

DocuWare AG, Germering

Produktprüfung 2007

Dokumentenmanagement-System

DocuWare 5.1

 **ERNST & YOUNG**

Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS	2
A. AUFTRAG UND AUFTRAGSDURCHFÜHRUNG	3
I AUFTRAGGEBER UND PRÜFUNGSGEGENSTAND	3
II PRÜFUNGS DURCHFÜHRUNG.....	3
III PRÜFUNGSKRITERIEN.....	5
B. DARSTELLUNG DER PRÜFUNGSERGEBNISSE	6
I NOTWENDIGE VERARBEITUNGSREGELN	6
1 Systemüberblick und Datenhaltung	6
2 Erfassung sowie Im- und Export Funktionalität	8
3 Belegfunktionalität	10
4 Integritätsfunktion	12
5 Sicherung der Lesbarkeit.....	13
6 Maßnahmen zur Sicherstellung des Zugriffs auf steuerrelevante Daten.....	14
II SICHERHEITSANFORDERUNGEN.....	16
1 Autorisierungsfunktion.....	16
2 Vertraulichkeitsfunktion.....	18
3 Nachvollziehbarkeit	18
4 Daten- und Softwaresicherheit	20
III DOKUMENTATIONSANFORDERUNGEN	22
C. ZUSAMMENFASSUNG DER PRÜFUNGSERGEBNISSE UND SOFTWAREBESCHEINIGUNG	23

ANLAGE

Allgemeine Auftragsbedingungen

ABKÜRZUNGSVERZEICHNIS

AO	Abgabenordnung
BMF	Bundesministerium der Finanzen
FAIT	Fachausschuss für Informationstechnologie
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBS	Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
IDW	Institut der Wirtschaftsprüfer
NTLM	NT LAN Manager
LAN	Local Area Network
PC	Personal Computer
PS	Prüfungsstandard
SDLC	Software Development Life Cycle
SQL	Structured Query Language
SSL	Secure Sockets Layer
TIFF	Tagged Image File Format
TCP/IP	Transmission Control Protocol/Internet Protocol
WHQL	Windows Hardware Quality Labs
WORM	Write Once Read Many
XML	Extensible Markup Language

A. AUFTRAG UND AUFTRAGSDURCHFÜHRUNG

I Auftraggeber und Prüfungsgegenstand

Die DocuWare AG, Germering (im Folgenden: „DocuWare“), erteilte uns auf der Basis unseres Angebots vom 19. Oktober 2006 den Auftrag zur Überprüfung der Ordnungsmäßigkeit des Dokumentenmanagement-Systems „DocuWare 5.1.2“

Gegenstand des Auftrages war die Überprüfung der Version 5.1 hinsichtlich der Ordnungsmäßigkeit und Revisionsicherheit gemäß dem Prüfungsstandard PS 880 des Instituts der Wirtschaftsprüfer (IDW). Weiterhin sollte überprüft werden, ob das System in der Lage ist, den Anwender hinsichtlich Revisionsicherheit und Aufbewahrungsfristen zu unterstützen.

II Prüfungsdurchführung

Die Prüfungshandlungen wurden im Dezember 2006 und im Januar 2007 in den Räumen der DocuWare AG durchgeführt. Dabei haben wir insbesondere eigene Funktionstests angesetzt, zu deren Durchführung uns von DocuWare eine Testkonfiguration eingerichtet wurde:

- Produkt „DocuWare 5.1.2“
- Datenbank DocuWare Internal Database 5.1.1 (MySQL Instanz)
- Betriebssystem Windows XP Professional
- Rechner IBM Notebook (Intel Pentium M 1,7 GHz)
- Scanner Kodak i40 Scanner

Im Rahmen der Zertifizierung wurde auf dem Testrechner eine vollwertige „Single Workstation“ Installation durchgeführt. Bei dieser Installationsart wird sowohl die Darstellungsebene (Client), als auch die Serverebene (der Authentication-, der Content- und der Workflow Server) sowie die Datenebene (MySQL DB) auf einer Maschine installiert.

Im produktiven Einsatz werden diese Ebenen gegebenenfalls auf verschiedenen Rechnern installiert. Die Kommunikation zwischen den Ebenen und den Servern wäre in diesen Fällen technisch identisch mit der Testkonfiguration. Sie erfolgt über das Kommunikationsprotokoll Transmission Control Protocol/Internet Protocol (TCP/IP).

Ferner wurden uns folgende Unterlagen ausgehändigt bzw. konnten wir folgende Informationsquellen nutzen:

- „DocuWare 5 White Paper Systemarchitektur“, Version 1.0a, Mai 2005
- „DocuWare 5 Technische Referenz“, Stand 11.12.2006
- „DocuWare 5“ - Umfassende Online Hilfe
- Software Development Life Cycle (SDLC), Version 1.0, Stand 20.08.2006

Die bei der Prüfungsdurchführung benötigten Auskünfte erteilten uns die Verantwortlichen aus den Bereichen Product, Quality Management und Research & Development.

