Z
D
V

# Public Key Infrastructure
# als Aufgabe des Informationsmanagements

**Dietmar Kaletta**

**Zentrum für Datenverarbeitung**

**Universität Tübingen**

**kaletta@zdv.uni-tuebingen.de**

**DINI-Jahrestagung, Dresden 30.09.2002**

# PKI als Aufgabe des Informationsmanagements

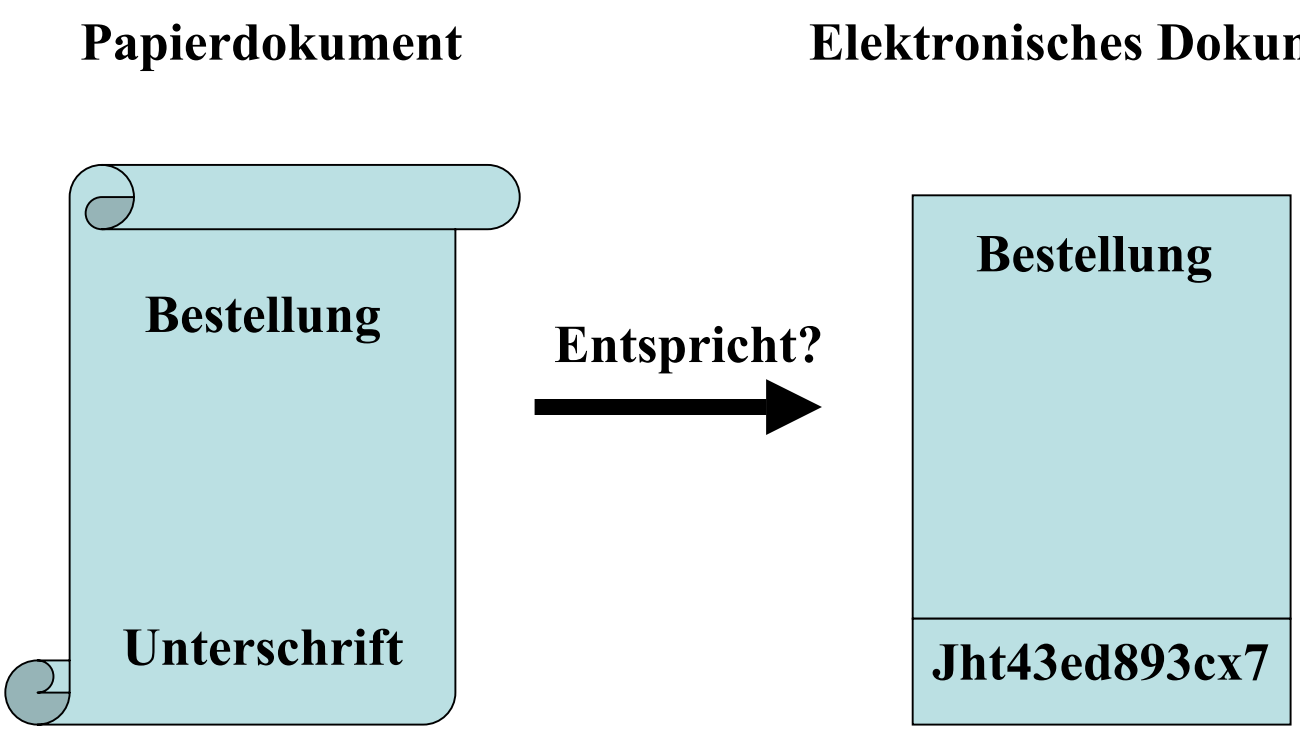


**Inhalt**

- **Einführung: Sicherheit im elektronischen Datenverkehr**
- **Was ist eine Public Key Infrastructure (PKI)? Wozu benötigt man sie?**
- **Rechtliche Grundlagen: Signaturgesetz, Signaturverordnung, Formanpassungsgesetz, EU-Richtlinie**
- **Technische Grundlagen: Kryptoalgorithmen, Interoperabilität, gegenwärtige Standards**
- **Das badenwürttenbergische Landesprojekt PKI/LDAP – eine Herausforderung an das Hochschul-Informationsmanage-ment**

