Department of Health and Human Services

Centers for Medicare & Medicaid Services
IT Modernization Program

Siebel 7.7 Guidelines

Version 1.1

March 3, 2006

Table of Contents

List of Figures

List of Tables

1. Introduction

As part of the Information Technology (IT) Modernization initiative, the Centers for Medicare & Medicaid Services (CMS) is migrating to a three-zone, web-enabled, and secure infrastructure based on a standard set of criteria documented in the CMS Internet Architecture. This document, *Siebel 7.7 Guidelines*, is one in a series of guidance documents that provide recommendations for achieving architecturally compliant solutions for successfully integrating commercial off-the-shelf (COTS)-based applications into the CMS Internet Architecture. This set of guidelines presents specific recommendations for so deploying Siebel 7.7.

To the extent practicable, these *Guidelines* prescribe specific implementation detail and conventions. They are by no means all inclusive. Where appropriate, the recommendations in this document should be adapted to individual projects based on the cost, complexity, and criticality of the proposed solution.

The intended audience for the *Siebel 7.7 Guidelines* includes teams involved in system development, project managers, and those CMS IT offices, government contractors, and product vendors participating in the COTS product reviews.

1.1 Document Organization

This document is organized as follows:

Section		Purpose
Section 2:	Siebel 7.7 Products	Identifies the Siebel 7.7 products addressed in these *Guidelines.*
Section 3:	Siebel 7.7 Architecture and Components	Describes the architectural requirements and components (hardware, software, gateway, security, and database) for the Siebel 7.7 implementation within a three-zone Internet Architecture.
Section 4:	Siebel Integration With J2EE Applications	Describes the access to J2EE components from Siebel applications and the creation of Java/J2EE components to access Siebel objects.
Section 5:	Recommended Configuration of Siebel 7.7	Presents the recommended configuration of hardware and software and components, including security and encryption, for Siebel 7.7
Acronym List		Defines the acronyms used in this document.
List of References		Presents the references used in the preparation of this document.

2. Siebel 7.7 Products

CMS has licensed the following Siebel products:

- Siebel Healthcare Call Center 7 Base
- Siebel Advanced Search 7
- Siebel Reports 7
- Siebel SmartScript 7
- Siebel Healthcare Providers and Facilities 7
- Siebel Personal Lines Claims 7
- Siebel Proposals & Presentations 7 for Financial Services.

The base product in this listing is Siebel Healthcare Call Center; the others are add-on modules.

All Siebel products are extensions of Siebel Customer Relationship Management (CRM) solutions. The Siebel "verticals," such as Siebel Healthcare Call Center, are identical from a deployment and configuration perspective. Therefore, this document does not discuss any particular Siebel product.

3. Siebel 7.7 Architecture and Components

Figure 1, courtesy of Siebel Systems, Inc.,[1] depicts an example deployment of Siebel components. The Siebel 7.7 Architecture consists of:

- Web Clients
  - Siebel Web Client
  - Siebel Mobile Client
  - Siebel Wireless Client
  - Siebel Handheld Client
- Web Server Extension
- Siebel Enterprise Server
  - Siebel Servers
  - Application Object Manager
  - Siebel Gateway Name Server
- Siebel Database
- Siebel File System
- Siebel Enterprise Integration Management
- Siebel Enterprise Application Integration.

The following subsections provide a description of these components.

3.1 Siebel Web Clients

The various Web Clients available in Siebel 7.7 consist of the Siebel Web Client, Mobile Web Client, Wireless Client, and Handheld Client. The following subsections describe each web client and, where applicable, the installed software, application connection, and database connection.

3.1.1 Siebel Web Client

The Siebel Web Client runs in a standard browser on the end user's client computer. ActiveX controls and JavaScript routines are downloaded to the browser automatically when the user runs a Siebel application in Siebel high-interactivity mode. The browser connects through a web server to the Siebel Server, which executes business logic and accesses data from the Siebel Database. Only the user interface layer of the Siebel eBusiness Applications architecture resides on the user computer.

[1] *Siebel 7 eBusiness Deployment Planning Guide*, Version 7.7, Revision A, May 2004, p. 10.

