Konfigurationsbeschreibung

GeBüV und EIDI-V konforme Einstellungen des Dokumentenmanagement Systems HyperDoc

HyperDoc Version 6.2x

IQDoQ GmbH
Document Management Company of Materna

Theodor-Heuss-Straße 59
D-61118 Bad Vilbel
Telefon: 06101/806-300
Telefax: 06101/806-590
E-Mail: info@iqdoq.de

www.iqdoq.de

Konfigurationsbeschreibung HyperDoc gemäß GeBüV und EIDI-V

Handbuchversion: 1.2

Datum: 31. Mai 2017

Autor: Sabrina Bockisch

1. Revisionssichere Konfiguration von HyperDoc

1.1 Das Dokumentenmanagement System HyperDoc

Das Dokumentenmanagement System HyperDoc ermöglicht eine revisionssichere, digitale Dokumentenverwaltung. Für Fachabteilungen oder das gesamte Unternehmen und über den vollständigen Dokumenten-Lebenszyklus hinweg. Zu den Basisfunktionen des Dokumentenmanagement Systems HyperDoc gehören:

- Die Übernahme von Papierdokumenten
- Die Übernahme elektronischer Dokumente
- Die Übernahme von Emails
- Die Übernahme und Prüfung elektronischer Signaturen
- Die Recherche nach archivierten Dokumenten
- Die Bearbeitung von Dokumenten
- Die Reproduktion von Dokumenten
- Das Weiterleiten von Dokumenten (Workflows)
- Das Löschen von Dokumenten

Dabei gilt, dass Dokumente in HyperDoc direkt nach Ihrer Erfassung revisionssicher archiviert werden. Eine Bearbeitung im Rahmen von Versionierung, Annotationen (Notizen, gelbe Zettel, Markierungen, etc.) und Workflows ist bei entsprechender Berechtigung jederzeit möglich. Hierbei werden alle Bearbeitungen protokolliert, so dass die Ursprungsversion des archivierten Dokuments jederzeit nachvollziehbar und abrufbar ist.

1.2 HyperDoc Komponenten

Das HyperDoc Dokumentenmanagement System (DMS) basiert auf einer Mehrschichtarchitektur mit Application-Server-Technologie. Präsentationslogik, Geschäftslogik und Datenhaltung sind dabei voneinander getrennt. Nachfolgende Abbildung veranschaulicht die HyperDoc Systemkomponenten.