# PKI als Aufgabe des Informationsmanagements





## Papierdokument:

**Ein Papierdokument setzt sich aus seinem Inhalt und seiner (beglaubigten) Unterschrift zusammen. Die Unterschrift soll**

- **die Urheberschaft und**
- **die Integrität und Authentizität des Dokuments**

**bestätigen.**

**Die Vertraulichkeit des Inhalts wird i.d.R. durch die Form seiner Übermittlung charakterisiert (Postkarte, Brief, Kurierdienst, persönliche Aushändigung)**

## Elektronisches Dokument:

**Ein elektronisches Dokument besteht primär aus seinem Inhalt. Für die Sicherstellung der Urheberschaft, Integrität und Authentizität dieses Inhalts ist ein zusätzliches Verfahren erforderlich, das als elektronische oder digitale Signatur bezeichnet wird. Diese Signatur wird dem elektronischen Dokument angehängt.**

**Die Vertraulichkeit wird**

- **entweder durch die Verschlüsselung des gesamten Inhalts *vor* der Übermittlung**
- **oder durch die Form seiner Übermittlung charakterisiert (ungeschütztes IP, geschütztes IPsec) bzw. gewährleistet.**

# Fazit:

**Sicherheit im elektronischen Datenverkehr bedeutet daher**

- **Sicherstellung der Urheberschaft und Integrität der versendeten/empfangenen Dokumente**
- **Sicherstellung der Vertraulichkeit der Inhalte**

**Beide Anforderungen sind grundsätzlich von einander unabhängig und können daher auch getrennt angewendet werden. Da in beiden Fällen das elektronische Dokument softwaremäßig behandelt werden muss, bieten die heutigen gängigen Softwareverfahren beide Möglichkeiten optional an**

# Was ist eine PKI? Warum ist sie notwendig?

**Für die Beglaubigung von Schriftstücken ist auch im üblichen Geschäftsverkehr eine Instanz erforderlich, die die Urheberschaft, Integrität und Authentizität durch Siegelung des Schriftstücks bestätigt (Behörden, in besonderen Fällen Notariate). Auch für die Übermittlung von Schriftstücken gibt es autorisierte und gesetzlich geschützte Verfahren.**

**Elektronische Dokumente können leicht durch den Verfasser, durch den Übermittler und durch den Empfänger manipuliert werden, so dass das traditionelle Beglaubigungs- und Übermittlungsverfahren nicht einsetzbar ist.**

**→ Es ist also eine neue Infrastruktur erforderlich**

# Was ist eine PKI? Warum ist sie notwendig? (2)

**Das traditionelle Signierungsverfahren durch Unterschrift und bei amtlichen Dokumenten die zusätzliche Beglaubigung durch Dienstsiegel wird in elektronischen Dokumenten durch ein elektronisches Signaturverfahren, *Die Digitale Signatur*, ersetzt, so dass die Urheberschaft, Integrität und Authentizität des Dokuments zweifelsfrei und rechtsgültig festgestellt werden können**

# Was ist eine PKI? Warum ist sie notwendig? (3)

**Die *Digitale Signatur* besteht aus vier Schritten**

- **der einmaligen Erzeugung eines Signaturschlüssels (Unterschrift) zur Unterzeichnung beliebig vieler Dokumente**
- **der einmaligen Zertifizierung (Beglaubigung, Dienstsiegel) des Signaturschlüssels**
- **der Signaturbildung für jedes verschickte Dokument mit Hilfe des zertifizierten Signaturschlüssels**
- **der Signaturverifizierung für jedes empfangene Dokument**

**Die ersten beiden einmaligen Schritte stellen die Voraussetzung für die Anwendung des beliebig oft wiederholbaren Signatur-verfahrens aus den beiden letzten Schritten dar**

# Was ist eine PKI? Warum ist sie notwendig? (4)

**Zur Erzeugung des Signaturschlüssels gibt es zwei Verfahren, von den sich das letztere durchgesetzt hat:**

**Im *symmetrischen Schlüsselverfahren* wird ein Schlüssel, der so genannte *geheime* Schlüssel erzeugt, der für die Kodierung und Dekodierung benutzt wird. Problem: Sowohl der Absender wie der Empfänger benötigen den gleichen geheimen Schlüssel**