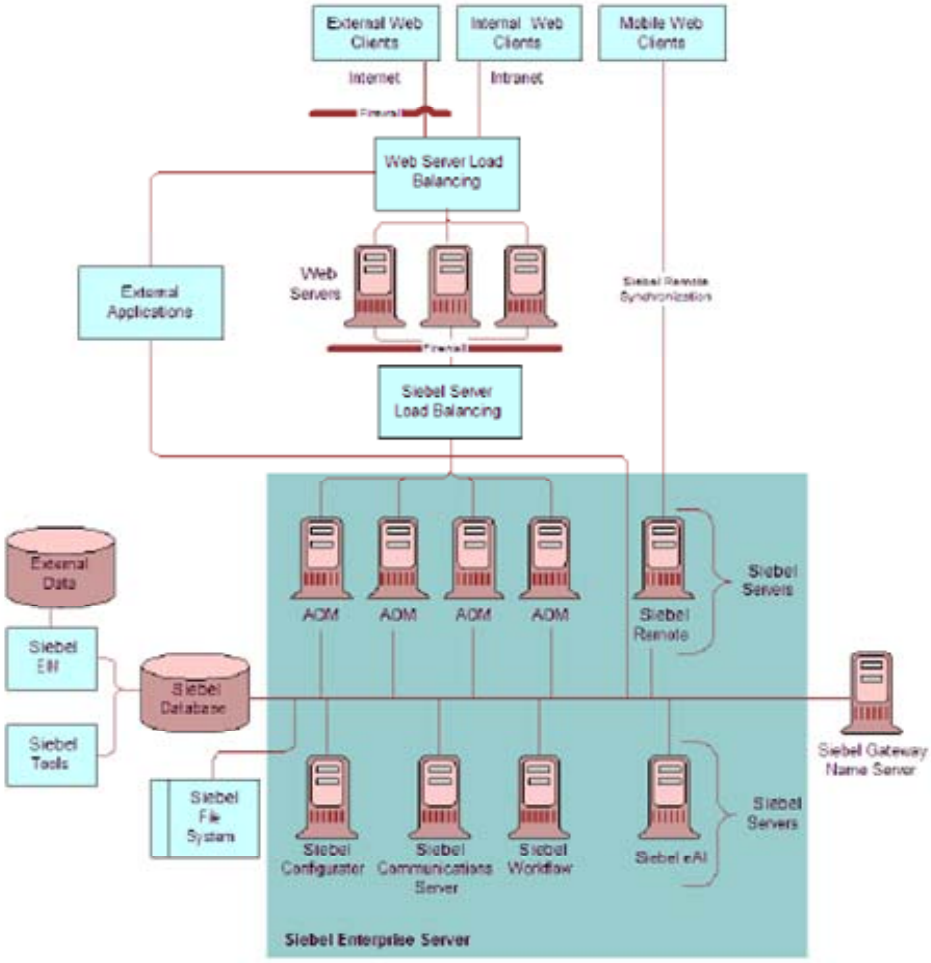

Figure 1. Example of a Siebel Deployment

The Siebel Web Client software, application, and database characteristics are as follows:

- **Installed software.** No additional application software is required on the client. The Siebel Web Client requires only a web browser.
- **Application connection.** Applications run on a Siebel Server(s) and forward pages to the client via a web browser.
- **Database connection**. No Siebel Database or database client is installed on the client. All data are accessed from the remote Siebel Database by the Siebel Server.

3.1.2 Siebel Mobile Web Client

The Siebel Mobile Web Client software, application, and database characteristics are as follows:

- **Installed software.** Windows-based software containing Siebel applications and related services is installed on each client.

- **Application connection.** Applications run on each client. Applications are displayed in a web browser.
- **Database connection.** A Siebel Database and Siebel File System are installed on each client. Applications access the client's local database.

Users periodically carry out a remote data synchronization using Siebel Remote. Users synchronize the Mobile Web Client's local database and Siebel File System to a remote Siebel Enterprise Server's Siebel Database and Siebel File System. Through Siebel Remote, users connect directly to the remote Siebel Database and Siebel File System without going through the Enterprise Web Servers or Siebel Servers.