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, unsere als Anlage beigefügten Allgemeinen Auftragsbedingungen in der Fassung vom 1. Januar 2002 maßgebend.

III Prüfungskriterien

Für die bei der Prüfung angewendeten Prüfungskriterien orientierten wir uns am IDW (Institut der Wirtschaftsprüfer) Prüfungsstandard „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW PS 880, Stand: 25. Juni 1999 inkl. Erg.-Lfg. Januar 2003) und an handels- und steuerrechtliche Vorschriften für eine ordnungsmäßige Buchführung (§§ 238 ff. HGB, § 257 HGB sowie §§ 145 ff. AO).

Weiterhin orientierten wir uns an der IDW Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“ (IDW RS FAIT 1 Fachausschuss für Informationstechnologie, Stand 24. September 2002) sowie der IDW Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren“ (IDW ERS FAIT 3 Fachausschuss für Informationstechnologie, Stand: 2. Februar 2005), denen wiederum handels- und steuerrechtliche Bestimmungen zu Grunde liegen.

Des Weiteren haben wir für die Bewertung der Programmfunktionalität die spezifisch für Buchführungssoftware geltende GoBS (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme), gem. BMF-Schreiben vom 7. November 1995 (Bundesministerium der Finanzen) sowie die GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen), gem. BMF-Schreiben vom 16. Juli 2001 herangezogen.

B. DARSTELLUNG DER PRÜFUNGSERGEBNISSE

Eine Software, die aufbewahrungspflichtige Informationen transformiert, speichert und wiedergibt, muss sich in erster Linie daran messen lassen, ob sie die Anforderungen der Grundsätze ordnungsmäßiger Buchführung erfüllt (§§ 238 ff HGB). Ordnungsmäßige, computergestützte Archivierungssysteme sind solche, die unter Einbeziehung aller maschinellen und manuellen Verfahren die ordnungsgemäße Transformation, die ordnungsgemäße Speicherung und die ordnungsgemäße Wiedergabe der aufbewahrungspflichtigen Informationen ermöglichen.

I Notwendige Verarbeitungsregeln

1 Systemüberblick und Datenhaltung

Zur Beurteilung der ordnungsgemäßen Funktionalität des Produkts „DocuWare 5.1“ sind Bewertungen der System und Datenbankarchitektur unabdingbar.

Die Systemarchitektur bildet eine Multi Tier Architektur ab, deren Ebenen Benutzerschnittstellen, die Serverebene (die Middleware) und die Datenhaltung umfasst.

Die Benutzerschnittstelle besteht mindestens aus dem „DocuWare“ Client und dem Administrationstool. Beim Einsatz eines Internet Servers ist der Standardbrowser das Zugriffsmedium auf die Archive. Weiterhin werden optional Module des Systems „DocuWare 5“ mit separaten Benutzeroberflächen ausgeliefert.

Bei einer „DocuWare 5“ Installationen sind der Authentication Server zur Steuerung der Benutzeranmeldung, der Content Server zur Steuerung des Datenzugriffs und der Workflow Server zur Steuerung von Arbeitsabläufen obligatorisch. Die Einbindung eines Internet Servers ist für den entfernten Zugriff auf die Archive fakultativ.

Weiterhin ist die redundante Auslegung mit maximal zwei Authentication Servern und mehreren Content- und Workflow Servern möglich.

Die Datenebene umfasst mindestens eine Datenbank und ein Filesystem. Die Dokumente werden mit den Indexdaten auf einem Filesystem abgelegt. Um eine strukturierte Recherche zu ermöglichen, werden die Indexdaten zusätzlich in der Datenbank abgelegt. Die Indexdaten, die das jeweilige Dokument näher beschreiben, sind demnach redundant verfügbar. Für die Datenbank kann wahlweise eine Instanz einer MySQL, einer MS-SQL oder einer Oracle Datenbank zum Einsatz kommen (MySQL 4 und 5; MS SQL 2000 und 2005; Oracle ab der Version 9.2). Als Filesystem wird wahlweise ein Windows-, ein Linux-, ein SUN- oder ein Novell-Dateisystem empfohlen. Der Einsatz anderer Dateisysteme mit Windows-Dateisystem-Support ist möglich.

Zur Sicherung der Revisionsicherheit wird dem Anwender empfohlen, vom direkten Zugriff auf die Datenbankebene und dem Filesystem abzusehen. Der Anwender sollte durch administrative Maßnahmen gewährleisten, dass der Benutzerzugriff auf die Verzeichnisse des Filesystems und die Datenbank nur durch das System „DocuWare 5“ möglich sind.

Fakultativ ist auf dieser Ebene die Einbindung eines externen Benutzerverzeichnisses (z. B. eines Active Directory) möglich. Die Konfiguration ermöglicht bei Veränderungen der Zuweisung von Benutzern zu Benutzergruppen im Filesystem eine synchronisierte Anpassung in der Benutzerverwaltung von „DocuWare“.

