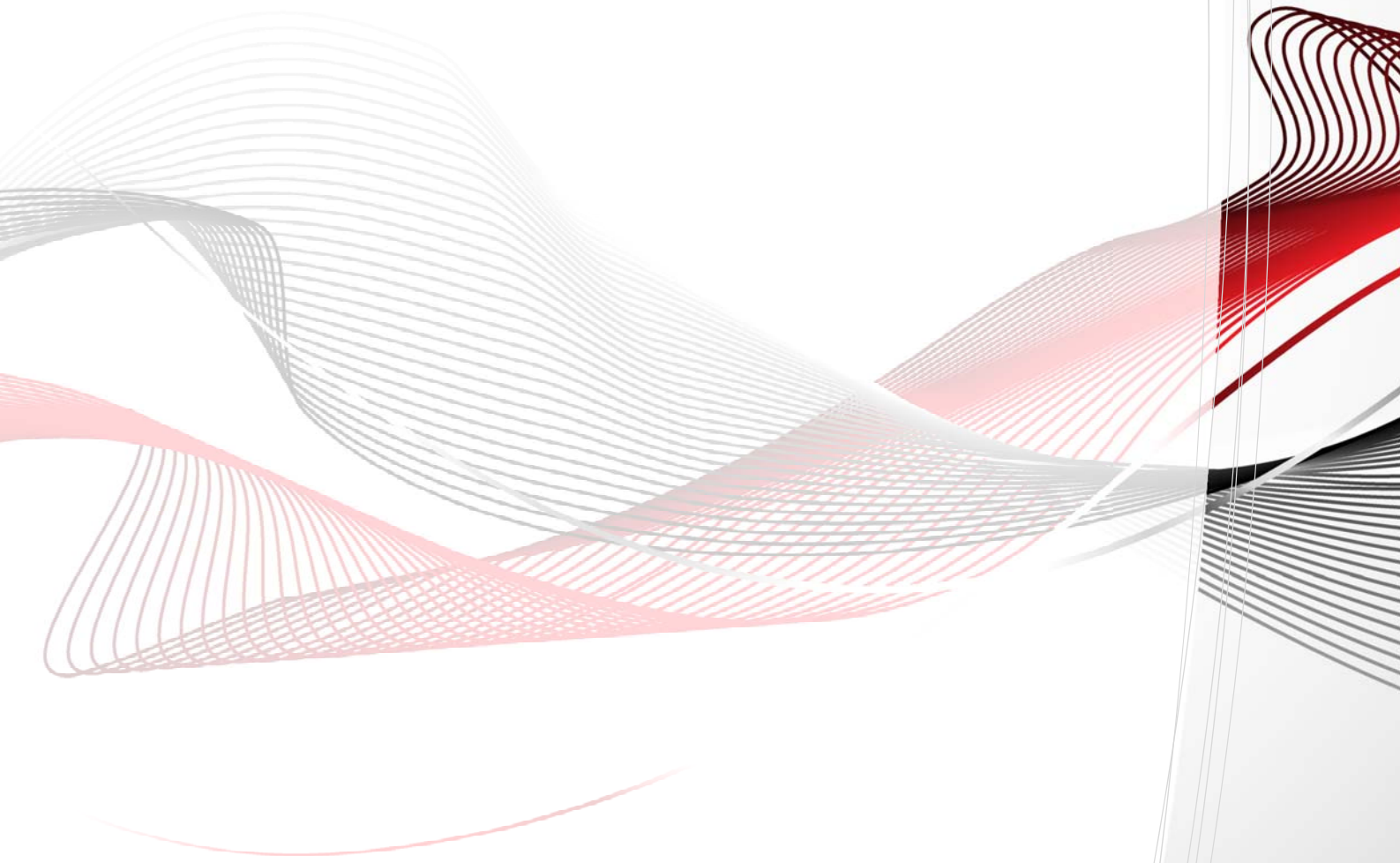
COI Solutions for DOCUMENTS

COI-BusinessFlow
Sicherheitskonzept

Business White Paper



1 Einführung

In einem großen Unternehmen mit einer sehr komplexen Verflechtung von Organisationsstrukturen und sehr hohen Anforderungen an die Integrität, die Authentizität, die Vertraulichkeit und die Verfügbarkeit der Daten sind spezielle Lösungen gefragt, welche diese Anforderungen optimal abdecken.