3.1.3 Siebel Wireless Client

The Siebel Wireless Client is a modified Siebel Web Client that runs on a mobile device. Users can view, edit, and create records in the Siebel Database through a wireless connection between a mobile device and a web server. A wireless device—such as an Internet-enabled mobile phone or personal digital assistant (PDA)—communicates by wireless application protocol (WAP) to a wireless gateway server, which in turn translates HyperText Transport Protocol (HTTP) messages into WAP. The Siebel interface is rendered on the mobile device using wireless markup language (WML). Siebel Wireless Client also supports specific eXtensible Markup Language (XML) and HTTP-based wireless browsers.

3.1.4 Siebel Handheld Client

The Siebel Handheld Client is a streamlined version of the Siebel Mobile Web Client. The Handheld Client includes only the functionality required by end users' field technicians. It supports the same data relationships and much of the same functionality as the Siebel Mobile Web Client. The Siebel Handheld runs on devices that support the Windows CE operating system.

3.2 Siebel Web Server Extension

The Siebel Web Server Extension (SWSE) is a plug-in for third-party web servers. It identifies requests for Siebel information coming from Web clients and flags these requests for routing to a Siebel Server. When information is sent from the Siebel Server back to the Web client, SWSE helps complete the composition of the web page for forwarding to the Web client.

Siebel Web Server Extension includes the Siebel load balancing module. This module provides round-robin load balancing for Application Object Managers (AOM) running on Siebel Servers.

3.3 Siebel Enterprise Server

The Siebel Enterprise Server is a logical grouping of Siebel Servers that connect to one Siebel Database. All Siebel Servers in a Siebel Enterprise Server are configured, managed, and monitored as a single logical group. Consequently, the Siebel administrator can start, stop, monitor, or set server parameters for all Siebel Servers within the Siebel Enterprise Server.

3.3.1 Siebel Servers

The Siebel Enterprise Server consists of one or more Siebel Servers. Siebel Servers function as application servers and are composed of server components. Each server component performs a defined function.

Server components or groups of components determine what applications and services a Siebel Server supports. Components run in one of three modes:

- **Interactive mode.** Interactive components start tasks automatically in response to user requests, and the tasks end when a user ends the session. Typical interactive mode tasks are the Synchronization Manager and all AOMs.
- **Background mode.** Background components handle background processing tasks. Typically, background tasks are called by interactive mode tasks. Background tasks run until explicitly shut down. Customary background tasks are Transaction Router and Workflow Monitor Agent.
- **Batch mode.** Batch mode components handle processing of asynchronous work requests. When the task is complete, the component exits. Database Extract and Enterprise Integration Manager are examples of batch mode components. Since many of the Siebel Server components operate on multiple Siebel Servers simultaneously, Siebel applications can scale across many Siebel Servers to support large numbers of users.

3.3.1.1 Additional Functionality

Other Siebel Server components provide functionality that extends beyond application support. This additional functionality includes:

- Siebel Mobile Web Client synchronization
- Integration with legacy or third-party data
- Automatic assignment of new accounts, opportunities, service requests, and other records
- Workflow management
- Document generation
- Siebel Connection Broker (SCBroker). This server component provides load balancing for multiple AOMs running on the same Siebel Server.

3.3.1.2 Implementation

The Siebel Server runs as a system service under Windows and as a process under UNIX. Whether as a system service or process, Siebel Server monitors and controls the state of all server components operating on it. Each Siebel Server is thus one instantiation of the Siebel Server system service or process within the current Siebel Enterprise Server.

Interactive mode and *batch mode* components can be configured to run as multiple processes or as multithreaded processes. *Background mode* components run as multiple processes only.

3.3.2 Application Object Manager

One of the most important types of server components is the Application Object Manager. The AOM server components run in interactive mode. These components process user requests and are application or service specific. For example, the Siebel Employee Relationship Management component group contains the Employee Relationship Object Manager. This Application Object Manager provides the session environment in which this application runs.

AOMs also contain a data manager, and the Siebel Web Engine. Upon receipt of a user request to start an application, an AOM does the following:

- The business object layer starts an application user session, processes any required business logic, and sends a data request to the data manager
- The data manager creates a Structured Query Language (SQL) query and forwards it the database server
- The data manager receives the data from the database and forwards it to the business object layer for additional processing
- The business object layer forwards the result to the Siebel Web Engine, which helps create the user interface (UI) for the data. The Siebel Web Engine then forwards the web pages to the Siebel Web Server Extension on the Web server.