2 Erfassung sowie Im- und Export Funktionalität

Um die Verwendung von Archiven der Vorgängerversionen von „DocuWare 5“ sicher zu stellen, existiert die Möglichkeit „DocuWare 4“ Archive in ein „DocuWare 5“ Archiv zu überführen.

Das Erfassen der Dokumente in „DocuWare 5.1“ kann durch folgende Verfahren durchgeführt werden:

- Scannen der Originalbelege. Die unterstützten Scanner sind in der technischen Dokumentation aufgeführt.
- TIFFMAKER, der aus einer externen Datei (z.B. einem Word-Dokument) eine Datei im „DocuWare“ Tagged Image File Format (TIFF) Format erstellt. Der TIFFMAKER arbeitet als Druckertreiber, dessen Funktionalität von Microsoft im Rahmen eines Windows Hardware Quality Labs (WHQL) Tests bestätigt wurde. Diese Bestätigung ist gültig bis 05.04.2008.
- Importieren von Dokumenten aus dem Dateisystem, auch durch automatisierte Überwachung von Ordnern durch das „DocuWare“ Modul „ACTIVE IMPORT“
- Importieren von E-Mails aus Microsoft Outlook, auch durch automatisierte Überwachung von Postfächern durch das Modul „ACTIVE IMPORT“
- Schnittstelle zu einem SAP System. Die Richtigkeit der Funktionsfähigkeit dieser Schnittstelle ist im Rahmen einer „Interface Certification“ für das Interface BC-AL HTTP CS 4.5 im Produkt SAP NetWeaver AS 6.40 vom 28.11.2006 durch SAP festgestellt und dokumentiert worden. Für diese Schnittstelle wurden, auf Grund der bereits durchgeführten Zertifizierung, keine Testaktivitäten vorgenommen.
- Direktes Importieren aus den Microsoft Produkten MS Excel, MS Word und MS Powerpoint durch ein von DocuWare bereitgestelltes Add In für diese Produkte.

Der Export, der Druck und das Weiterleiten per E-Mail von dafür freigegebenen Dokumenten werden autorisierten Nutzern ermöglicht. Die Exportfunktionalität umfasst weiterhin die Übertragung aller Dokumente eines Archivs, oder einer definierten Auswahl dieser, in andere Archive.

Weiterhin ist es möglich alle Dokumente eines Archivs, oder eine definierte Auswahl dieser, durch das separate „DocuWare“ Modul („DocuWare REQUEST“) zu archivieren und weiteren Personen zur Ansicht zur Verfügung zu stellen.

Die Verifikation der eingelesenen Dokumente muss manuell durch den Benutzer mit Hilfe des integrierten Anzeigeprogramms erfolgen. Systemseitige Fehler beim Transport der Dokumente in die Archive werden abgefangen und dem Anwender kommuniziert. Im Falle eines Fehl-Transports durch das „DocuWare“ Modul „ACTIVE IMPORT“ besteht ein Backup Ordner, der nicht bearbeitete Dokumente enthält.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Erfassung sowie des Im- und Exports im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

3 Belegfunktionalität

Die Belegfunktion stellt den nachvollziehbaren Nachweis über den Zusammenhang zwischen dem konkreten Geschäftsvorfall und dessen Abbildung in der Buchführung dar. Die Software hat sicherzustellen, dass die archivierten Buchungsdaten und Belege eindeutig zugeordnet und gespeichert werden (Indexierungs- und Archivierungsfunktion). Die eindeutige Zuordnung von Dokumenten zu Geschäftsvorfällen kann durch folgende Verfahren, auch in Kombination erfolgen:

- Manuelle Erfassung der Metadaten in nutzerabhängig konfigurierbaren Erfassungsmasken. Dabei können Indexeinträge vordefiniert, als Pflichtfelder oder als eindeutige Felder konfiguriert werden.
- Barcodeerkennung und Texterkennung für Standarddokumente zur eindeutigen Identifizierung mit Hilfe des „DocuWare“ Moduls „RECOGNITION“.
- Auslesen von Metadaten aus Microsoft Outlook bei Archivierung von E-Mails.
- Verknüpfung zu externen Datenbanken und externen Dateien zum Auslesen von Stammdaten auf der Grundlage von eindeutigen Suchattributen mit Hilfe des „DocuWare“ Moduls „AUTOINDEX“.
- Weiterleitung von Indexinformationen, wie Barcodes aus dem SAP System über die bereits erwähnte von SAP zertifizierte Schnittstelle mit dem „DocuWare“ Modul „SAP CONNECT“.

Die Archivierung erfolgt logisch in so genannten „DocuWare Archiven“. Es sind mehrere Archive für eine „DocuWare“ Installation möglich.

Bei der Archivierung sind einfache Plausibilitätsprüfungen durch Pflichtfelder oder eindeutige Felder in den Archiven möglich. Weiterhin ist es möglich Plausibilisierungen in Abhängigkeit der Indexdaten frei zu definieren.