Im Rahmen dieses Dokumentes werden die Sicherheitsaspekte des COI-Business-Flow-Systems in Bezug auf Vertraulichkeit, Authentizität und Integrität beleuchtet. Des Weiteren werden die Maßnahmen gegen die Eingriffe von innen und außen vorgestellt.

2 Produkthighlights

Hier eine Übersicht der sicherheitsrelevanten Produkthighlights des COI-Business-Flow-Systems:

- Vertraulichkeit, Integrität und Authentizität
- Digitale Signatur
- Verschlüsselung
- Protokollierung aller Zugriffe
- Protokollierung der Änderungen in der Organisationsdatenbank
- Protokollierung der Änderungen der Systemkonfiguration
- Langfristige Archivierung unter höchsten Sicherheitsanforderungen
- Verfügbarkeit der Daten und Ausfallsicherheit, auch mehrere Betriebsstätten möglich
- Aufdeckung/Verhinderung von internen und externen Missbrauchsversuchen

3 Features

In diesem Kapitel werden die einzelnen sicherheitsrelevanten Funktionalitäten des Systems beschrieben.

3.1 Authentifizierung

Authentifizierung ist der Nachweis der Identität eines Benutzers gegenüber dem System. Dies erfolgt während der Anmeldung an dem COI-BusinessFlow System, dabei wird im SingleSignOn-Verfahren die Betriebssystemidentität des Benutzers verwendet. Während des Anmeldevorgangs erzeugt der Client eine Benutzeridentifikationsdatei, welche vom Server ausgewertet wird. Dabei wird die Identität des Benutzers auf Basis der Betriebssystem-Identität festgestellt. Das Verfahren beinhaltet keine interne Verwaltung von Passwörtern, das COI-BusinessFlow speichert lediglich die Passwörter für den Web-Client Zugang, wenn die Identifikation über Single-SignOn-Verfahren nicht möglich ist.

In den Umgebungen mit höheren Sicherheitsanforderungen werden für die Windowsanmeldung oft Smartcards und biometrische Verfahren eingesetzt. Durch das SingleSignOn-Verfahren wird die Windows-Authentifizierung automatisch auch für den Zugriff auf das COI-BusinessFlow angewandt, was einen zusätzlichen Schutz der vor den unbefugten Zugriffen auf die Archivdaten bietet.

3.2 Mehrstufiges Administrationsrechtekonzept

Das COI-BusinessFlow-System sieht für die Administratoren ein mehrstufiges Rechtekonzept vor. Die Systemadministrationsrechte sind feingranular nach zu administrierenden Teilbereichen aufgeteilt. Alle relevanten Administrationsaktivitäten werden protokolliert, sodass auch bei Administrationszugriffen alle Veränderungen der Zugriffsrechte, Organisationsstrukturen und Konfiguration lückenlos nachvollziehbar sind. Eine zeitnahe Meldung, dass dieses "Mehraugenprinzip" unterwandert werden könnte, wird durch das Intrusion Detection (siehe Kapitel 3.7) abgefangen.

Standardmäßig sind innerhalb von COI-BusinessFlow Administratorenrollen für folgende Bereiche vordefiniert:

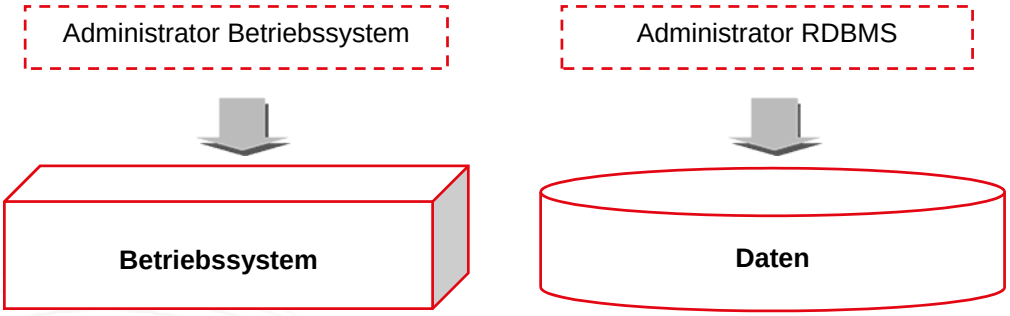
- Organisationsdatenbank
- Storage-Administration
- Workflow-Konfiguration
- Server-Konfiguration
- Konfiguration von Dokumentfamilien/ Attributen / Wortsystemtabellen
- Konfiguration von Hooks
- Systemeinstellungen

Die aufgelisteten Rollen können beliebig kombiniert werden. Dadurch können einer Person mehrere Rollen zugeordnet werden.

Auf der Betriebssystemebene ermöglicht COI-BusinessFlow die Umsetzung eines Konzepts, bei dem Manipulationen der Dokumente auf Betriebs- und RDBM-Systemebene verhindert werden. Organisatorisch sind folgende zwei Rollen vorzusehen:

- Rolle Betriebssystem-Administration
- Rolle RDBMS-Administration

Der Betriebssystem-Administrator hat Zugriff auf die Installationsverzeichnisse der Applikation und auf die Archivierungsmedien. Der RDBMS-Administrator hat Zugriff auf die verwendete Datenbankinstanz und damit auf die Daten von COI-BusinessFlow.



Um auch den unerlaubten Zugriff auf Dokumente von Seiten der Systemadministration zu verhindern, muss die Rolle Organisationsdatenbank-Administrators betrachtet werden. Diese verwaltet die Systembenutzer und deren Zugriffsberechtigungen, d. h. der Organisationsdatenbank-Administrator ist in der Lage beliebige Zugriffsrechte zu vergeben. Mit Hilfe der COI-BusinessFlow-Funktionen

- Protokollierung aller Anpassungen innerhalb der Benutzer-/Zugriffsrechteverwaltung

und

- Sicherheitskomponente „Intrusion Detection“ zur Prüfung/Meldung von Manipulationen innerhalb der Benutzer-/Zugriffsrechteverwaltung.

kann sichergestellt werden, dass mögliche Zugriffsverletzungen verhindert oder zumindest nachverfolgt werden können.

Mit Hilfe folgender COI-BusinessFlow-Funktionen kann sicherstellt werden, dass lesende Zugriffe oder mögliche Manipulationen auf Dokumente verhindert werden können:

- Durch die symmetrische Verschlüsselung der Dokumente (oder von Teilbereichen) wird sichergestellt, dass von Betriebssystemseite keine Lesemöglichkeit auf archivierte Dokumente besteht.
- Eine Manipulation der archivierten Dokumente wird einerseits durch Sicherung der archivierten Dokumente über MD5-Checksummen und andererseits durch den Einsatz von revisionssicheren Archivierungsmedien ausgeschlossen.

3.3 Digitale Signatur

Die Integrität der Daten spielt eine wichtige Rolle. Zum Schutz gegen Veränderung von Daten wird die digitale Signatur eingesetzt. Das Signaturgesetz (SigG) unterscheidet zwischen den folgenden Formen der digitalen Signatur: allgemeine elektronische Signatur, fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur.

Abbildung 1: Formen der digitalen Signatur

Einfache elektronische Signaturen (§ 2 Nr. 1 SigG) dienen dazu, den Urheber einer elektronischen Nachricht zu kennzeichnen, z. B. durch das Abspeichern einer eingescannten Unterschrift. Für einfache elektronische Signaturen sind keine Anforderungen bezüglich ihrer Sicherheit oder Fälschungssicherheit definiert, so dass diese Signaturen nur einen sehr geringen Beweiswert haben.