**Im *asymmetrischen Schlüsselverfahren* wird ein Schlüsselpaar erzeugt, ein so genannter *privater* Schlüssel zur Signaturbildung durch den Absender und ein *öffentlicher* Schlüssel (public key) für die Signaturprüfung durch den Empfänger. Der private Schlüssel bleibt (geheim) beim Absender, der öffentliche Schlüssel wird mitgeschickt oder von einer Stelle verwaltet.**

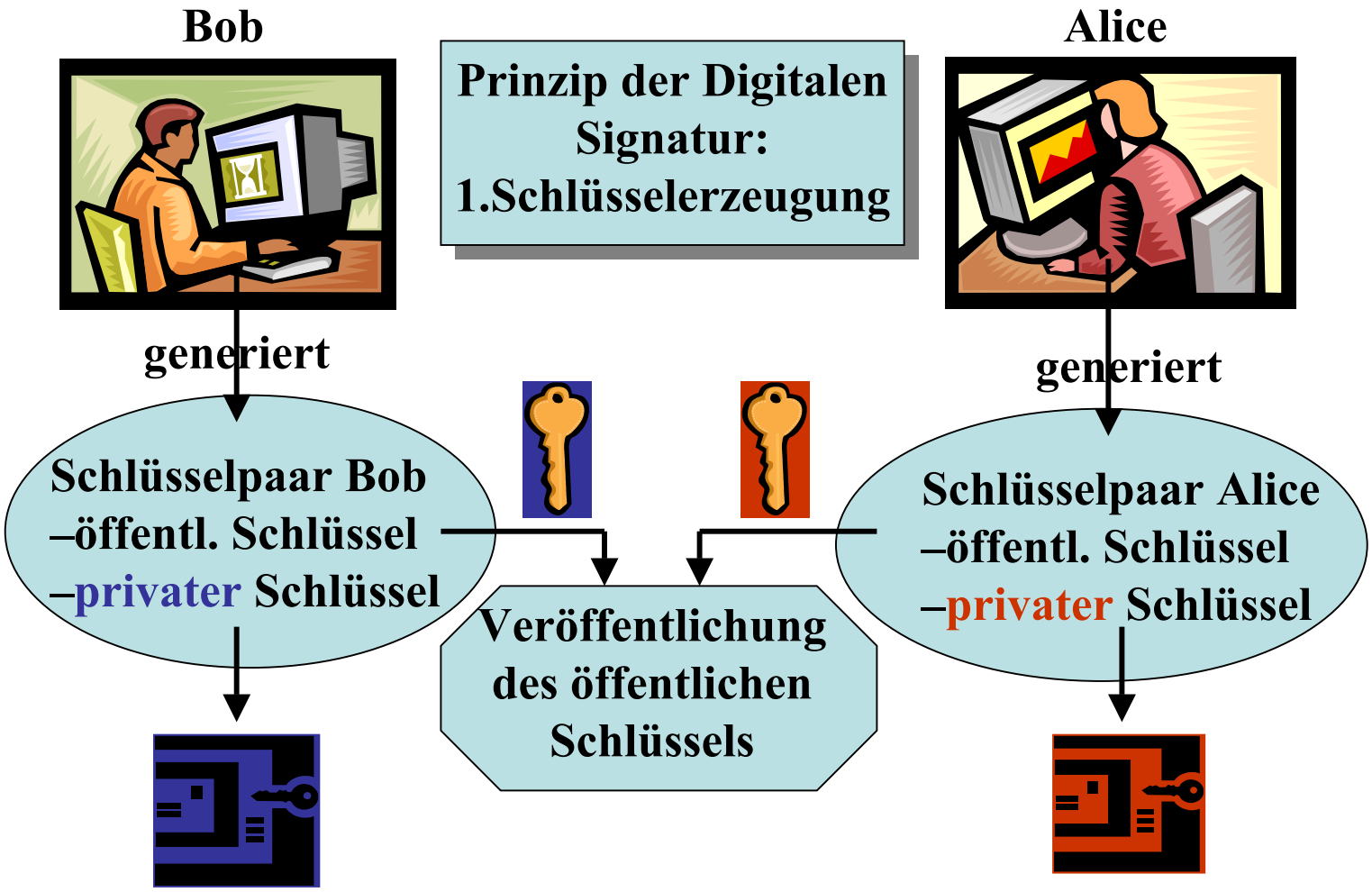
## Was ist eine PKI? Warum ist sie notwendig? (5)