„DocuWare 5.1“ stellt die grundsätzlichen Sicherheitsmechanismen zur Verfügung, um Dokumente vor unberechtigten Veränderungen oder vor Manipulation zu schützen. In welcher Ausprägung diese Mechanismen zum Einsatz kommen, ist abhängig von der konkreten „DocuWare“ Konfiguration, die die ordnungsgemäße Einhaltung der Archivierungserfordernisse der abgelegten Dokumente widerspiegeln sollte.

Die physische Ablage der Dokumente erfolgt in einem Filesystem. Zu jedem Dokument wird die Header Datei im Extensible Markup Language (XML) Format gesichert. Die Indexinformationen mit Metadaten und Links zum Filesystem sind in der Datenbank hinterlegt.

Der Zugriff auf das Filesystem erfolgt durch den Content Server. Die Verantwortung zur ordnungsgemäßen Einrichtung der Zugriffsberechtigungen zum Filesystem obliegt dem Anwender und kann durch die „DocuWare“ Funktionalität nicht garantiert werden.

Falls Bilddaten in das TIFF Format konvertiert werden, werden nur die konvertierten Dokumente hinterlegt. Eine Konvertierung ist jedoch nicht notwendigerweise erforderlich, sondern wird optional angeboten. Digitale Dokumente jeglicher Art können grundsätzlich immer im Original archiviert werden. Die Sicherung der Originaldaten ist demnach ermöglicht.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Indexierung und Archivierung von Dokumenten im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

4 Integritätsfunktion

Im Hinblick auf die Datensicherheit und die Nachvollziehbarkeit des archivierten Geschäftsvorfalles über die gesamte Aufbewahrungsfrist sind die Softwarefunktionen dahingehend zu verifizieren, ob die buchführungsrelevanten Informationen für die Dauer der gesetzlichen Aufbewahrungspflichten gegen Verlust gesichert und gegen unberechtigte Veränderungen geschützt werden.

Einzelne Dokumente oder eine Menge von Dokumenten kann mit einem Hash Code versehen werden, der die Unveränderlichkeit der Dokumente sicherstellt. Falls Dokumente unberechtigt (z. B. direkt im Filesystem) verändert werden, erfolgt der entsprechende Hinweis auf eine Manipulation.

Dokumente können zusätzlich digital signiert werden. Die Signatur kann mit einem frei zu definierenden Stempel erfolgen. Zu unterscheiden sind hierbei öffentliche Stempel und persönliche Stempel, die nur dem jeweiligen Benutzer zur Verfügung stehen. Stempel können mit einem Passwortschutz gesichert werden. Eine Zuordnung der Integrität und Authentifizierung des Benutzers ist durch die digitale Signatur gesichert.

Dokumente die nicht verändert werden sollen, können durch eine "check out" Funktionalität vor Änderungen geschützt werden. Diese Dokumente stehen ausschließlich im lesenden Zugriff zur Verfügung. Das „ausgecheckte“ Dokument kann nur durch einen Administrator oder dem Benutzer, der das „check out“ vorgenommen hat, wieder eingechekkt werden. Veränderungen an Dokumenten können ausschließlich in Form eines neuen Dokuments archiviert werden.

Weiterhin besteht die Möglichkeit, über Indexbegriffe Abteilungen oder anderen Personengruppen eingeschränkte Berechtigungen, wie z. B. ausschließlich lesenden Zugriff, zuzuweisen. Als organisatorische Maßnahme außerhalb des Systems „DocuWare“ besteht die Möglichkeit, die Archive, deren Dokumente keine Veränderungen erfahren dürfen, auf so genannte Write Once Read Many (WORM) Platten zu hinterlegen und somit eine nachträgliche Veränderung der Dokumente auszuschließen.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Sicherung der Integrität im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

5 Sicherung der Lesbarkeit

Bei der Aufbewahrung des Archivierungsstoffes auf Datenträgern muss durch die Software insbesondere sichergestellt werden, dass die Informationen unverändert bleiben und permanent lesbar sind (Sicherung der Lesbarkeit).

Die integrierte Dokumentenanzeige "DocuWare Viewer" ermöglicht die unverzügliche Lesbarmachung der archivierten Dokumente in Standardformaten, insbesondere im TIFF Format. Die Dokumentarten, die der Viewer unterstützt, sind in der technischen Dokumentation hinterlegt. Falls der Viewer die Dokumente nicht anzeigen kann, sind jederzeit eine Lesbarmachung und gegebenenfalls eine Bearbeitung der Dokumente mit zu definierenden Programmen möglich. Ein Export der Originaldokumente ermöglicht zusätzlich die lokale Lesbarmachung und gegebenenfalls eine Bearbeitung der Dokumente mit installierten Applikationen. Die Originaldokumente liegen temporär zur Ansicht beim Client.