Für fortgeschrittene elektronische Signaturen (§ 2 Nr. 2 SigG) gelten höhere Anforderungen: Sie müssen eine Manipulation der Daten erkennbar machen, sich eindeutig einer natürlichen Person zuordnen lassen, die Identifizierung dieser Person erlauben und es ermöglichen, dass nur diese Person die erforderlichen Mittel zur Signaturerzeugung unter ihrer alleinigen Kontrolle halten kann. Insofern verfügen fortgeschrittene elektronische Signaturen grundsätzlich über einen etwas höheren Beweiswert. Die tatsächliche Sicherheit einer fortgeschrittenen elektronischen Signatur hängt jedoch von den eingesetzten Signaturverfahren, den verwendeten Komponenten und nicht zuletzt von der Sorgfalt der Anwender bei der Signaturerstellung ab. Im Streitfall muss der Anwender daher im Zweifel beweisen, dass die Signatur tatsächlich in diesem Sinne sicher erzeugt wurde.

Anders verhält sich dies bei der qualifizierten elektronischen Signatur (§ 2 Nr. 3 SigG), für deren Echtheitsüberprüfung ein Anscheinsbeweis gefordert wird. Bei dieser höchsten Sicherheitsstufe der elektronischen Signatur wird die Signatur ihrem Urheber über ein qualifiziertes Zertifikat (§ 2 Nr. 7 SigG) zugeordnet. Durch das qualifizierte Zertifikat, das von einem vertrauenswürdigen Zertifizierungsdiensteanbieter (§ 2 Nr. 8 SigG) signiert wird, wird die Zusammengehörigkeit zwischen dem öffentlich bekannten Signaturprüfschlüssel, der zur Prüfung der Signatur verwendet wird

(vgl. Abschnitt 3), und der Identität des Signaturschlüsselinhabers belegt. Der Zertifizierungsdiensteanbieter garantiert, dass die Angaben im qualifizierten Zertifikat und die Auskünfte seiner Verzeichnis- und Zeitstempeldienste korrekt sind und er die Anforderungen gemäß Signaturgesetz und Signaturverordnung erfüllt. Dazu gehört, dass der Zertifizierungsdiensteanbieter die sensiblen Zertifizierungsdienste in einer besonders geschützten Umgebung betreibt (Trust Center). Außerdem klärt der Zertifizierungsdiensteanbieter den Anwender über seine Sorgfaltspflichten im Umgang mit der Signatur auf. Zertifizierungsdiensteanbieter unterliegen der Aufsicht durch die Bundesnetzagentur und müssen dort im Rahmen ihrer Betriebsaufnahme und Betriebsanzeige Nachweise, Belege und Erklärungen einschließlich eines Sicherheitskonzepts einreichen, die die Erfüllung der gesetzlichen Anforderungen gemäß Signaturgesetz und Signaturverordnung dokumentieren.

Das COI-BusinessFlow-System unterstützt alle drei Formen der digitalen elektronischen Signatur. Abhängig von dem Anwendungsszenario wird projektspezifisch die geeignete Form eingesetzt.

3.3.1 Erfüllung der Anforderungen an die Qualifizierte Elektronische Signaturen

Das COI-BusinessFlow-System integriert die von der Bundesnetzagentur durch Herstellererklärung anerkannten Komponenten von Drittanbietern. Gemäß der Klassifizierung des §2 Nr. 13 SigG, handelt es sich dabei um Signaturanwendungskomponenten im Sinne des § 2 Nr. 11 des SigG, die Daten dem Prozess der Erzeugung Qualifizierter Elektronischer Signaturen zuführt. Durch die offene Programmierschnittstelle des COI-BusinessFlow-Systems können projektspezifisch auch kundenspezifische Signaturanwendungskomponenten integriert werden.