3.3.2.1 Implementation

An AOM server component is implemented as a multithreaded process on the Siebel Server. At runtime, a parent process starts one or more AOMs as multithreaded processes according to the AOM configuration. The terms “multithreaded server” or “MT server” are alternative terms for the multithreaded process.

Each thread in an AOM hosts tasks that are typically linked to one user session. These threads may be dedicated to particular user sessions or they may serve as a pool that can be shared by user sessions. For each AOM, a few threads are dedicated to housekeeping functions.

Each AOM task uses the Siebel Server to communicate with the Siebel Database, the Web server (through the SWSE), and other Siebel Enterprise Server components as follows:

- **Communication with the Siebel Database** uses Open Database Connectivity (ODBC) database connections. Database connections can be managed and tuned for optimal performance. The Siebel administrator has the option to configure connection sharing for database connections.
- **Communication with the Siebel Web Server Extension** uses SISNAPI [Siebel Internet Session Application Programming Interface (API)], a Siebel messaging format that runs on top of the Transmission Control Protocol/Internet Protocol (TCP/IP). SISNAPI connections may be configured to use encryption and authentication based on Secure Sockets Layer (SSL).
- **Communication with other Siebel Enterprise Server components** (including other Siebel Servers) also use SISNAPI
- The SCBroker on each Siebel Server listens on a static, configurable TCP port for requests coming from the Web server. SCBroker forwards these requests to AOMs.

3.3.3 Siebel Gateway Name Server

The Siebel Gateway Name Server is the dynamic address registry for Siebel Servers and components. At startup, a Siebel Server within the Siebel Enterprise Server stores its network address in the Gateway Name Server's nonpersistent address registry.

Siebel Enterprise Server components query the Gateway Name Server address registry for Siebel Server availability and address information. When a Siebel Server shuts down, this information is cleared from the address registry.

The Gateway Name Server also includes a persistent file (siebns.dat) containing Siebel Server configuration information, including:

- Definitions and assignments of component groups and components
- Operational parameters
- Connectivity information.

Whenever this information changes, such as during the installation or configuration of a Siebel Server, it is written to the configuration file on the Gateway Name Server.

In a production environment, there can be only one Gateway Name Server installed per machine. The same Gateway Name Server should not be shared for development, test, and production environments.

3.4 Siebel Database

The Siebel Database is a third-party relational database management system (RDBMS). It stores database records, including Siebel tables, indexes, and seed data. The Siebel Database uses ODBC database connections for all communications. The Siebel administrator can manage and tune these connections for optimal performance and can configure them for connection sharing.

3.5 Siebel File System

The Siebel File System is a shared file system directory. The Siebel File System stores document files, Siebel Configurator models, Web template definitions, and other files not appropriate for database storage.

The File System Manager (FSM), a Siebel Server component, manages all file requests from other Siebel Server components, such as Application Object Managers.

3.6 Siebel Enterprise Integration Management

Siebel Enterprise Integration Manager is Siebel's Extract, Transform and Load (ETL) tool. Siebel EIM is designed for batch processing data (import or export), and is capable of high-speed data migration.

Siebel EIM manages the bidirectional exchange of data between the Siebel Databases and other corporate databases. This exchange is accomplished through intermediary tables called EIM tables; in earlier releases, these tables were known as Interface Tables. The Siebel EIM tables act as a staging area between the Siebel application database and other databases.

The EIM is required for performing bulk imports, exports, updates, and deletes. Siebel Systems does not support the use of native SQL to load data directly into Siebel base tables (those tables targeted to receive the data).

3.7 Siebel Enterprise Application Integration

Siebel EAI provides components for integrating Siebel eBusiness Applications with external applications and technologies. The Siebel EAI is designed to work with such third-party solutions IBM, CrossWorlds, TIBCO, Vitria, SeeBeyond, webMethods, and others.

Siebel EAI provides bidirectional real-time and batch solutions for integrating Siebel applications with other applications. It also includes tools for cross-application integration through the Siebel Universal Applications Network (UAN).

Siebel EAI is designed as a set of interfaces that interact with each other and with other components within the Siebel application. These interfaces are compatible with IBM WebSphere MQ; Microsoft MSMQ, BizTalk, and OLE DB; Sun Microsystems Java and J2EE (Java 2 Platform, Enterprise Edition); XML, and HTTP; and many other standards.