Wie bereits in Abschnitt B.I.3 erwähnt, stellt „DocuWare 5.1“ die grundsätzlichen Sicherheitsmechanismen zur Verfügung. Für die Konfiguration der jeweiligen „DocuWare“ Installation, in Abhängigkeit der konkreten Archivierungserfordernisse, ist der Anwender verantwortlich.

Zusätzliche Sicherheit bietet das, bereits in Abschnitt B.I.2 erwähnte, „DocuWare“ Modul „DocuWare REQUEST“, das autonom betrieben werden und somit als Anzeigetool verwendet werden kann. Voraussetzung für die Nutzung ist eine „NET 2“ Umgebung.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Sicherung der Lesbarkeit im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

6 Maßnahmen zur Sicherstellung des Zugriffs auf steuerrelevante Daten

Im Rahmen des Steuersenkungsgesetzes hat der Gesetzgeber durch Änderungen und Ergänzungen der Abgabenordnung mit Wirkung zum 1. Januar 2002 die Voraussetzungen für erweiterte Zugriffs- und Prüfungsmöglichkeiten der Finanzverwaltung in die EDV-Systeme der Steuerpflichtigen im Rahmen der Betriebsprüfung geschaffen. Dies betrifft insbesondere die §§ 146, 147 und § 200 der Abgabenordnung. Zur Anwendung dieser Vorschrift in der Praxis der Betriebsprüfung, veröffentlichte das Bundesfinanzministerium am 16. Juli 2001 ein Schreiben über die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“ (GDPdU). „DocuWare“ begegnet hier den Archivierungsanforderungen mit der Möglichkeit Daten, neben der rein bildlichen Speicherung im TIFF-Format, auch in einem maschinell auswertbaren Format zu speichern.

Die Anforderungen in den GDPdU gelten für alle steuerlich relevanten Daten. Die GDPdU schreiben (vereinfacht dargestellt) vor, dass die im Datenverarbeitungssystem originär digital erzeugten Unterlagen, für die Dauer der 10-jährigen Aufbewahrungsfrist, auf einem maschinell verwertbaren Datenträger zu speichern und archivieren sind. Eine weitere in der GDPdU konkretisierte Forderung bezieht sich auf die Verfügbarmachung dieser Informationen für die Steuerbehörden, die in Form eines „mittelbaren bzw. unmittelbaren Datenzugriffs“ und/oder durch eine „Datenträgerüberlassung“ zu organisieren ist.

Diese GDPdU-Anforderungen werden von „DocuWare 5.1“ dahingehend behandelt, dass neben der bereits praktizierten Archivierung von Belegen in bildlicher Übereinstimmung über die Druckausgabe des Abrechnungssystems (z.B. im TIFF-Format über den TIFFMAKER), dasselbe Dokument in einem maschinell auswertbaren Dateiformat in das Archivsystem importiert und dort gemeinsam mit der Image-Datei aufbewahrt werden kann. In „DocuWare 5.1“ ist zusätzlich ein Zusammenbinden („Heften“) der zusammengehörenden und inhaltlich identischen Dokumente möglich.

Voraussetzung für die GDPdU-konforme Archivierung ist allerdings, dass die vorgelagerten Abrechnungssysteme neben der Druckausgabe zusätzlich über ein Exportinterface verfügen, welche die Daten in einem maschinell auswertbaren Format bereitstellen.

Die Lesbarmachung der Archivdaten auf einem PC, auf dem keine „DocuWare“ Installation benötigt wird, ist mit Hilfe eines auf einen Datenträger gespeicherten unabhängigen „DocuWare“ Moduls „REQUEST“ möglich, womit die von den GDPdU geforderte Datenträgerüberlassung, für die Auswertungszwecke der Steuerbehörden, ermöglicht wird.

Um die in den GDPdU geforderten Anforderungen zu erfüllen, ist der Anwender verpflichtet, die maschinelle Auswertbarkeit der zu archivierenden Daten sicherzustellen. „DocuWare“ bietet die Funktionalität diese Daten revisionssicher zu archivieren und bei Bedarf zur Verfügung zu stellen.

II Sicherheitsanforderungen

1 Autorisierungsfunktion

Der Zugriff auf die Archive erfolgt durch dezidierte Archivberechtigungen innerhalb der „DocuWare“ Benutzerverwaltung. Es besteht die Möglichkeit, ein dezidiertes Berechtigungskonzept mit Funktionsrechten und Archivrechten auf einzelne Archive einzurichten. Die Funktionsrechte legen fest, welche Menüpunkte und Funktionalitäten der Benutzer zur Ausführung angezeigt bekommt. Die Archivrechte legen je Archiv fest, welche Dokumente in welcher Art archiviert, gesucht und angezeigt werden kann. Die Rechte können zu Profilen und diese zu Rollen zusammengefasst werden. Benutzer können zu Gruppen zusammengefasst werden, denen ebenfalls Rechte, Profile oder Rollen zugewiesen werden können. Die einzelnen Rechte eines konkreten Benutzers werden grundsätzlich additiv zusammengefasst.