Das COI-BusinessFlow-System erfüllt in Verbindung mit den Einsatzbedingungen folgende Anforderungen an die Qualifizierten Elektronischen Signaturen:

- Identifikationsdaten zur Anwendung von Signaturschlüsseln werden ausschließlich auf der Signaturerstellungseinheit gespeichert. Der Zugriff auf die Signaturerstellungseinheit erfolgt über Chipkarten-Terminals, die über eigene Tastatur verfügen. Eine Preisgabe der Identifikationsdaten kann hierdurch ausgeschlossen werden (§15 Abs. 2 Nr. 1 a) SigV1).
- Nur dafür berechtigte Personen dürfen Signaturstempel benutzen (§15 Abs. 2 Nr. 1 b) SigV)
- Die Daten, auf die sich die zu erstellende Signatur bezieht, werden angezeigt (§17 Abs. 2 Satz 1und 3 SigG).
- Die Erzeugung der Signatur wird vorher eindeutig angezeigt (§15 Abs. 2 Nr. 1 c) SigV).
- COI-BusinessFlow berechnet den Hash-Wert
- COI-BusinessFlow übernimmt die geeignete Speicherung des signierten BusinessFlow-Dokuments.

[1] Verordnung zur elektronischen Signatur; SigV

Für die Prüfung von Qualifizierten Elektronischen Signaturen werden folgende Funktionen angeboten:

- Prüfung automatisch (bei jedem Zugriff auf ein Dokument) oder manuell
- Die Anzeige des signierten Dokuments bzw. der signierten Klassifizierungsdaten (§17 Abs. 2 SigG)
- Die Prüfung, ob die Daten insgesamt unverändert sind (Hash-Vergleich) (§17 Abs. 2 Nr. 2 SigG)
- Anzeige, welchem Signatur-Schlüsselinhaber die Signatur zuzuordnen ist, wenn eine persönliche Signatur vorliegt (§17 Abs. 2 Nr. 3 SigG)
- Das Zertifikat auf dem die Signatur beruht und zugehörige Attribute werden dem Benutzer auf Anforderung angezeigt (§17 Abs 2 Nr. 4 SigG).
- Eine erfolgreiche oder nicht erfolgreiche Prüfung der Signatur wird zuverlässig angezeigt (§15Abs. 2 Nr. 2 a) SigV).
- Anzeige ob das qualifizierte Zertifikat zum Signaturzeitpunkt noch nicht abgelaufen war und nicht gesperrt war (§17 Abs. 2 Nr. 3 SigG)
- Anzeige ob das qualifizierte Zertifikat zum Signaturzeitpunkt vertrauenswürdig war (Prüfung der Zertifikatskette) (§15, Abs. 2 Nr. 2 a), b) SigV)

Im Folgenden werden die typischen Einsatzszenarien wie das automatische Signieren beim Importieren der Dokumente in das Langzeitarchiv und das manuelle Signieren direkt nach dem Erstellen der Dokumente vorgestellt.

3.3.2 Automatisches Signieren beim Archivieren

Die erste Variante ist das automatische serverseitige Signieren der Dokumente beim Importieren in das System. Die Signaturdaten werden abhängig von der Konfiguration entweder in einer separaten Datei abgelegt oder direkt in dem Dokument integriert, mit diesen Daten kann ein Dokument jederzeit validiert werden.

3.3.3 Manuelles Signieren durch den Benutzer

Bei dem zweiten Einsatzszenario werden die Dokumente direkt durch den Ersteller signiert. Die Art der Signatur – von der einfachen bis hin zu qualifizierten Signatur - ist projektspezifisch zu konfigurieren. Durch die modulare Architektur ist das Einbinden von den meisten verfügbaren Lösungen für die Erzeugung von digitalen Signaturen möglich. Auch bei manuellem Signieren wird in den meisten Fällen eine zusätzliche Signaturdatei erzeugt, welche als zusätzliches Element in dem Dokument Container abgelegt wird. Das System stellt in der Oberfläche Funktionen zur Überprüfung der digitalen Signatur zur Verfügung.

Serverseitig werden die Signaturen zusätzlich bei jedem Zugriff auf das Dokument überprüft, bei Problemen werden entsprechende Fehlerberichte erzeugt.