**Eine *Public Key Infrastructure* hat somit die beiden folgenden Aufgaben zu lösen**

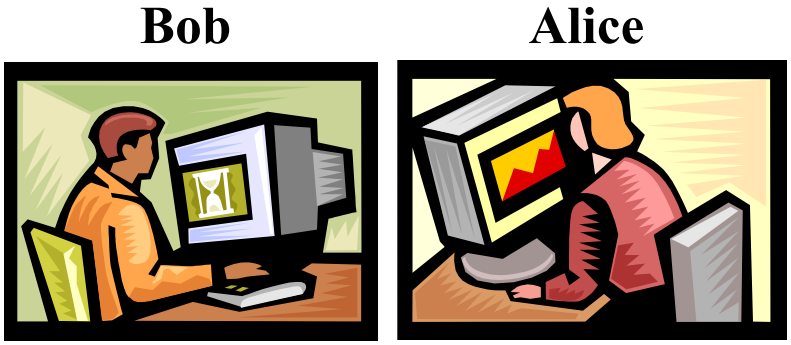
- **die Verwaltung von öffentlichen Signaturschlüsseln**
- **die Sicherstellung, dass der öffentliche Schlüssel zu der Person gehört, die als Eigentümer des öffentlichen Schlüssel (und des damit zugehörigen privaten Schlüssels) ausgewiesen ist (Beglaubigung bzw. Zertifizierung)**

**Eine PKI besteht aus einer oder mehreren Zertifizierungsstellen (Certification Authority, CA) mit den o.g. und weiteren organisatorischen Aufgaben, die sich einem gemeinsamen Regelwerk (Policy) unterworfen haben**

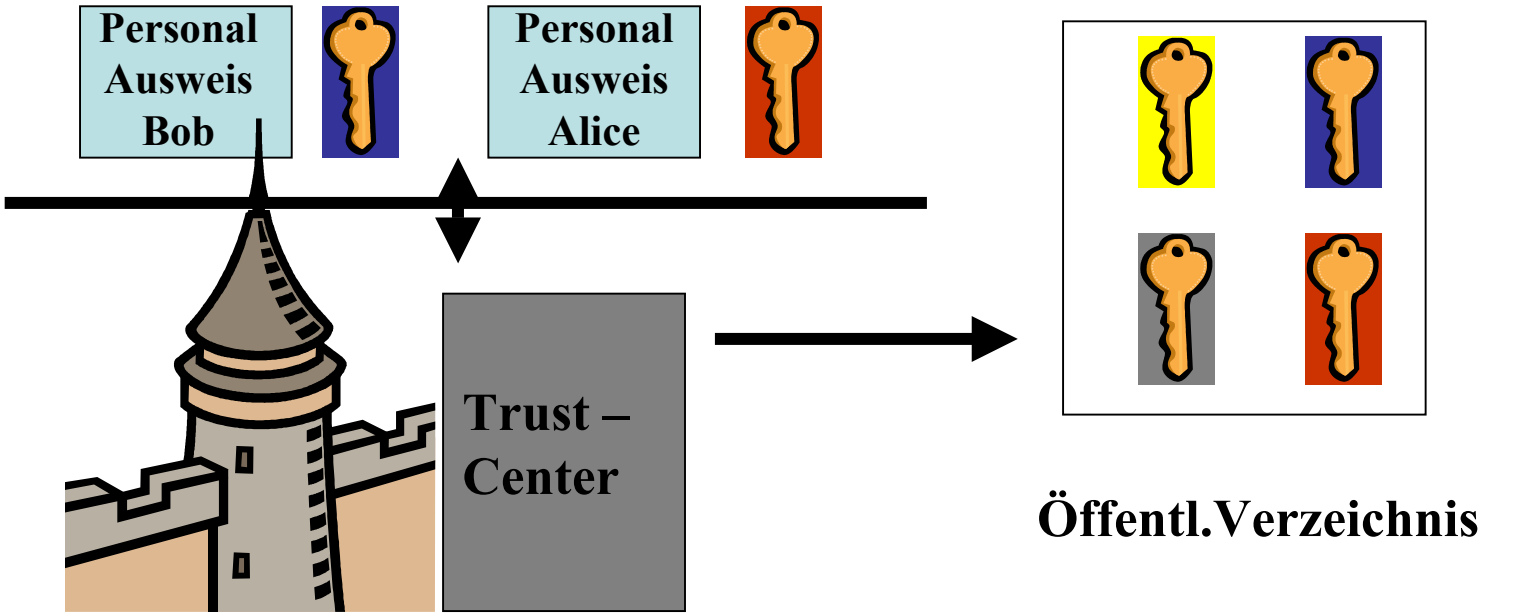
# PKI als Aufgabe des Informationsmanagements



