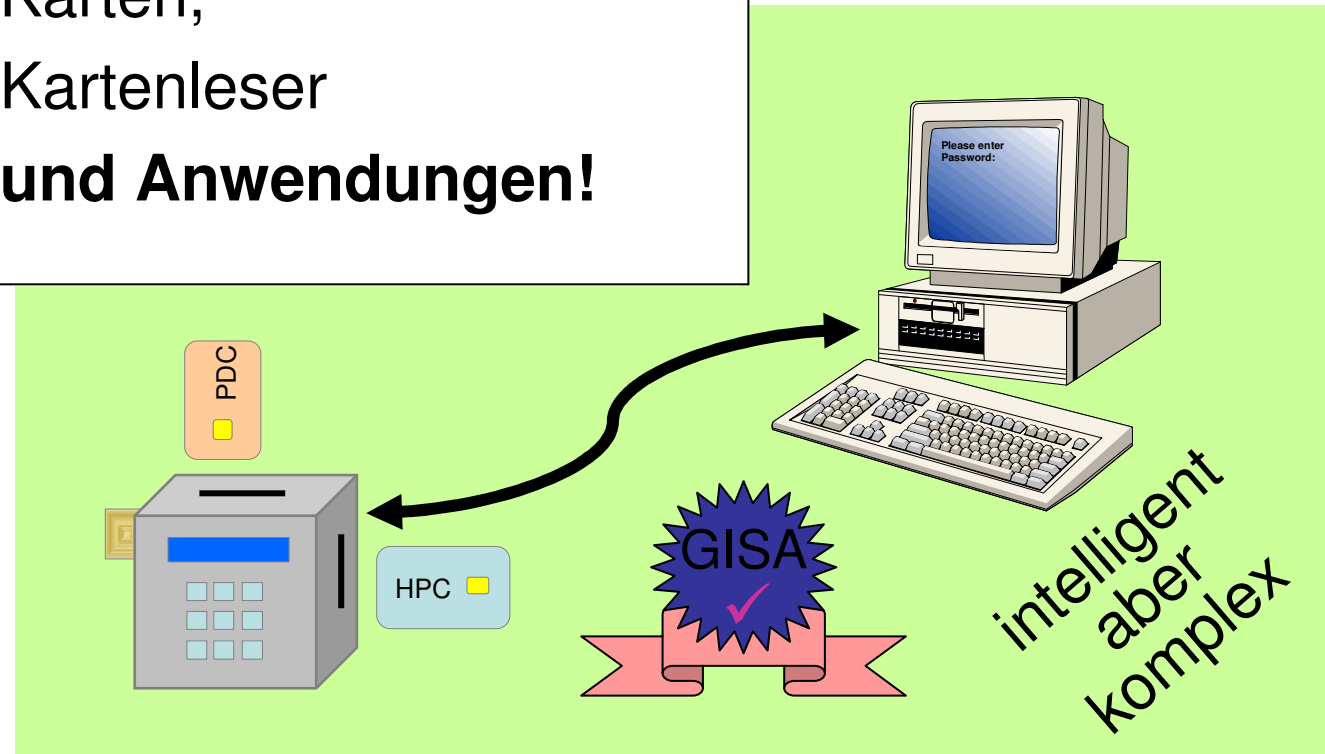
# „Nach-Zeitstempeln“ für Zeitstempel



# eGK-Authentifizierung mit Anwendungssteuerung

Evaluierung & Zertifizierung:

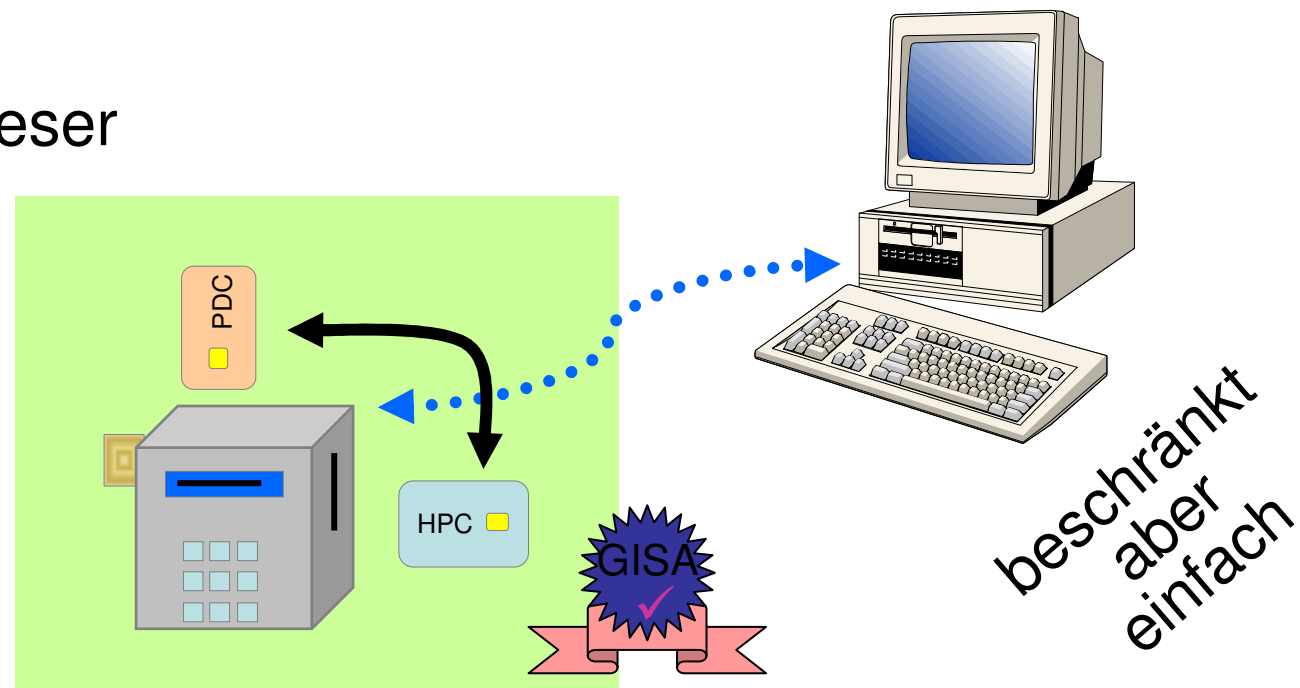
- Karten,
- Kartenleser
- **und Anwendungen!**



# eGK-Authentifizierung mit CV Zertifikaten

Evaluierung & Zertifizierung:

- Karten
- Kartenleser



# Datensicherheit bei multimedialen Inhalten

- Vielfalt an heutigen und künftigen technischen Möglichkeiten
- Kurz- und Langzeitarchive, multimediale Daten, Übertragung
- Einfaches Kopieren und Verändern digitaler Daten
- Keine bis kaum prinzipielle Spuren bei Manipulationen
- Problem der Sicherung der Authentizität der Daten (Integrität des Urhebers, Senders, Besitzers)
- Problem der Datenintegrität (Unverfälschtheit, Unversehrtheit, Aspekt eines Zeitstempels / einer Zeitsignatur)
- Sicherheitsdienste
  - **Integrität:** Erkennung von Änderungen an Medien
  - **Authentizität:** Bestätigte Echtheit von Sender, Empfänger (Verbindlichkeit) und Medium
  - **Zugriffsschutz** und Vertraulichkeit: Eingrenzen des Anwenderkreises über PMAC-Mechanismen



# Umsetzung von Integrität und Authentizität

- Digitale Signaturen bieten
  - Zuordnung von signierendem Kommunikationspartner und digitalem Medium
  - Bitgenaue Gewährleistung der Integrität
- Schwachpunkte
  - Keine feste Verbindung von Signatur und Medium
  - Nach Empfang und Entferne der Signatur: keine Zuordnung
  - Fehlende Lokalisierbarkeit von Manipulationen
  - Keine Aussage über die Stärke der Manipulation



# Aussagekraft digitaler Signaturen



Original



Kontrast erhöht  
(Änderung unerheblich)



Bruch vorgetäuscht  
(Änderung erheblich)