Neben dieser operationalen Rechteverwaltung erlaubt die administrative Rechteverwaltung die Vergabe von dezidierten Administrationsrechten für drei zu betrachtende Administrationsebenen:

- Ebene 1: Systemadministrator, zur Administration der gesamten „DocuWare“ Installation, wie z. B. die Server Konfiguration,
- Ebene 2: Organisationsadministrator, zur Administration der Organisationen einer „DocuWare“ Installation und
- Ebene 3: Archivadministrator, zur Administration der Archive, die einer Organisation zugeordnet sind, wie z. B. die Rechteverwaltung der Benutzer zum Zugriff auf die Dokumente in den Archiven.

Der Zugriff auf das System erfolgt passwortgeschützt wahlweise durch die Netzwerk anmeldung („Trusted Login“) oder durch eine separate Anmeldung am „DocuWare“ System. Sämtliche Zugriffe auf die Dokumente erfolgen durch den Client.

Falls die Windows-Sicherheitseinstellungen in der Konfiguration zum Authentication Server in „DocuWare“ nicht eingeschaltet sind, ist ein Trusted Login nicht möglich, und der Client benötigt grundsätzlich ein „DocuWare“ Login. So wird garantiert, dass kein ungesicherter Zugriff möglich ist und ein Trusted Login nur ermöglicht wird, wenn die Netzwerkanmeldung sicher prüfbar ist.

Weiterhin ist die Aktivierung einer Hochsicherheitsstufe auf Archivebene möglich. Ist diese Option aktiviert, kann ein Administrator der Organisation einen Benutzer und ein Archiv auf die Sicherheitsstufe „hoch“ setzen. Nur ein Benutzer mit der Sicherheitsstufe „hoch“ kann dann auf Archive mit der Stufe „hoch“ zugreifen. Für einen Benutzer mit der Stufe „hoch“ ist ein Trusted Login nicht möglich.

Es besteht systemseitig keine Möglichkeit zur Erstellung von Mindestanforderungen an Passwörter. Falls solche Mindestanforderungen systemseitig realisiert werden sollen, muss die Netzwerkanmeldung verwendet werden, deren Passwordeinstellungen validiert ist. Weiterhin ist beim Anwender organisatorisch sicher zu stellen, dass Passwörter definierten Mindestanforderungen entsprechen. Die Zugriffsberechtigungen auf Betriebssystem-, Datenbank- und Netzwerkebene waren nicht Gegenstand unserer Untersuchung. Die Benutzerverwaltung dieser Ebenen ist durch Standardfunktionalität des jeweiligen Systems abgedeckt und war nicht Gegenstand unserer Untersuchungen.

Die Passwörter werden verschlüsselt angezeigt und verschlüsselt in der Datenbank hinterlegt.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Sicherung der der Autorisierung im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

2 Vertraulichkeitsfunktion

Die Kommunikation zwischen den Servern kann verschlüsselt erfolgen. Dabei kann zwischen Microsoft-Standardverschlüsselungsmechanismen, wie NTLM (NT LAN Manager) und Kerberos oder einer Secure Sockets Layer (SSL) Verschlüsselung unterschieden werden.

Die sichere Verschlüsselung der Dokumente auf dem Filesystem kann in der Administration konfiguriert werden. Dabei kann sowohl der Header als auch das Dokument verschlüsselt werden. Die Dokumente werden beim Aufruf entschlüsselt und temporär beim Client abgelegt. Die temporären lokalen Verzeichnisse werden automatisch bei Beendigung von „DocuWare 5.1“ geleert. Die temporären Verzeichnisse der Client Installation sollten demnach im Netzwerk nicht verfügbar sein, sondern ausschließlich dem Nutzer lokal zur Verfügung stehen. Diese Aufgabe liegt wiederum im Verantwortungsbereich des Anwenders.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Sicherung der Vertraulichkeit im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

3 Nachvollziehbarkeit

Es existieren drei Ebenen der Protokollierung. Diese Einteilung orientiert sich an der Einteilung der Administrationsebenen, wie bereits im Abschnitt B.II.1 beschrieben.

- Ebene 1: Systemadministrator
- Ebene 2: Organisationsprotokollierung
- Ebene 3: Archivebene

Grundsätzlich ist die Einstellung der Ereignisart, auf der protokolliert wird, möglich. Dabei kann zwischen den Ebenen „Information“, „Warnung“, „Fehler“ und „kritischer Fehler“ unterschieden werden. Je nach Konfiguration, können auf allen Ebenen Informationen wie GUID, Name, Benutzername, Organisation, Typ und Datum protokolliert werden.

Alle Konfigurationen, die dem Systemadministrator zugänglich sind können protokolliert werden. Dies umfassen unter anderem sämtliche Ereignisse an den Datenverbindungen, an den Servern, an den Speicherorten und auch an der Protokollierung selbst. Es kann das Anlegen, das Ändern und das Löschen protokolliert werden.