3.3.4 Signieren von Klassifizierungsdaten

Neben dem Signieren von Dokumenten ist das COI-BuinessFlow-System in der Lage auch die Klassifizierungsdaten zu signieren. Die Daten werden in einem XML Container zusammengefasst und gemäß dem XML Signature[2] Standard signiert. Die Art der Signatur - von der einfachen bis hin zur qualifizierten Signatur - ist auch in diesem Einsatzszenario projektspezifisch zu konfigurieren. Die signierten Daten werden entweder im Ablagebereich der Dokumente oder in der Datenbank aufbewahrt.

Das Signieren der Klassifizierungsdaten kann sowohl automatisch als auch manuell erfolgen. Falls zu einem Dokument signierte Klassifizierungsdaten vorliegen, werden diese beim Zugriff auf das Dokument aufgelistet und können vom Benutzer eingesehen und verifiziert werden.

3.4 Verschlüsselung

Die strenge Verschwiegenheit, wie sie z. B. von Notaren gefordert wird oder in der Rechtsabteilung Ihres Unternehmens notwendig ist, wird durch die Anwendung von Verschlüsselung auch bei den elektronisch abgelegten Daten erreicht. Die Dokumente werden mit den modernen Verfahren verschlüsselt. Es ist zwischen symmetrischer und asymmetrischer Verschlüsselung zu unterscheiden. Das symmetrische Verfahren eignet sich sehr gut für die automatische Verschlüsselung, das asymmetrische Verfahren bietet höheren Schutz, bringt aber weitere Komplexität mit sich. COI-BusinessFlow unterstützt beide Verfahren. Die Wahl des für das Anwendungsszenario richtigen Verfahrens muss projektspezifisch erfolgen.

3.4.1 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung benutzt einen einzigen Schlüssel für die Ent- und Verschlüsselung von Daten. Der Schlüssel wird im COI-System zentral verwaltet und ist vor unbefugtem Zugriff geschützt. Der Schlüssel wird vom System für die automatische Verschlüsselung der im System abgelegten Dokumente verwendet. Jedes Dokument wird beim Importieren in das System automatisch verschlüsselt und ist somit vor unbefugtem Zugriff auf den Ablagebereich geschützt. Das System entschlüsselt die Dokumente automatisch bei einem entsprechenden autorisierten Zugriff.

3.4.2 Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung erfolgt nach dem Public/Private-Key Prinzip. Die Verschlüsselung ist mit dem öffentlichen Schlüssel möglich, welches allgemein bekannt ist, die Entschlüsselung ist allerdings nur mit dem privaten Schlüssel des Benutzers möglich. Das Verfahren eignet sich sehr gut, um die persönlichen Daten des Benutzers zu schützen, z. B. um die archivierten E-Mails nur für den Benutzer lesbar

[2] XML Signature Syntax and Processing; http://www.w3.org/Signature/

zu machen. In diesem Szenario werden die archivierten E-Mails vom System automatisch mit dem öffentlichen Schlüssel des Benutzers verschlüsselt. Einen Zugriff auf die E-Mails hat ab diesem Moment nur der Benutzer selbst, die Daten des Benutzers sind optimal geschützt.

3.5 Checksummenbildung

Mit der abgesicherten Dokumentenablage wird die Authentizität und Integrität der gespeicherten Dokumente unabhängig von den benutzten Archivierungsmedien sichergestellt. Im COI-BusinessFlow wird von jedem abgelegten Dokument eine MD5-Checksumme ermittelt und in der Datenbank gespeichert. Bei jedem Zugriff auf das Dokument wird dieses bei der Bereitstellung gegen die Checksumme geprüft und damit die Dokumentenechtheit sichergestellt.

Um sicherzustellen, dass dies auch während der Übertragung aus einem abgebenden System gewährleistet wird, müssen zusätzliche Informationen ausgetauscht werden. Im Fall einer dateisystembasierten Übergabe an COI-BusinessFlow, müssen MD5-Checksummeninformationen bzgl. der übergebenen Dateien mitgeliefert werden. Idealerweise findet die Bereitstellung der Checksummeninformationen über einen separaten Weg (z.B. Datenbankschnittstelle) statt. COI-BusinessFlow prüft während des Imports die vorliegenden Dateien gegen die übergebenen Informationen und stellt damit sicher, dass nur Originaldateien in das System Aufnahme finden.

