



Authentizität und Langzeitarchivierung

Frank Scholze

Universitätsbibliothek Stuttgart

Workshop

**“Langzeitverfügbarkeit digitaler Dokumente –
Erarbeitung eines ersten kooperativen Konzepts für
Deutschland”**

Frankfurt/Main, 30.10.2002



Authentizität

- Authentizität - Zuordnung von Dokumenten zu dem darin bezeichneten Absender bzw. Verfasser
- Integrität - Keine undokumentierten Änderungen möglich
- Authentizität sagt nichts über den Inhalt aus
- Dokument - inhaltlich: Durch den Autor (?) bestimmte abgeschlossene Informationseinheit
- Dokument - technisch: Besteht aus fundamentalen Datentypen (Text, Zeichnung, Festbild, Ton etc.)



Sicherung des Dokumentenservers

- Sicherster Ansatz: Keine Netzverbindung zum Server möglich – in der Praxis nicht realisierbar
- Trotzdem: Trennung in Dokumentenspeicher und Depotserver mit ggf. unterschiedlichen Sicherheitsstufen
- Der Server sollte zertifiziert sein
- Der Server sollte nur über verschlüsselte Verbindungen (z.B. SSL) erreichbar sein
- Die Maßnahmen zum Schutz des Servers sollten veröffentlicht sein (policy)



Sicherung des Dokumentenservers II

- Eingeschränkter Zugang zum Server:
 - Administration des Servers ausschließlich durch einen autorisierten (möglichst kleinen) Personenkreis
 - Nachweis der Administrationsaktivitäten
 - Physischer und softwaremäßiger Zugriffsschutz
 - Registrierung und Kontrolle der Zugriffe
 - Regelmäßige Datensicherung und Konsistenzprüfung

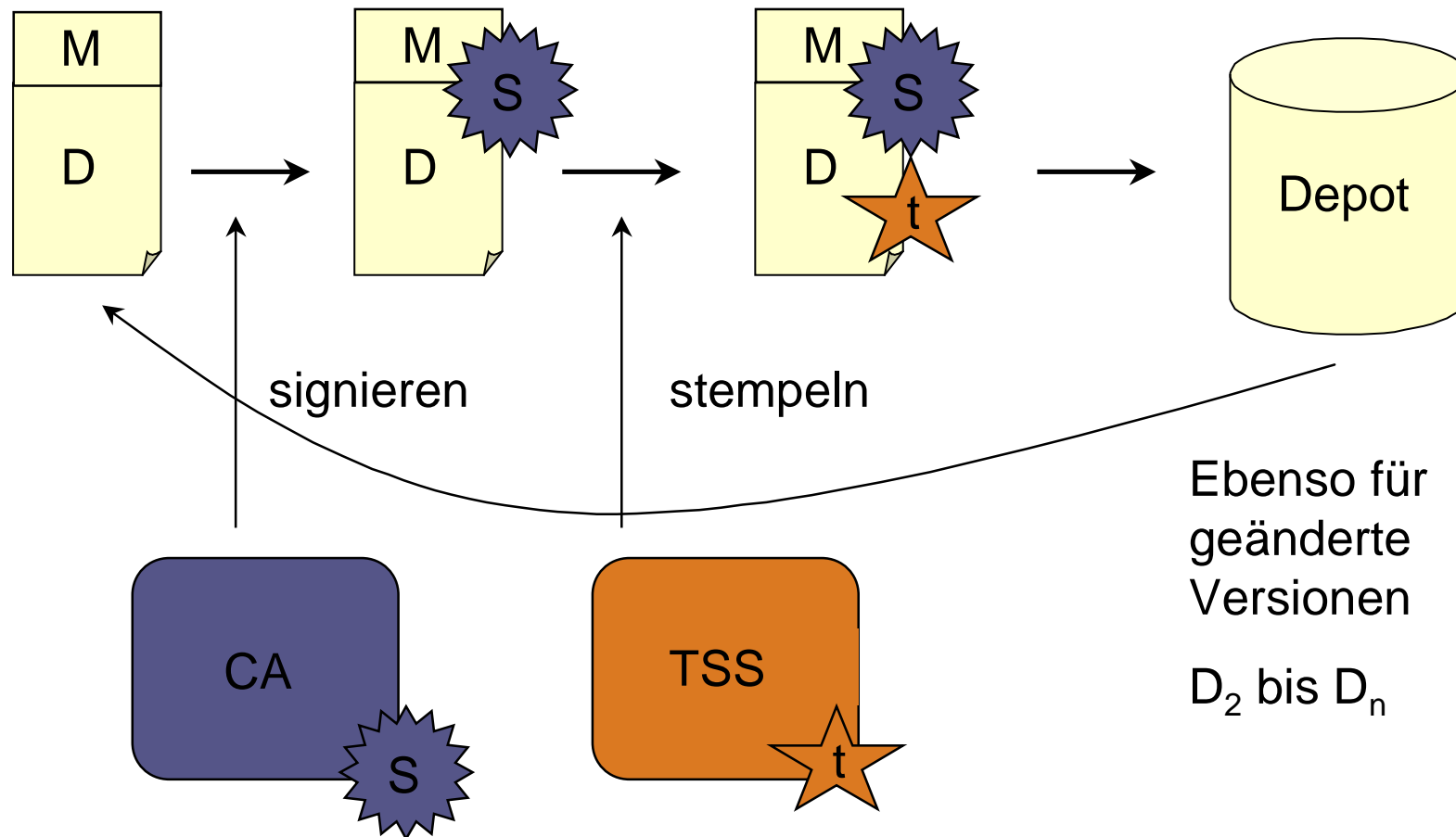


Sicherung einzelner (Teil-)Dokumente

- Die Authentizität und Integrität digitaler Dokumente muss stets nachweisbar sein
- Wenn Änderungen notwendig wurden, muss das geänderte Dokument als neue (dokumentierte) Version abgelegt werden
- Einsatz von digitalen Signaturen, d.h. einer Public Key Infrastruktur, und Zeitstempeln
- Trustcenter (TeleSec, Signtrust etc. DFN-PCA bislang nicht konform zum Signaturgesetz)



Sicherung einzelner (Teil-)Dokumente II





Zeitstempeldienst

- Zeitstempeldienst (Time Stamping Service – TSS), ordnet die Signaturen nachprüfbar ihrem Erstellungsdatum zu
- Zeitstempeldienste bieten eine zusätzliche Sicherheit gegenüber digitalen Signaturen, da sie keine geheime Komponente besitzen, die passwortgeschützt sein muss
- Beispiele: TIMESEC (Leuven), PKITS (Spanien)



Langfristige Verfügbarkeit digitaler Zertifikate

- Falls die ursprünglich verwendeten Signaturen technisch nicht mehr sicher sein sollten, müssen die Dokumente mit neu zertifizierten, technisch sicheren Signaturen nachsigniert werden
- Falls die Stelle, die das entsprechende Wurzelzertifikat ausgestellt hat nicht mehr existiert, muss die Existenz und Überprüfbarkeit der damit erzeugten Signaturen für digitale Dokumente weiter gewährleistet sein
- Dies kann in Form eines Digitalen Schlüsselarchivs geschehen (Key Archival Service – KAS)



Ausblick

- Policy aufstellen und implementieren
- Aufbau bzw. Nutzen einer Public Key Infrastruktur
- Aufbau bzw. Nutzen von Zeitstempeldiensten
- Aufbau von Digitalen Schlüsselarchiven (Key Archival Service – KAS)