Alle Konfigurationen und Objekte, die dem Administrator der Organisation zugänglich sind können protokolliert werden. Unterschieden wird zwischen der Protokollierung von administrativen Ereignissen und Ereignissen, die eintreten können, während die Objekte aktiv sind (Laufzeit). Zu den administrativen Ereignissen gehört das Anlegen, Bearbeiten oder Löschen eines Objekts. Zu den Laufzeit-Ereignissen gehört der Start eines Workflows.

Zu den Objekten, die auf Archivebene protokolliert werden können, gehören Archive und Dokumente, Archivprofile sowie Such-, Ablagemasken und Ergebnislisten. Unterschieden wird auch hier zwischen der Protokollierung von administrativen Ereignissen und Ereignissen, die eintreten können, während die Objekte aktiv sind (Laufzeit). Zu den administrativen Ereignissen gehört das Anlegen eines Archivs. Zu den Laufzeit-Ereignissen gehört beispielsweise das Bearbeiten eines Dokuments. Bei den Laufzeit Ereignissen werden bei Zugriff, Änderungen, Ablegen und Löschung wahlweise unter anderem der Dokumentenname, die Organisation, das Datum und der Benutzer protokolliert.

Zusammenfassend stellen wir fest, dass die untersuchten Funktionen zur Sicherung der Nachvollziehbarkeit im Produkt „DocuWare 5.1“ ordnungsgemäß gestaltet und in das Gesamtsystem integriert sind.

4 Daten- und Softwaresicherheit

Die Prüfung der Softwaresicherheit umfasst die Beurteilung der Programmentwicklung, -wartung und des Programmfreigabeverfahrens. Die Datensicherheit umfasst die Prüfung der Autorisierungsfunktion, die bereits im Abschnitt B.II.1 bestätigt wurde sowie die integrierte Datensicherungs- und Wiederherstellungsfunktionalität.

Ein formales Freigabeverfahren zum Nachweis der Programmidentität existiert, d.h. es kann nachgewiesen werden, welche Programmversion zu welchem Zeitpunkt für die Auslieferung an die Kunden freigegeben wurde.

Es existiert ein Dokument zur Beschreibung des internen Software Development Life Cycles (SDLC). Es wurden Stichproben zur Dokumentation der Prozessschritte im Rahmen dieser Prüfung zur Verfügung gestellt.

Die Fehlerbehebung wird nach einer separaten Arbeitsanweisung zum Umgang mit auftretenden Programmfehlern dokumentiert. Für die Fehlerbehebung wurden im Rahmen der Prüfung ebenfalls Stichproben der Dokumentation des beschriebenen Prozesses zur Verfügung gestellt. Die Dokumentationen zur Fehlerbehandlung und dem Status der Fehler werden in einem separaten System geführt.

Weiterhin bestehen Arbeitsanweisungen zu den Dokumentationsanforderungen bei der Durchführung von Implementierungen.

Die Prozesse zur Entwicklung und Verbesserung des Produkts „DocuWare“ sind in schriftlich fixierten Anweisungen beschrieben. Die Verfahren erfüllen die Anforderungen hinsichtlich der Anforderungs-, Test und Freigabedokumentation von Entwicklungen.

Die integrierte Datensicherungs- und Wiederherstellungsfunktionalität ist im Produkt „DocuWare“ durch die Exportmöglichkeit von Archiven oder Teilen dieser mit Hilfe des Systemmoduls „REQUEST“ erfüllt. Die Konfiguration der jeweiligen Installation wird nicht gesichert. Eine Sicherung der kompletten Systemumgebung ist nicht vorgesehen, kann jedoch vom Anwender durch gängige, in der Praxis erprobte Maßnahmen, realisiert werden.

Weiterhin ist die Sicherung der Dokumente im Filesystem zu empfehlen. Da die Indexeinträge dieser Dokumente ebenfalls im Filesystem hinterlegt sind, können diese durch integrierte Wiederherstellungsmechanismen in einer Datenbanktabelle nachgebildet werden.

Die Datensicherungs- und Wiederherstellungsfunktionalität erfüllt bei gewissenhafter Sicherung der Daten durch den Anwender die Anforderungen gemäß dieser Zertifizierung.

III Dokumentationsanforderungen

Der Umfang und die Aussagefähigkeit der Software-Dokumentation sind wichtige Qualitätskriterien für Anwender und Prüfer. Die Verfahrensdokumentation besteht aus der Systemdokumentation und der Anwenderdokumentation. Sie ist erforderlich für die sachgerechte Handhabung und künftige Fortführung der Software. Eine sachgerechte Dokumentation ist die Voraussetzung für die Nachvollziehbarkeit und damit die Prüfbarkeit des Verfahrens.

Aus der geforderten Verfahrensdokumentation müssen Inhalt, Aufbau und Ablauf des Aufbewahrungsverfahrens ersichtlich sein und sie muss sowohl die sachlogische Lösung als auch eine programmtechnische Lösung beschreiben.

