COI-BusinessFlow
Verschlüsselung

Business White Paper

1 Zusammenfassung

Die Sicherung der Unternehmensdaten und -informationen hat in jedem Unternehmen höchste Priorität. Durch den heute oftmals weltweiten Zugriff auf Unternehmensdaten aus unterschiedlichsten Umgebungen und Netzwerken heraus, steigen die Anforderungen an die Datensicherheit ständig.

Folgende Fragen stehen bei der Sicherheit der Datennutzung im Vordergrund:

- Wie können Daten gegen den Zugriff Dritter geschützt werden?
- Wie lassen sich Informationen, neben den Berechtigungsmechanismen, systemweit durchgängig bis in die Administration inhaltlich schützen?
- Wie wird die dezentrale Datennutzung vor Datenmissbrauch geschützt?
- Wie können Datennutzungsabweichungen erkannt und Schutzmechanismen entsprechend aktiviert werden?

COI-BusinessFlow bietet zwei neue Sicherheitsmodule, welche den Schutz der Daten gewährleisten und die Antwort auf die oben genannten Fragen geben.

- COI-BusinessFlow Verschlüsselung auf der Basis AES256
- COI-BusinessFlow Intrusion Detection (siehe separates Business White Paper)

2 Einführung

Die Kryptographie, welche auch als Lehre vom Ver- und Entschlüsseln von Nachrichten verstanden wird, beschäftigt sich mit der Codierung von Daten. Das Ziel ist die Vertraulichkeit der Daten, hier im Bezug Anwenderdatennutzung in Verbindung mit der ECM-Software COI-BusinessFlow, zu gewährleisten. Im Fokus steht dabei der Ausschluss nicht autorisierter Dritter und der Schutz der Daten durch den Mechanismus der Verschlüsselung bei der Datenablage und der Entschlüsselung bei der autorisierten Datennutzung. Technisch werden die lesbaren und interpretierbaren Daten über ein kryptographisches Verfahren in ein nicht direkt lesbares Datenformat gewandelt. Die Entschlüsselung erfolgt in Verbindung mit dem passenden Schlüssel, der in COI-BusinessFlow direkt integriert und damit gegen Missbrauch geschützt ist.

Große Bedeutung hat die Kryptographie heute in den Bereichen Kopierschutz zur Wahrung des Urheberrechts und zum Schutz von digitalen Daten und Nachrichten, z. B. im Bereich des E-Mail-Managements.

Im Umfeld der ECM-Anwendungen geht es in erster Linie um den Schutz der kritischen Unternehmensinformationen, sowohl intern, als auch bei der externen Nutzung.

2.1 Technologiebasis

Die Verschlüsselungskomponente der COI-BusinessFlow Plattform basiert auf dem Advanced Encryption Standard (AES). Diese Technologie war der Gewinner des 1997 von der US Regierung durchgeführten Auswahlverfahrens zur Datenverschlüsselung. AES setzte sich damals gegen den älteren Data Encryption Standard (DES) durch, welcher durch seine geringe Schlüsselgröße und der notwendigen Rechnerperformance als zu schwach bewertet wurde. Im Herbst 2000 wurde der AES als der zukünftige Standard bewertet und ausgewählt. Basis war eine modifizierte Version des AES Rijndael.

Rijndael, benannt nach seinen Entwicklern Joan Daemen und Vincent Rijmen, ist ein symmetrisches Kryptosystem auf symmetrischer Basis (sog. Blockchiffre). Der Algorithmus selbst arbeitet mit festgelegten Bitgruppen (Blöcke). Es werden Eingabeblöcke mit einer definierten Größe verarbeitet und ein dazu korrespondierender Ausgabeblock der gleichen Größe generiert. Entspricht die Länge des Eingabestroms nicht einem Vielfachen der Blockgröße, wird diese Länge durch Anfügen von 0x00 Bytes an den Intermediärstrom erreicht. Der verschlüsselte Ausgabestrom erhält am Anfang einen zusätzlichen Header, der 14 Byte lang ist und mit COI_AES beginnt. Die Entschlüsselung benötigt denselben Schlüssel wie die Verschlüsselung, um die Datenblöcke wieder zurück zu transformieren. Header und Füllbytes werden dem entschlüsselten Ausgabestrom entzogen.

Wesentliche Kriterien der Rijndael-Verschlüsselung sind die Effizienz, sowie die mathematisch elegante und einfache Struktur. Der zusätzlich geringe Ressourcenbedarf beim Einsatz der Technologie bietet unterschiedlichen Möglichkeiten der Integration.

2.2 Geschwindigkeit

Die Rijndael-Verschlüsselung ermöglicht eine sehr schnelle Implementierung. Der Algorithmus hat eine gute gleichbleibende Performance und ist aus diesem Grund die ideale Erweiterung für die Verschlüsselung von Daten in Verbindung mit der COI-BusinessFlow ECM-Plattform.

2.3 Speicherbedarf

Die Rijndael-Verschlüsselung hat nur geringe Anforderungen an die eingesetzte Hardware (RAM-Speicher). Auch aus diesem Grund ist diese Verschlüsselungstechnologie sehr gut geeignet für die performante Integration in das Leistungsspektrum einer ECM-Umgebung. Der Verschlüsselungsalgorithmus bietet auch die Option der separaten Berechnung der Schlüsselerzeugung „on-the-fly“.