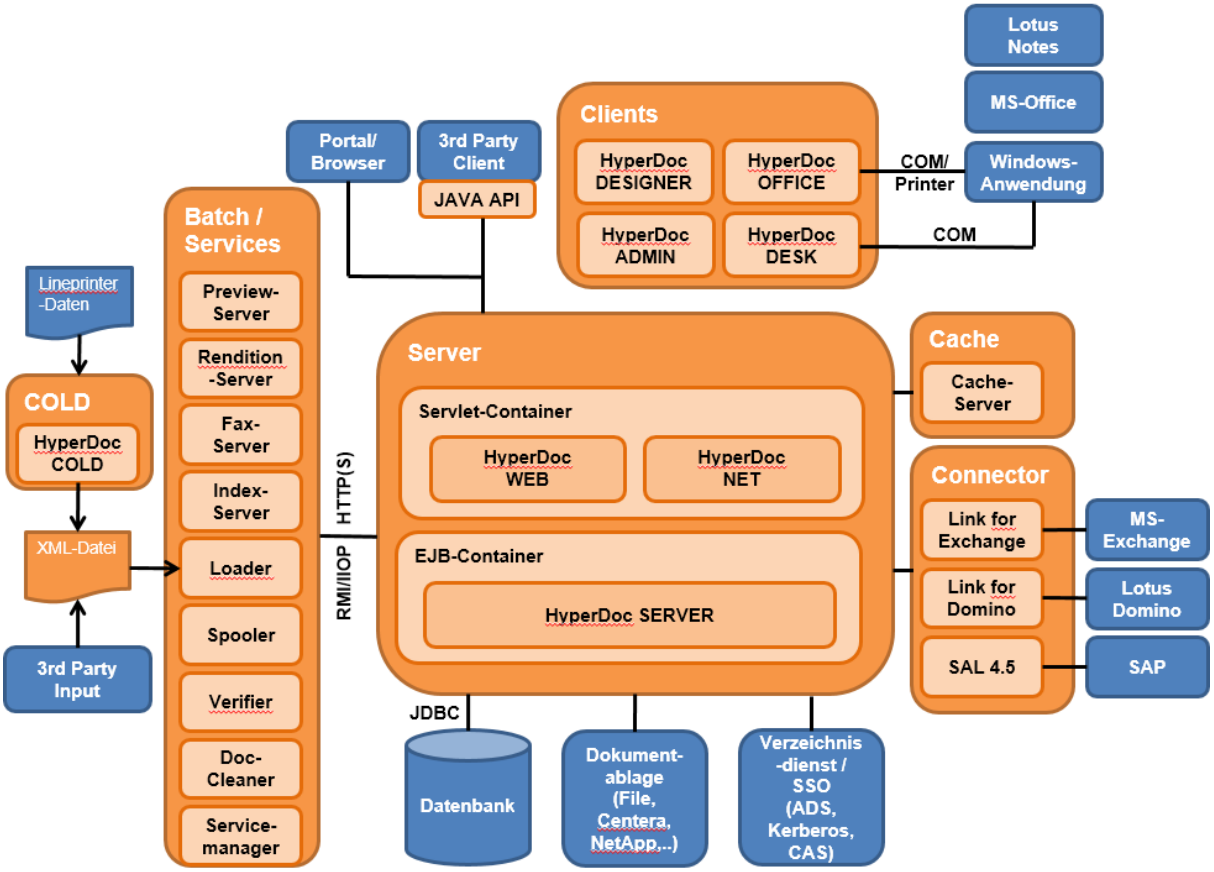

Abbildung 1: Architektur HyperDoc

1.3 HyperDoc Konfiguration gemäß GeBüV und EIDI-V

Für eine revisionssichere Archivierung kaufmännisch aufbewahrungspflichtiger Dokumente in der Schweiz wird folgende HyperDoc Konfiguration empfohlen:

- Daten- und Dokumentablage
  - Die Ablage der Indexdaten von Dokumenten und ggf. Akten erfolgt auf einer relationalen Datenbank gemäß HyperDoc Freigabeliste. Eine Datenbankverschlüsselung wird dabei (abhängig von der verwendeten Datenbank) HyperDoc-seitig unterstützt.
  - Die HyperDoc Funktion „selbsttragendes Archiv" ist zu aktivieren, so dass alle Archivdaten ohne Einsatz des oder der Liefersysteme jederzeit gefunden werden können. Alle Zugriffe auf das Archiv und Anpassungen müssen protokolliert werden.
  - Die Dokumentablage erfolgt auf einem WORM (-Like) Medium (Write Once Read Many) wie z.B. Centera, Netapp oder iCAS.
  - Ablageformat: Alle Dokumente werden in ihrem Originalformat abgelegt. Für Dokumente, deren Originalformat keinem Langzeitformat (z.B. PDF/A, Tiff) entspricht, wird zusätzlich zu jedem Dokument eine PDF/A Rendition als Langzeit- und Anzeigeformat erzeugt.
  - Für die GeBüV konforme Archivierung müssen neben den systemseitig gesetzten Indexdaten Owner, Dokumentenklasse, Aufbewahrungsfrist, Zeitstempel

(Abspeicherung) auch die aus fachlicher Sicht zusätzlichen Metadaten (z.B. Barcode, ID eines führenden Systems etc.) als Dokumentattribute definiert werden. Für den Fall, dass HyperDoc nur als Archiv für ein Drittsystem (z.B. SAP) verwendet wird, müssen fachlich relevante Indexdaten der Dokumente neben dem Drittsystem auch in HyperDoc verfügbar sein.