# PKI als Aufgabe des Informationsmanagements




**Prinzip der Digitalen Signatur: 2.Zertifizierung**



## Rechtliche Grundlagen

- **Signaturgesetz SigG vom 16.05.2001 legt die Rahmenbedingungen für die elektronische Signatur fest und definiert die Begriffe wie Signatur, Zertifikat, Signaturschlüssel, Zertifizierungsdiensteanbieter etc.**
- **Signaturverordnung SigV vom 16.11.2001 erläutert explizit die Verfahren für die elektronische Signatur, insbesondere auch die Pflichten der Zertifizierungsdiensteanbieter**
- **Formanpassungsgesetz vom 13.07.2001 regelt die Gültigkeit elektronischer Signaturen im herkömmlichen Rechtsverkehr, indem das BGB entsprechend angepasst wird**
- **EU-Richtlinie vom 13.12.1999 vereinheitlicht die Kommunikation und den elektronischen Geschäftsverkehr innerhalb der EU**

# Rechtliche Grundlagen (2)

**Nach dem SigG ist die RegTP die Wurzelinstanz für die genehmigten Zertifizierungsstellen. Für die meisten Universitäten ist die DFN-PCA die Wurzelinstanz. Alle von der DFN-PCA bis jetzt (09.09.02) ausgestellten Zertifikate sind weder**
**•fortgeschrittene Zertifikate (§ 2 Abs. 2 SigG 2001),**
**•qualifizierte Zertifikate (§ 2 Abs. 3 SigG 2001) noch**
**•akkreditierte Zertifikate (§ 15 SigG 2001).**
**Damit sind digitale Signaturen, die mit einem von der DFN-PCA zertifizierten passenden Schlüssel erstellt wurden, ebenfalls nicht fortgeschritten, qualifiziert oder gar akkreditiert. Die von der DFN-PCA ausgegebenen Zertifikate und digitale Signaturen, die mit einem von der DFN-PCA zertifizierten passenden Schlüssel erstellt wurden, sind "*einfache*" elektronische Zertifikate, bzw. elektronische Signaturen nach § 2 Absatz 1 SigG 2001.**

## Technische Grundlagen

- **Kryptoalgorithmen: Die Stärke einer elektronischen Signatur hängt von den zugrundegelegten Kryptoalgorithmen ab. Für qualifizierte Signaturen müssen sie mindestens für die *kommenden sechs Jahre* als geeignet anzusehen sein**
- **Interoperabilität: Der Erfolg der Einführung einer bundes-weiten PKI für elektronische Signaturen hängt davon ab, dass die unterschiedlichen Implementierungen untereinander operabel sind**
- **Chipkarten: Die missbräuchliche Nutzung des privaten Schlüssels soll durch eine geeignete Besitzform (Chipkarte) und durch Wissen (PIN) verhindert werden. Lösungen sind hier allerdings erst ansatzweise sichtbar**

# Technische Grundlagen (2)

**Die kryptografischen Anforderungen sind in der Anlage 1 des SigV festgelegt und betreffen folgende Algorithmen**

- **Hash-Algorithmus zur Komprimierung des Textes und des geheimen Schlüssels in einen 160-Bit langen Hashwert, den digitalen Fingerabdruck (*Message Digest*). Signiert werden nicht die Daten, sondern der Hashwert (Hash-Funktionen der MD4-Familie sind SHA-1 oder RIPEMD-160)**
- **Signatur-Algorithmus zur Erzeugung des privaten und öffentlichen Schlüsselpaars für die Signierung und Verifizierung der Signatur (RSA, DSA, DSA-Varianten mit Schlüssellängen von mind. 1024 Bit)**

# PKI als Aufgabe des Informationsmanagements

**Dokument**

.....
.....
.....