2.4 Verschlüsselung

Rijndael ist, wie bereits kurz beschrieben, eine Blockchiffre. Es können Block- und Schlüssellänge unabhängig voneinander die Werte 128, 160, 192, 224 oder 256 Bits erhalten, während bei AES die Einschränkung der festgelegten Blockgröße von 128 Bit und der Schlüsselgröße von 128, 192 oder 256 Bit gilt. Es wird dabei jeder Block zunächst in eine zweidimensionale Tabelle mit vier Zeilen geschrieben, deren Zellen ein Byte groß sind. Die Anzahl der Spalten variiert je nach Blockgröße von 4 (128 Bits) bis 8 (256 Bits). Jeder Block wird nacheinander bestimmten Transformationen unterzogen. Rijndael wendet verschiedene Teile des erweiterten Originalschlüssels nacheinander auf den Klartext-Block an und verschlüsselt so die abzulegenden Daten.

2.5 Entschlüsselung

Bei der Entschlüsselung von Daten wird rückwärts, bezogen auf den Vorgang der Verschlüsselung, vorgegangen. Die Daten werden aus den zweidimensionalen Tabellen gelesen und die dafür notwendigen Rundenschlüssel generiert. Begonnen wird mit der Schlussrunde. Alle Funktionen werden je Runde in der umgekehrten Reihenfolge aufgerufen. Die meisten Funktionen zum Entschlüsseln unterscheiden sich nicht von denen der Verschlüsselung. Die entschlüsselten Daten werden dem Anwender direkt in der COI-BusinessFlow-Umgebung zur Verfügung gestellt.

3 Verschlüsselung mit COI-BusinessFlow

Als ECM-Plattform mit den Standardfunktionsbereichen Archivierung und Dokumentenmanagement steht die Sicherheit der verwalteten Daten an erster Stelle. Revisionssichere Archivierung ermöglicht die über Jahre hinweg unveränderbare Speicherung von Unternehmensdokumenten und –informationen. In Verbindung mit dem Modul COI-BusinessFlow Verschlüsselung erhalten die Daten einen zusätzlichen Schutz. In Kombination mit der umfangreichen Rechte- & Rollentechnologie der COI-Plattform werden Informationen durchgängig gegen unberechtigte Nutzung Dritter geschützt. Dabei haben die Aspekte der Datensicherheit und des Datenschutzes höchste Priorität.

Mit der verschlüsselten Ablage der Objekte werden die Daten im Dateisystem so geschützt, dass beim direkten Auslesen der verschlüsselten Daten ohne Entschlüsselung aus dem Dateiinhalt keine inhaltlichen Informationen gewonnen werden können.

3.1 Beschreibung

COI-BusinessFlow ermöglicht die Aktivierung eines systemweiten Serverdienstes zur Ver- und Entschlüsselung der abgelegten Daten. Der Zugriffsschutz, gesteuert über die Berechtigungen der einzelnen User, Usergruppen und Organisationseinheiten, wird dabei mit der Verschlüsselungstechnologie verknüpft.

Bei der Ablage der Daten erfolgt eine Verschlüsselung der Dokumentinhalte und der Klassifizierungsfiles. Die Verschlüsselung basiert auf der Advanced Encryption Standard (AES) 256-Bit-Verschlüsselung. Die Verschlüsselung erfolgt als Serverdienst automatisch im Hintergrund. Der Anwender wird in seinen Arbeitsabläufen davon nicht eingeschränkt. Dabei wird die Funktion der Ver- und Entschlüsselung administrativ zentral geregelt. So können unnötige Performance-Einschränkungen umgangen werden.

Das Verschlüsselungsverfahren ist ein fester Bestandteil des COI-BusinessFlow. Der Schlüssel wurde in den Softwarecode integriert und ist so vor unbefugtem Zugriff geschützt. Bestandsdaten oder Migrationsdaten (z. B. Datenübernahme aus anderen ECM-Plattformen) unterstützt COI-BusinessFlow ebenfalls umfangreich. COI-BusinessFlow erlaubt einen gemischten Betrieb mit verschlüsselten und unverschlüsselten Dokumenten.

3.2 Funktionsübersicht

- Symmetrische Verschlüsselung auf Basis AES256
- Verschlüsselung von Dokumentinhalten und Klassifizierungsfiles
- Automatische systemseitige Verschlüsselung
- Ver- und Entschlüsselung läuft automatisch im Hintergrund
- Nutzung der Verschlüsselung ist optional (ein-/ausgeschaltet)
- Feste Integration des AES256-Verfahrens im COI-BusinessFlow ECM-System
- Schutz des Schlüssels vor unbefugtem Zugriff
- Möglichkeit des gemischten Betriebs mit verschlüsselten und unverschlüsselten Daten in einer Umgebung

4 Resümee

Mit der Integration der Verschlüsselungstechnologie AES256 ermöglicht COI-BusinessFlow, zusätzlich zum Leistungsumfang der unveränderbaren und revisionssicheren Datenarchivierung, einen umfassenden Daten- und Dokumentschutz. Die Berechtigungsstrukturen der COI-Anwendung erlauben die gezielte Nutzung der Daten an den jeweils dafür zugelassenen und vorgesehenen Einheiten und unterbinden den unberechtigten Zugriff durch Dritte.

Dies trägt zu einem wesentlichen Schutz des Unternehmenswissens und der in der ECM-Umgebung abgelegten Daten und Informationen bei. Der Sicherheitsstandard des COI-BusinessFlow wurde durch die Integration der AES256-Technologie in Verbindung mit der ebenfalls neuen Funktion Intrusion Detection des COI-BusinessFlow umfangreich ausgebaut.

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