- Backup
  - Es wird eine gespiegelte Ablage über verteilte Standorte (zwei Rechenzentren) empfohlen für eine hohe Verfügbarkeit der Dokumente.
  - Wird keine gespiegelte Ablage eingesetzt, wird die Erstellung regelmäßiger Backups empfohlen.
- Aufbewahrungsfristen
  - Dokumente werden gemäß ihren Aufbewahrungsfristen nach Dokumentklassen unterteilt. Dabei können unterschiedliche Dokumentklassen verschiedene Aufbewahrungsfristen erhalten. Ein manuelles Hochsetzen der Aufbewahrungsfrist von archivierten Dokumenten ist für die Systemadministratoren möglich (z.B. im Fall eines laufenden gerichtlichen Verfahrens). Ein manuelles Herabsetzen der Aufbewahrungsfrist von archivierten Dokumenten ist auch mit Administrator-Rechten nicht möglich.
  - Nach Ablauf der Aufbewahrungsfrist werden nicht mehr aufbewahrungspflichtige Dokumente durch den HyperDoc Doc Cleaner Prozess in einem ersten Durchlauf als zu löschendes Dokument markiert („Löschprotokoll“) und in einem zweiten zeitversetzten Durchlauf rückstandsfrei gelöscht. Der Doc Cleaner ist so konfiguriert, dass zwischen den beiden Durchläufen mindestens 14 Tage liegen.
  - Der Doc Cleaner ist so zu konfigurieren, dass er im zweiten Durchlauf transaktionsgesichert sowohl das entsprechende Dokument von der Ablage und ggf. der gespiegelten Ablage, als auch den zugehörigen Datenbankeintrag und ggf. den Eintrag aus dem selbsttragenden Archiv löscht .(vgl. Abschnitt Verfügbarkeit und Verschlüsselung). Dazu muss die HyperDoc Server-Einstellung „allow_destroy=true“ gesetzt sein. Andernfalls werden nur Einträge aus der Datenbank gelöscht.
  - Der für die Ablage verwendete WORM-Datenträger ist so zu konfigurieren, dass die Aufbewahrungsfristen auf dem Datenträger mit den Aufbewahrungsfristen in HyperDoc übereinstimmen. Abhängig vom verwendeten WORM-System wird dies sichergestellt, indem entweder beim Archivieren eines Dokuments dessen in HyperDoc gesetzte Aufbewahrungsfrist dynamisch auf dem WORM-Datenträger gesetzt wird, oder indem der WORM-Datenträger beim Setup des Archivierungsprojekts in n Partitionen / Shares mit unterschiedlicher Aufbewahrungsfrist geteilt wird. Dabei entspricht n der Anzahl der in HyperDoc verwendeten Dokumentklassen mit unterschiedlichen Aufbewahrungsfristen. Beim Archivierungsvorgang wird nun jedes Dokument gemäß seiner Dokumentklasse auf der dafür definierten WORM-Partition mit der zur Dokumentklasse passenden Aufbewahrungsfrist abgelegt. Für den Löschvorgang bei einer WORM-Ablage gilt, dass ausschließlich die HyperDoc-eigenen Löschprozesse verwendet werden. Die WORM-Ablage ist dazu so zu konfigurieren, dass kein Benutzer außer dem HyperDoc Systembenutzer Löschrechte auf der Ablage erhält. Für den Fall, dass ein Administrationszugang des WORM-Datenträgers über Löschrechte verfügen soll, empfehlen wir die Verwendung eines geteilten Passworts, um ein 4-Augen-Prinzip für einen möglichen Löschzugriff auf der Ablage sicher zu stellen.
- Verfügbarkeit und Verschlüsselung
  - Der Transport von Dokumenten zwischen Server und HyperDoc-Client erfolgt per http oder https-verschlüsselt. Client-Verbindungen über das Netzwerk werden so konfiguriert, dass sie https zum Transport verwenden. Falls Client und Server auf dem