**Alice**

**Prinzip der Digitalen Signatur: 3.Signaturbildung**

**Hash-Algorith-mus**

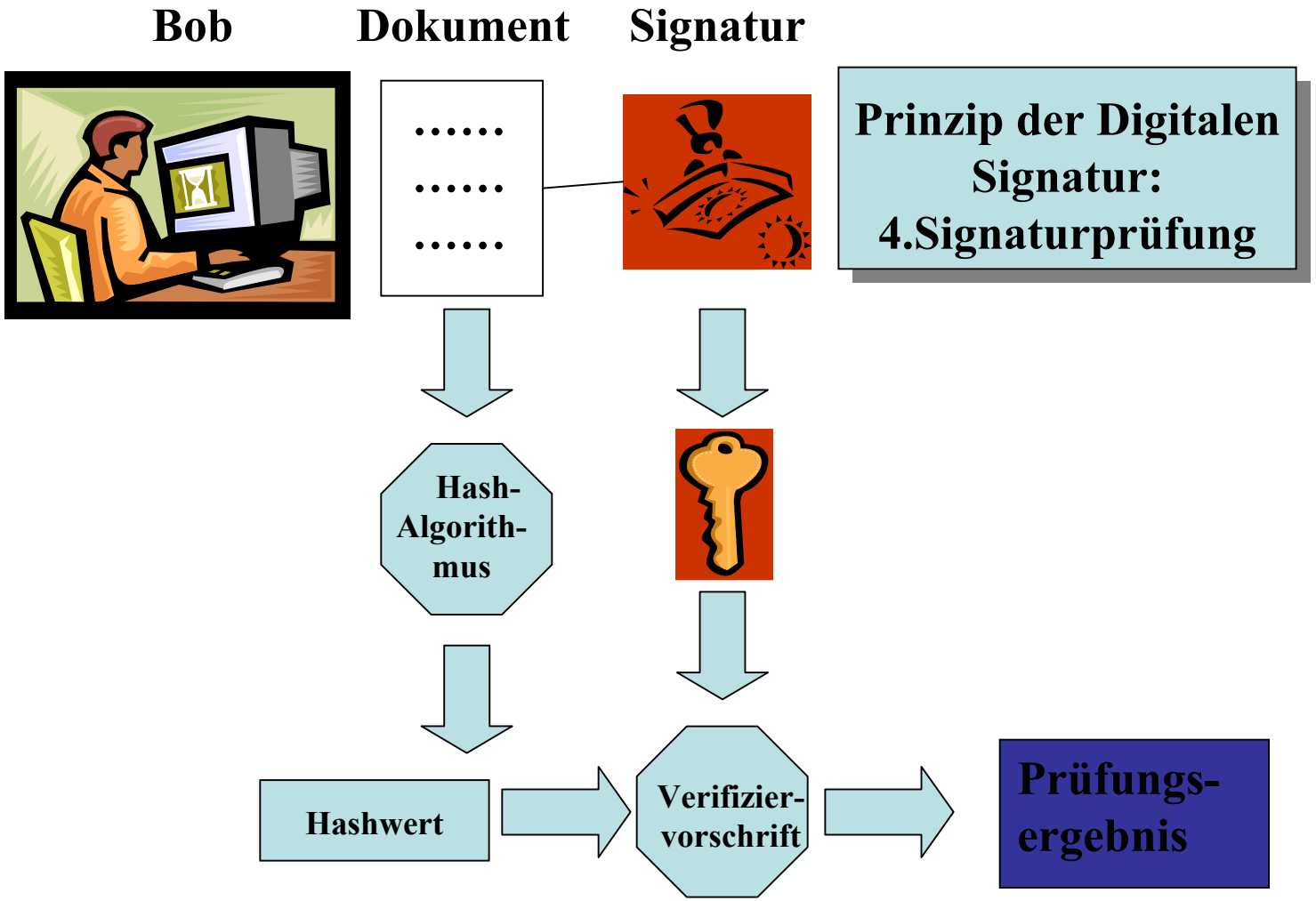
**Signatur**
**=verschlüssel-ter Hashwert**