The Siebel EAI interfaces provide the following features:

- Allow a flexible, service-based architecture to be built on top of configurable messages using XML and other formats
- Expose internal Siebel Objects to external applications
- Provide compatibility with prebuilt adapters and enterprise connectors, as well as with third-party adapters and connectors
- Allow for data transformation
- Integrate external data through Virtual Business Components (VBC)
- Provide a graphical business process designer, programmatic interfaces, and a high-volume batch interface.

4. Siebel Integration With J2EE Applications

Siebel eBusiness Applications provide standards-based technologies that allow developers to access J2EE components from Siebel applications and support the creation of Java/J2EE components to access Siebel objects.

4.1 Accessing Java/J2EE Components From Siebel Applications

Siebel eBusiness Applications provide three mechanisms for invoking Java/J2EE components—Java Server Pages (JSP), Servlets, or Enterprise Java Beans (EJB):

- Web Services
- Outbound HTTP adapter
- Java Business Service.

Web Service

When interacting with J2EE components published as a Web Service, Siebel applications can process the WSDL (Web Service Description Language) document that describes the service and operations, and then generate a proxy Business Service. This allows the Siebel eBusiness Application to invoke the Web Services like a local object. When the Business Service is invoked, the Object Manager detects that the Business Service is a proxy to a Web Service and generates the appropriate SOAP (Simple Object Access Protocol) message. The Business Service then dispatches the request using a configured transport such as HTTP.

Outbound HTTP Adapter

Siebel EAI also allows the developer to interact with J2EE components using the Outbound HTTP transport adapter. This adapter is used when including external content within the Siebel user interface, or when the desired component does not support a Web Service interface (SOAP or WSDL).

Java Business Service

The Java Business Service allows the sending or receiving of messages though a Java Messaging Service (JMS). The JMS Receiver server component allows the asynchronous receipt of messages in a fashion identical to the MQ Series Receiver component. The only difference is that in this instance the user is employing EAI JMS Business Service rather than EAI MQSeries Server Transport.

Developers can create custom business services in Java (and accessed from the Siebel code) within the Java Business Service. The Java Business Service uses the Java Native Interface API provided by Java Virtual Machines (JVM) and native code interaction.

4.2 Accessing Siebel Applications From a Java/J2EE Component

Java/J2EE components can request information from Siebel applications using a variety of methods, including:

- Siebel Java Data Bean (JDB)
- Siebel Resource Adapter
- Web Services
- Java Message Service.

Java Data Bean

The Java Data Bean is a collection of Java classes that allow developers to interact with a variety of Siebel objects such as business objects and business components. Using this interface, developers can develop Java/J2EE components that interact with Siebel applications.

Siebel Resource Adapter

The Siebel Resource Adapter plays a central role in the integration and connectivity between Siebel applications and a Java application server. It serves as the point of contact between application components, application servers, and enterprise information systems. A resource adapter must communicate with other components based on well-defined contracts that are specified by the J2EE Connector Architecture.

Web Services are emerging as an important technology for exposing application functionality independent of the underlying technology used to provide that functionality. Siebel Release 6.x introduced the notion of Business Services that could be invoked through XML over HTTP and WebSphere MQ. This functionality is now the basis for supporting Web Services. Siebel eBusiness Applications provide support for SOAP and WSDL. These two standards provide the basis for Web Services and allow for interoperability between J2EE and Siebel eBusiness Applications.

The Java Message Service is a standard Java API for accessing enterprise messaging systems. As part of the J2EE, JMS permits Java applications to create, send, receive, and read messages using a messaging product. JMS also allows for a loosely coupled interaction between J2EE applications and any other system capable of messaging. JMS is required for use whenever an enterprise messaging vendor supplies a JMS provider.

5. Recommended Configuration of Siebel 7.7

This section presents the recommended configuration for the deployment of Siebel 7.7 in a CMS Internet Architecture-compliant implementation. The recommended configuration includes the hardware and software, gateways, security, and data architectural components.