Die an uns ausgehändigte Verfahrensdokumentation wurde von uns stichprobenartig überprüft. Zusätzlich haben wir die fachliche Richtigkeit einzelner, von uns geprüfter Verarbeitungsregeln anhand der Dokumentation nachvollzogen.

Dem Anwender steht zu der von ihm eingesetzten Programmversion die jeweils aktuelle Programmbeschreibung zur Verfügung, auf die er über die Hilfefunktion im Programm zugreifen kann.

Zur Administration liegen ausführliche Dokumente zur technischen Beschreibung des Produkts vor. Weiterhin geben White Papers zur Systemarchitektur und zur Abbildung von Sicherheitsmaßnahmen einen detaillierten Einblick in die sachlogischen und teils programmtechnischen Lösungen.

Zusammenfassend stellen wir fest, dass die vorliegende Dokumentation zum Produkt „DocuWare 5.1“ ordnungsgemäß und ausreichend gestaltet und zugänglich ist.

C. ZUSAMMENFASSUNG DER PRÜFUNGSERGEBNISSE UND SOFTWAREBESCHEINIGUNG

Auftragsgemäß haben wir die Funktionen der Anwendungssoftware „DocuWare 5.1“ hinsichtlich der, die Archivierung betreffenden, Teilaspekte der Grundsätze ordnungsgemäßer Buchführung, wie Vollständigkeit, Richtigkeit und Nachvollziehbarkeit geprüft.

Ferner haben wir uns über die bestehende Ordnungsmäßigkeit zu den Bereichen:

- Softwaresicherheit,
- Programmentwicklung, -freigabe und -wartung,
- sowie Dokumentation

überzeugt.

Der Prüfung wurden folgende Prüfungskriterien zu Grunde gelegt:

- Handels- und steuerrechtliche Vorschriften für eine ordnungsmäßige Buchführung (§§ 238 ff. HGB, § 257 HGB sowie §§ 145 ff. AO),
- BMF-Schreiben vom 7. November 1995 IV A 8 - S 0316 - 52/95 betreffend die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS),
- IDW Prüfungsstandard (IDW PS 880) zur Erteilung und Verwendung von Softwarebescheinigungen, Stand: 25. Juni 1999 inkl. 9. Erg.-Lfg. Januar 2003,
- Grundsätze ordnungsgemäßer Buchführung beim Einsatz von Informationstechnologie (IDW RS FAIT 1), Stand: 24. September 2002,
- Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW ERS FAIT 3), Stand: 2. Februar 2005 sowie
- BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 betreffend die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).

Eine Vollständigkeitserklärung, dass alle für die Prüfung sowie die Erteilung der Softwarebescheinigung bedeutsamen Unterlagen, Angaben, Erläuterungen und Auskünfte vollständig und richtig erteilt wurden, wurde eingeholt.

Bei der Beurteilung der Frage, ob die geprüfte Software den Ordnungsmäßigkeitsgrundsätzen entspricht, ist zu beachten, dass eine Softwareprüfung unter "Laborbedingungen" nicht die aufbau- und ablauforganisatorische Ebene des internen Kontrollsystems mit einbeziehen kann, so dass eine umfassende Beurteilung der Ordnungsmäßigkeit einer installierten Version hier nicht möglich ist. Das Ergebnis dieser Prüfung kann sich daher nur isoliert auf die Anwendungssoftware erstrecken und setzt voraus, dass die Abläufe im Unternehmen angemessen eingerichtet sind.

Da zukünftige Programmänderungen die Ordnungsmäßigkeit der Software beeinflussen können, bezieht sich unsere Aussage nur auf die von uns geprüfte Version 5.1.2

Als Ergebnis unserer Prüfung stellen wir fest:

Die von uns geprüfte Anwendungssoftware „DocuWare“ in der Version 5.1.2 ermöglicht bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung und den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme entsprechende Archivierung.

Wir weisen in diesem Zusammenhang darauf hin, dass die in den GDPdU geforderte maschinelle Auswertbarkeit der in „DocuWare“ archivierten steuerlich relevanten Daten nur dann erreicht werden kann, wenn diese Daten in einem maschinell auswertbaren Format vollständig, unverdichtet und ungefiltert über eine geeignete Schnittstelle aus dem originären Buchhaltungssystemen geliefert werden. Ferner versteht die Finanzverwaltung den Begriff der „maschinellen Auswertbarkeit“ als den wahlfreien Zugriff auf alle in sämtlichen Systemen gespeicherten Daten einschließlich der Stammdaten. Die Ordnungsmäßigkeit kann deshalb abschließend nur in der Gesamtheit mit den beim Anwender installierten Systemen sowie eingesetzten Verfahren beurteilt werden.

München, 24. Januar 2007

Ernst & Young AG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft



Hans-Robert Walbröl
Wirtschaftsprüfer



Gerd Marxer
Wirtschaftsprüfer