## Umsetzung von Integrität

- Fragile digitale Wasserzeichen
  - Erlauben Lokalisierung und Bewertung der Angriffsstärke
  - Ermöglichen folglich die Unterscheidung von Manipulationen und Nachbearbeitungen
- Schwachpunkte
  - keine vollständige Garantie hinsichtlich der Integrität der Medien
  - Einbetten verursacht minimale Veränderung der Medien
- Herausforderungen
  - Optimierung der Einbettungsparameter
  - Integration in Arbeitsumgebungen



# Aussagekraft fragiler Wasserzeichen



Original



Kontrast erhöht



Bruch vorgetäuscht

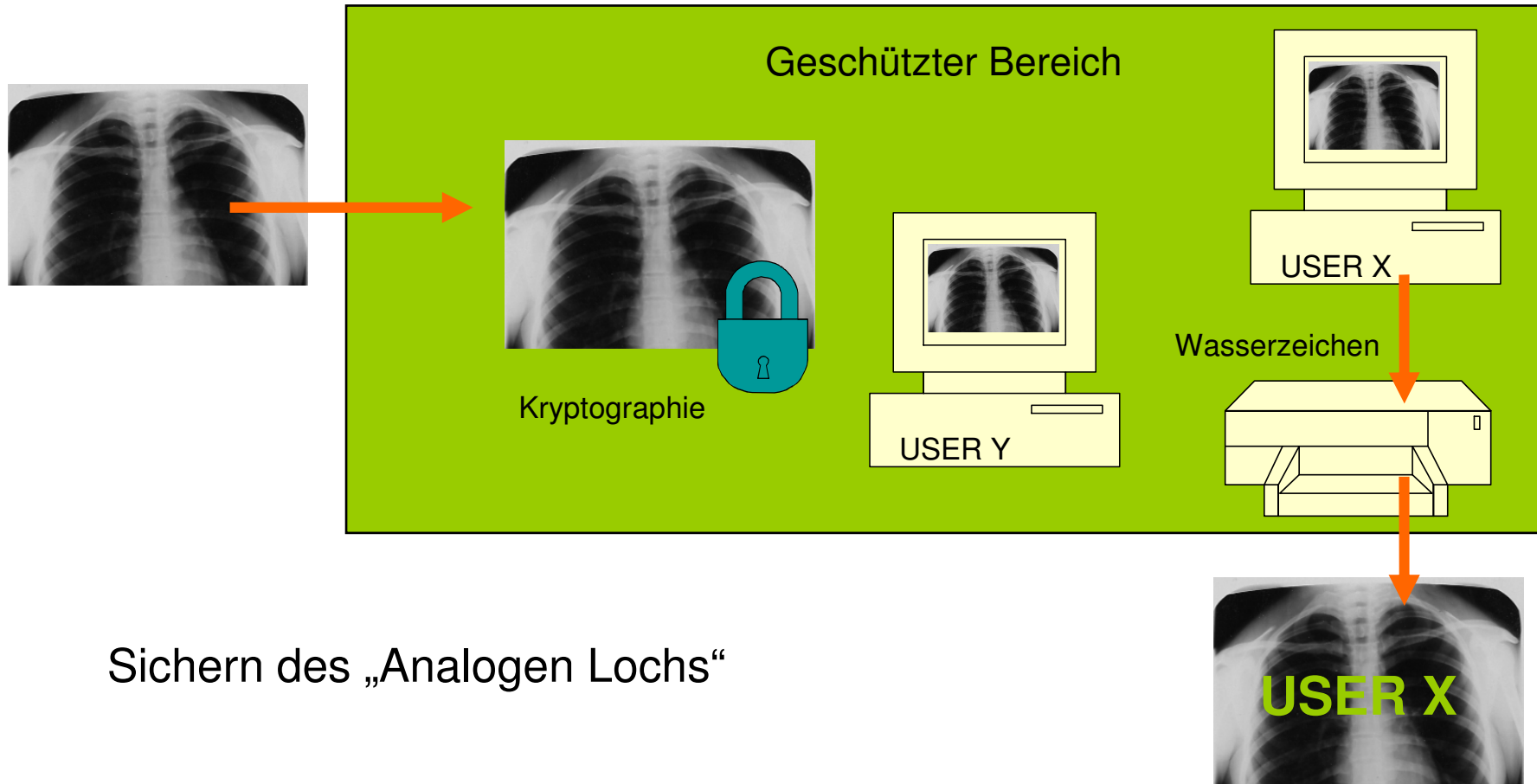


# DRM bei multimedialen medizinischen Daten

- In erster Linie im Bereich des Urheberrechtsschutzes
- Methoden zum Gewährleisten von Authentizität und Zugriffsschutz
- Rechte bezüglich einer Mediendatei
- Möglichkeit des Sicherstellens des Vorhandenseins einer digitalen Signatur für alle relevanten Medien
- Geschützter Transport der Medien zu allen Beteiligten
- Detaillierte Kontrolle über Zeitraum, Personenkreis und Typ der Nutzung der Medien
- Robuste digitale Wasserzeichen als sinnvolle Ergänzung der DRM Umgebung



# Lösungskomponente „fragiles Wasserzeichen“



Sichern des „Analogen Lochs“