5.1 Siebel 7.7 Components by Zone

Figure 2 shows the recommended configuration of Siebel 7.7 components mapped to the CMS 3-Zone Internet Architecture. The configuration within the three zones (Presentation, Application, and Data) is as follows:

- **Presentation Zone.** The Presentation Zone is where Siebel Web servers and Web server load balancers reside. The Siebel Web Server Extension is installed on the Web server machine. This zone is where the external network first interacts with the Siebel environment.
- **Application Zone.** The components that reside inside the Application Zone include Siebel Servers and the Siebel Gateway Name Server.
- **Data Zone.** The Siebel Database, Siebel File System Manager, and Database Server reside in this zone.

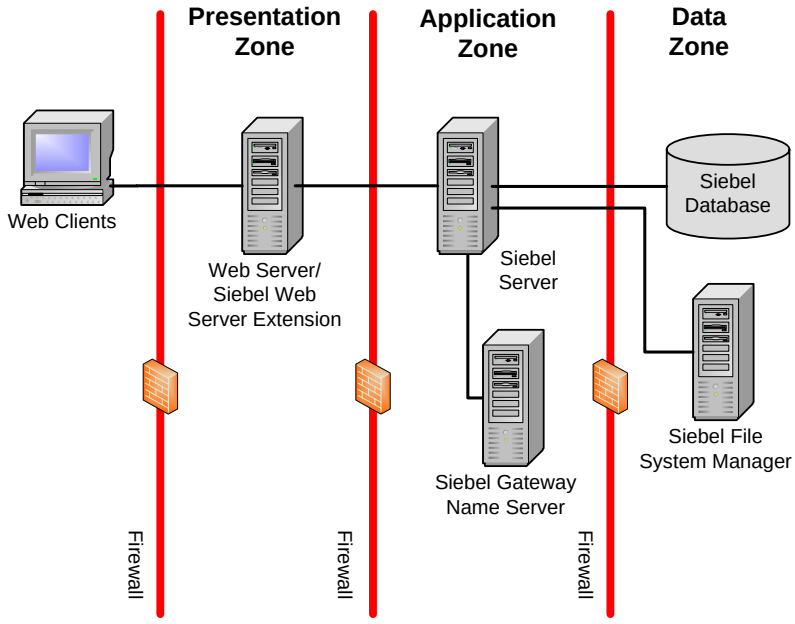

Figure 2. Placement of Siebel 7.7 Components Within the CMS Internet Architecture

5.2 Hardware and Software Recommendations

Siebel 7.7 will run on the Sun Solaris platform within the CMS Internet Architecture. The various Siebel server components can reside on multiple machines. Table 1 lists specific minimum hardware and software requirements for configuring Siebel 7.7 in a UNIX environment.

Table 1. Hardware/Software Requirements (UNIX Environments)

Requirement	Hardware/Software Recommendation
Operating System	Sun Solaris 8, 9 Recommended Patch Cluster DATE: May/31/04 (kernel at level 117171-02 or above). Must include C++ Run time patch level 111711-10 and Linker Patch level 112963-12 or above running on UltraSPARC processors or SPARC64 processors compatible with the V9 plus instruction set.
Web Servers	IBM HTTP Server v. 2.0.47 or above
Java Runtime Environment (JRE)	Sun 1.4.1_02 or above
Databases Supported	• IBM DB2 Universal Database (UDB) 7.2 with minimum FixPak 101 • IBM DB2 UDB 8.1, with minimum FixPak 51 • Oracle 8i Enterprise Server 8.1.7.4 • Oracle 9i Enterprise Server 9.2.0.4 or above
Web Browser	Microsoft Internet Explorer or above

5.3 Component Recommendations

This subsection provides specific recommendations for the selection and configuration of Siebel 7.7 components within the CMS Internet Architecture. Table 2 presents the entire set of recommendations for selecting and configuring Siebel 7.7 components.

Table 2. Recommendations for Selection and Configuration of Siebel 7.7 Components

Selection and Configuration of Siebel 7.7 Components	
Number	**Recommendation**
Components	
1	Placement of Siebel File System Manager in the Data Zone
2	Distribute AOMs Across Multiple Siebel Servers
3	Provide User-Centric and Server-Centric AOMs
4	Segregate Intranet and Extranet Traffic on Separate Gateway Name Servers
Security	
5	Provide Authentication Through the Siebel Security Adapter
6	Change Default Passwords
7	Store Encrypted Passwords
8	Maintain Audit Trails

Selection and Configuration of Siebel 7.7 Components	
Number	**Recommendation**
Encryption	
9	Use SSL Encryption
10	Use SSL Encryption for Connection to LDAP
11	Use Encryption for SISNAPI Connections Between Components
12	Protect Sensitive Information With AES Database Encryption
13	Use RSA SHA-1 Password Hashing
Cookies	
14	Disable Auto-Login Credential Cookies
Port Usage	
15	Minimize Number of Open Ports Between Components

5.3.1 Recommendation 1 – Placement of Siebel File System Manager in the Data Zone

Place the Siebel File System Manager in the Data Zone of the CMS 3-Zone Internet Architecture.