3.6 Zugriffsprotokollierung

COI-BusinessFlow beinhaltet standardmäßig eine umfangreiche Zugriffsprotokollierung. Alle manipulierenden Zugriffe innerhalb des Archivsystems (Frontend und Server) werden in der Datenbank und im Dateisystem (Dokumentbezogen innerhalb der class.all) protokolliert.

Dokumentbezogen können folgende Ereignisse protokolliert werden:

- Ändern des Dokumentinhalts
- Ändern der Klassifizierung
- Ändern von Rechten (am Dokument)
- Ändern von Redlining-Layern
- Ändern des Status
- Ändern von Ordnerinhalten (bei Ordnern)
- Versenden des Dokuments (mit Empfängern)
- Erzeugen, Importieren, Scannen des Dokuments
- Exportieren, Auschecken und Einchecken von Dokumenten (mit der Möglichkeit den Empfänger und den Zweck einzutragen)
- Archivierung des Dokuments
- Lesender Zugriff auf ein Dokument
- Workflow-Aktivitäten

Konfigurationsbezogen können folgende Ereignisse protokolliert werden:

- Änderungen in der Organisationsdatenbank
- Änderungen in der Storage-Administration
- Änderungen in der Workflow-Konfiguration
- Änderungen in der Server-Konfiguration
- Änderungen an der Konfiguration von Dokumentfamilien/ Attributen / Wortsystemtabellen
- Änderungen an der Konfiguration von Hooks
- Änderungen der Systemeinstellungen

Zusätzlich zu der Zugriffsprotokollierung kann projektspezifisch die technische Protokollierung um die prozessbezogene Protokollierung ergänzt werden. Insbesondere beim Einsatz von Workflow-Prozessen können z. B. die Zusatzinformationen, welche zu der Entscheidung geführt haben, protokolliert werden. Bei einem Freigabeprozess könnte so der Grund für eine Freigabeablehnung protokolliert werden.

3.7 Intrusion Detection

Das COI-BusinessFlow-System beinhaltet ein Framework zum Implementieren der Eingriffserkennung. Das Framework besteht aus einer Reihe von Sensoren, die für das Sammeln von Daten zuständig sind. Die Sensoren liefern die Rohdaten an die Analysekomponenten. Diese entscheiden, ob ein Eingriff vorliegt und leiten die Ergebnisse an die Reaktionskomponente. Die Reaktionskomponente benachrichtigt den Administrator über einen vorliegenden Eingriffsfall.

Das System bietet standardmäßig folgende Sensoren-Implementierungen:

- Benutzer-Aktionen (Liste der Benutzeraktionen pro Zeitraum, z. B. der Benutzer hat ein Dokument angeschaut, zwei bearbeitet und zehn exportiert)
- Update-Server Aktionen (Liste der Gets/Puts/ …)

Das System bietet standardmäßig folgende Analyse-Implementierungen:

- Benutzer-Aktionen
- Update-Server-Aktionen

Das System bietet standardmäßig folgende Reaktion-Implementierungen:

- Administrator per E-Mail benachrichtigen
- Benutzer mit Eingriffsverdacht ausloggen
- Benutzer mit Eingriffsverdacht deaktivieren

Weitere ID-Module sind projektspezifisch zu definieren, z. B. möglich sind Sensoren zum Überwachen von Rechnungsfreigaben oder Analyse-Module abhängig von der Rechnungssumme.

COI Solutions for DOCUMENTS

COI-BusinessFlow -

die moderne ECM-Plattform aus dem Hause COI.

Ihr Vorteil: Einzigartige Integrationsfähigkeit,
umfassende Prozessoptimierung und
übergreifendes Informationsmanagement.
Mit diesen innovativen Lösungen werden Visionen von morgen
schon heute Realität.

COI – Consulting für Office und Information Management GmbH
Am Weichselgarten 23 – 91058 Erlangen
Telefon: +49 (0)9131 / 9399 0 - Telefax: +49 (0)9131 / 9399 4959
E-Mail: info@coi.de
Web: www.coi.de