**Hashwert**

**Signatur-Vorschrift**

Z D V

# PKI als Aufgabe des Informationsmanagements



## Interoperabilität am Beispiel von E-Mail-Programmen

**Gegenwärtig sind zwei Methoden für die Versendung sicherer E-Mails von Bedeutung: S/MIME und PGP. Beide Verfahren sind zueinander inkompatibel, so dass der Kommunikationspartner das gleiche Verfahren benutzen muss. Folgende Voraussetzungen sind erforderlich:**

- **Die E-Mail-Programme MS Outlook bzw. MS Outlook Express oder Netscape Messenger**
- **Bei Nutzung von S/MIME muss keine spezielle Software installiert werden. S/MIME ist in MS Outlook bzw. MS Outlook Express und Netscape Messenger schon enthalten. Allerdings ist vor der Nutzung eine Zertifizierung des Benutzers durch eine Zertifizierungsstelle (Uni-CA, web.de, Deutsche Telekom etc.) erforderlich.**
- **Bei Nutzung von PGP muss die PGP-Software installiert werden, die frei verfügbar ist. Eine Zertifizierung über eine Zertifizierungsstelle ist nicht erforderlich, da das Schlüsselpaar selbst erzeugt werden kann**

## Interoperabilität (2)

| Mandatory features | S/MIME v3 | OpenPGP |
|---|---|---|
| **Message format** | Binary, based on CMS | Binary, based on previous PGP |
| **Certificate format** | Binary, based on X.509v3 | Binary, based on previous PGP |
| **Symmetric encryption algorithm** | TripleDES (DES EDE3 CBC) | TripleDES (DES EDE3 Eccentric CFB) |
| **Signature algorithm** | Diffie-Hellman (X9.42) with DSS | ElGamal with DSS |
| **Hash algorithm** | SHA-1 | SHA-1 |
| **MIME encapsulation of signed data** | Choice of multipart/signed or CMS format | multipart/signed with ASCII armor |
| **MIME encapsulation of encrypted data** | application/pkcs7-mime | multipart/encrypted |

# BW-Landesprojekt PKI/LDAP

- **Thema: Landesweite PKI auf Basis von indizierten Verzeichnisdiensten mit LDAP-Zugriffsmechanismen**
- **Projektdauer: 24 Monate**
- **Personal: 15 Mannjahre**
- **Ziele**
  - **Schaffung einer Infrastruktur für den Einsatz Digitale Signatur**
  - **Sichere und vertrauliche Kommunikation für Personen und Maschinen**
  - **Ausstellung von Echtheitszertifikaten (Urheberrecht, Fälschung)**
  - **Authentifizierung von Personen zur Nutzung von DV-gestützten Ressourcen (Schriftverkehr mit Prüfungsämtern, I-Ämtern etc.)**

# Zusammenfassung



- **Die Einführung einer PKI ist weniger eine technische, sondern in erster Linie eine organisatorische Herausforderung**
- **Die Abbildung der Organisationsstrukturen (Hochschulen, Verwaltung etc) auf eine Verzeichnisstruktur (LDAP) mit Authentifizierung der Teilnehmer ist sehr personalaufwendig**
- **Aufgabe des Informationsmanagement muß es daher sein, die Notwendigkeit und die Vorteile einer solchen Infrastruktur den Leistungsträgern vor Augen zu führen**
- **Der Anspruch auf Rechtsgültigkeit der Digitalen Signatur im jeweiligen Geschäftsbereich wird den entscheidenden Einfluss auf die jeweilige Form der zu etablierenden Infrastruktur haben**
- **Die Vertraulichkeit (Verschlüsselung) von Informationen steht nicht im Vordergrund, sondern ihre Echtheit bzgl. des Inhalts und des Absenders**