Rationale

Siebel relies on the File System Manager for permanent storage of documents and emails exchanged with or accessed on behalf of a customer. These documents must be stored on a hard drive. The FSM is a component of the Siebel Server, which is designed to enable a decoupling of the Siebel Application from the disk storage environment. It is a key component in supporting a 3-Zone Internet Architecture. Since the FSM does not serve up any specific application functionality, but rather provides permanent storage services to the application, it should be regarded as a data service. Although installation of FSM requires the installation of a Siebel Server in the Data Zone, all application components can be disabled. This would leave FSM as the only component running within the Siebel Suite and would ensure compliance with its data service role. If the FSM is located in the Data Zone, there is no need for a Network File System (NFS) mount because the FSM will be able to communicate with the file system in the Data Zone.

5.3.2 Recommendation 2 – Distribute AOMs Across Multiple Siebel Servers

All AOMs should be distributed across multiple Siebel Servers.

Rationale

The Siebel Enterprise Server is designed to distribute activity among multiple Siebel Servers. This allows for maximum scalability and failover. It is also the most common way to deploy Siebel.

5.3.3 Recommendation 3 – Provide User-Centric and Server-Centric AOMs

Siebel Applications should have separate AOMs for user interfaces and process interfaces.

Rationale

AOMs can be configured to meet specific needs, and should be configured to avoid any conflict with another usage. The needs of human users are distinctly different from and contradict those of server processes, as illustrated by timeout values. For example, user interfaces require long timeout values to ensure a positive user experience. The typical timeout for a user-centric interface is 15 minutes.

Process interfaces require much shorter timeout values. A timeout value of 15 minutes for a process interface would quickly exhaust the Siebel Server processing threads. All the threads would be busy waiting for server connection timeouts. Accordingly, a typical process-centric timeout value would be 1 minute.

5.3.4 Recommendation 4 – Segregate Intranet and Extranet Traffic on Separate Gateway Name Servers

Intranet and extranet traffic should be segregated into separate Siebel Gateway Name Servers.

Rationale

Segregating intranet traffic from extranet traffic is necessary to separate sensitive internal traffic from public-facing traffic.

5.4 Security Recommendations

Establishing the appropriate security configuration settings to protect financial and medical data is just as important as configuring the system for optimal performance. This subsection provides an overview of the minimum required security settings when implementing Siebel 7.7.[2]

5.4.1 General Security Overview

CMS' system security mission is dedicated to ensuring the use of adequate safeguards to protect the personal, proprietary, and other sensitive data contained in CMS' automated systems.[3] These safeguards are intended to protect the confidentiality, integrity, and availability of the Agency's information.[4] CMS has long recognized the need for increased security to ensure continuity of service for business processes. "Security program management and related implementation of controls over access to data, systems, and software programs are central factors affecting CMS' ability to protect its information resources."[5]

---

2 This subsection assumes the reader has a basic understanding of the Siebel application architecture. The information in this subsection was derived from the *Security Guide for Siebel eBusiness Applications, Version 7.7*, Siebel Systems, Inc., March 2004. Readers should consult that guide for a more in-depth understanding of the Siebel security settings.

3 *CMS Information Systems Security Policy, Standards and Guidelines Handbook (The Handbook)*, Version 1.2, Centers for Medicare & Medicaid Services, July 19, 2004.

4 Ibid.

5 Ibid.

Protecting the Confidentiality, Integrity and Availability (CIA) of information is not always an easy task. The proper mechanisms within the application, operating system, and network must be installed and configured correctly to provide adequate security. This subsection addresses how to configure Siebel to protect the CIA of the information served by the application.