gleichen System arbeiten und keine Daten über das Netzwerk versendet werden, kann alternativ auch eine unverschlüsselte http-Verbindung eingesetzt werden.
    - Bei datenschutzrelevanten Inhalten empfehlen wir, die Ablage der Dokumente auf der Dokumentablage durch HyperDoc zu verschlüsseln (AES)
    - Im Fall einer geplanten Abschaltung / Ablösung von HyperDoc, verfügt HyperDoc über Exportmechanismen, die die archivierten Dokumente entschlüsselt mit ihren Indexdaten zur Verfügung stellen können.
    - Die HyperDoc Funktion „selbsttragendes Archiv" ist zu aktivieren. Diese erzeugt pro Dokument einen Ordner, in dem eine unverschlüsselte, ungeblockte Kopie des Dokuments, sowie die Index- und Zugriffsdaten des Dokuments (Document Log) gespeichert werden. Im selbsttragenden Archiv kann über die standardmäßig verfügbaren Betriebssystem-Suchfunktionen nach Dokumenten recherchiert werden.
- Berechtigungen
    - Alle HyperDoc Administratoren verfügen über personalisierte Zugänge zum System.
    - Alle Benutzer, soweit Sie direkt über einen HyperDoc Client auf das System zugreifen, verfügen ebenfalls über personalisierte Benutzeraccounts (dabei ist eine Kopplung an ein vorhandenes Active Directory bis hin zu einem Single-Sign-on möglich).
    - Im Fall eines Zugriffs über SAP Archive Link, nutzen alle Benutzer den HyperDoc-Benutzeraccount des SAP-Systems. Um in diesem Fall die personalisierten Zugriffe nachvollziehen zu können, ist das SAP-System so zu konfigurieren, dass die Benutzerprotokolle als Archivobjekt an HyperDoc übergeben und archiviert werden.
    - Alle Benutzerberechtigungen sind nach dem Minimal-Prinzip zu vergeben: Ein Benutzer erhält genau die Zugriffsberechtigungen, die für die Erfüllung seiner Aufgaben notwendig sind. Die Verwendung von Passwort-Regeln (BSI-konform) wird empfohlen und kann über die Benutzerverwaltung vorgegeben werden.
    - Für Dokumente mit Aufbewahrungsfrist erfolgt das Löschen ausschließlich nach Ablauf der Aufbewahrungsfrist durch den HyperDoc Doc Cleaner Prozess.
    - Für Dokumente ohne Aufbewahrungsfrist ist bei Bedarf ein Löschen durch Benutzer nach einem 4-Augen-Prinzip möglich (rollenbasierte Berechtigungen).
    - Zur Überwachung der Berechtigungsvergabe wird das HyperDoc Audit Log verwendet. Dieses protokolliert Änderungen an Berechtigungen und kann an externe Monitoring-Systeme angebunden werden.
- Legal Hold
    - Der Legal Hold Prozess erfolgt für Dokumente mit Aufbewahrungsfrist über ein Stoppen des HyperDoc Doc Cleaner Prozesses. Dazu wird durch den Administrator über die Benutzerverwaltung der Systembenutzer des Doc Cleaners deaktiviert. Nach Abschluss des Verfahrens wird der Benutzer wieder aktiviert.
    - Betrifft der Legal Hold Dokumente ohne Aufbewahrungsfrist, werden den Benutzern der zweiten Löschstufe (endgültiges aus dem Papierkorb löschen) temporär die Löschrechte entzogen, so dass Dokumente zwar noch in den Papierkorb verschoben, dieser aber für die Dauer des Verfahrens nicht geleert werden kann.
- Protokollierung und Systemzeit
    - Das Document Log wird in die von HyperDoc genutzte Datenbank geschrieben. Eine Kopie der Logdateien ist über die Funktion „selbsttragendes Archiv" zusammen mit einer Kopie des Dokuments auf eine (unverschlüsselte) Dokumentablage zu schreiben und zu archivieren.
    - Für eine gesetzeskonforme Archivierung ist das Audit Log auf dem WORM-Datenträger der Dokumentablage abzulegen. Betriebsempfehlung: Zusätzlich sollte das Audit Log an ein vorhandenes Monitoring mit aktiver Benachrichtigung der Systemadministratoren / Compliance Beauftragten im Fall von Berechtigungsänderungen eingebunden werden

- Die Protokolldatei des Doc Cleaners (Kopie der Auftragstabelle der als zu löschend markierten Dokumente) wird ebenfalls auf der Dokumentablage abgelegt. Die Löschprozesse sind zu protokollieren und aufzubewahren. Es wird projektspezifisch definiert, welche Indexdaten zum Nachweis von Löschprozessen notwendig sind.
- Zur Sicherstellung der korrekten Systemzeit des HyperDoc Servers wird empfohlen, die Systemzeit über einen automatischen Prozess wie NTP regelmäßig abzugleichen.

- Integrität
  - Zur Absicherung der Integrität (Erkennung von Manipulation) wird zu jedem Dokument eine Prüfsumme erzeugt (SHA 256) und in der Datenbank zusammen mit den Indexdaten des Dokuments abgelegt. Die Prüfsumme wird bei jeder Auslieferung eines Dokuments durch den HyperDoc DESK-Client überprüft.
  - Zusätzlich erfolgt eine zufallsbasierte regelmäßige serverseitige Überprüfung der Integrität durch den HyperDoc Verifier.
    - Der Verifier ist dabei so zu konfigurieren, dass er in regelmäßigen Zeitabständen einen zufälligen Anteil der Dokumentablage verifiziert und die Korrektheit der Prüfsumme und damit des Dokumentinhalts überprüft. Die Häufigkeit und der Anteil der überprüften Dokumente sind entsprechend des Sensibilität der Inhalte, der Größe und auch der Art der Ablage (WORM vs. Festplatte) im Projekt zu definieren.
  - Empfehlung IQDoQ: Zur Erschwerung der Manipulation von Dokumentindexdaten, sollten Datenbankadministrator und HyperDoc-Administrator nach Möglichkeit personell getrennt sein.