## Augsburger Veranstaltungen der AG DGI

- **Dienstag, 18. September 2007, Augsburg, Raum „Musiker 2“ von 14 Uhr bis 17 Uhr: Workshop „ID Management in Anwendungen des Gesundheitswesens (SV 56)“ gemeinsam mit dem europäischen Projekt „BioHealth“; Fortsetzung des thematisch ähnlichen Workshops (Start des Projektes „BioHealth“) von Leipzig 2006 und Vorbereitung des Abschlussworkshops des Projektes in 2008.**
- **Mittwoch, 19. September 2007, Augsburg, Raum „Syndicate 4“ von 9 Uhr bis 12:30 Uhr: Sitzung der GMDS-AG „Datenschutz in Gesundheitsinformationssystemen (DGI)“ als SV 55.**

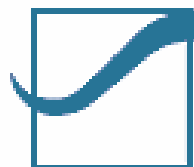
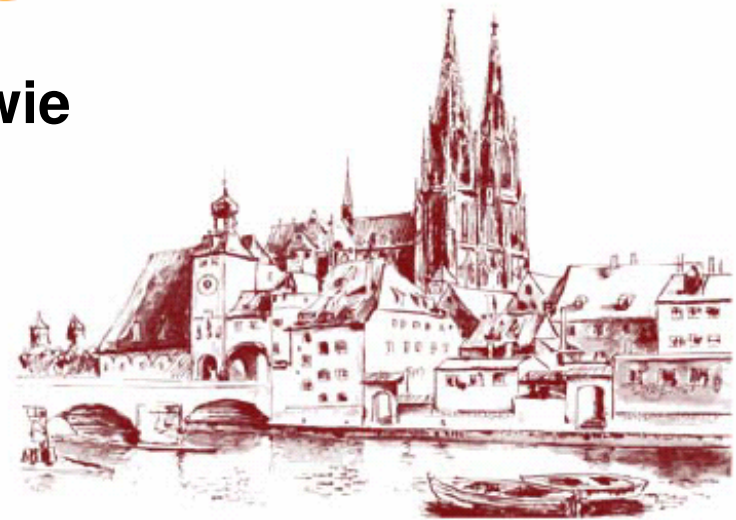


# Announcement

## eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge

**Programm und Registrierung sowie  
weitere Informationen unter  
<http://www.CeHR.de>**

INTERNATIONAL CONFERENCE 2007  
December 2-5, 2007  
REGENSBURG / GERMANY



Fragen und  
Kommentare zu  
diesem Komplex  
bitte an:



- Peter Pharow
- eHealth Competence Center
- Klinikum der Universität Regensburg
  
- Franz-Josef-Strauß-Allee 11
- 93053 Regensburg
- Tel.: +49 (0) 941 / 944 6767
- Fax: +49 (0) 941 / 944 6766
- Email: [peter.pharow@ehealth-cc.de](mailto:peter.pharow@ehealth-cc.de)
- URL: <http://www.ehealth-cc.de>