Siebel is an application that runs on top of an operating system. Consequently, it is crucial to protect the CIA of the operating system in order to also protect the Siebel application. Although these *Guidelines* do not address the extensive procedures needed to protect the operating system, CMS has established standards for protecting operating systems:

> Any operating system (UNIX, Windows NT, etc.) must be configured in accordance with National Security Agency [NSA] guidelines on server/operating system vulnerabilities and guidelines provided by the National Institute of Standards and Technology [NIST] Special Publications, including but not limited to the Special Publications 800-7 and 800-43 as applicable.[6]

Whenever Siebel is implemented, the underlying system must be properly protected in accordance with NSA and NIST guidelines.

5.4.2 Recommendation 5 – Provide Authentication Through the Siebel Security Adapter

The Siebel Security Adapter should be used whenever possible.

Rationale

According to the *CMS Target Architecture*, Lightweight Directory Access Protocol (LDAP) is the approved authentication service. Siebel has developed a special security adapter that allows users to conduct verify credentials through LDAP or Active Directory Server (ADS).

5.4.3 Recommendation 6 – Change Default Passwords

Default passwords should be changed for use of Siebel 7.7.

Rationale

The valid character set for usernames and passwords is configured with the authentication service being used. The System Administrator should use the LDAP vendor documentation to set parameters that are within CMS policy.

Not changing default pas*swords represents one of more egregious mistakes administrators make. For example, the Siebel Security Guide for Siebel eBusiness Applications* states:

> The Siebel Database Server installation script and the seed data provided with Siebel eBusiness Applications create several default accounts on your site. These accounts are used to manage and maintain your Siebel network. To safeguard the security of your

[6] *CMS Internet Architecture*, CMS-CIO-STD-INT01, Centers for Medicare & Medicaid Services, July 2003.

site, make sure you change the default passwords for these accounts.[7]

The Siebel accounts that must be changed are:

- SADMIN
- Windows Service Owner Account
- Siebel administrator database account
- Database Table Owner account (SIEBEL)
- All default Oracle accounts
- Any anonymous guest accounts (disable).

The System Administrator should also define a password for updating cached images and other Siebel application-related static files on the Web server.

5.4.4 Recommendation 7 – Store Encrypted Passwords

All encrypted passwords should be stored according to Siebel instructions.

Rationale

The eapps.cfg file contains parameters that help define how passwords are stored. Passwords should never be stored in the clear. To ensure passwords are stored encrypted, set the following parameter within the eapps.cfg file: EncryptedPassword = TRUE.

5.4.5 Recommendation 8 – Maintain Audit Trails

The System Administrator should maintain an audit trail.

Rationale

To maintain data continuity and monitor activity on a Siebel site, Siebel applications can maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed.

At a minimum, the audit trail should include:

- Fields that have been changed
- Who made the change?
- What has been changed?
- When were the changes made?

[7] *Security Guide for Siebel eBusiness Applications,* Version 7.7, March 2004.

Auditing can also be enabled through the database server. The CMS auditing standard is as follows:

- All activity involving access to and modifications of sensitive or critical files is logged[8]
- The audit trail includes sufficient information to establish what events occurred and who or what caused them.[9]

5.4.6 Encryption

Encryption is an essential mechanism for maintaining the confidentiality portion of the CIA triad.

5.4.6.1 Recommendation 9 – Use SSL Encryption

SSL encryption should be used to protect sensitive data over the Internet.

Rationale

For data security over the Internet, the Siebel application uses the SSL capabilities of supported web server platforms to secure transmission for data between the web browser and web server. The data transferred between the web server and client is most likely either sensitive financial or medical data or a combination of both. Accordingly, the entire session should be encrypted.

5.4.6.2 Recommendation 10 – Use SSL Encryption for Connection to LDAP

SSL should be used for connection to certified LDAP.

5.4.6.3 Recommendation 11 – Use Encryption for SISNAPI Connections Between Components

Siebel recommends that for communications between Siebel components, Siebel administrators can enable encryption for SISNAPI (Siebel Internet Session API) to protect communications between Siebel components.[10] SISNAPI is a TCP/IP-based Siebel communications protocol that "provides a security and compression mechanism for network communications."[11] Whenever Siebel components communicate across a zone, SISNAPI should be enabled using SSL.

5.4.6.4 Recommendation 12 – Protect Sensitive Information With AES Database Encryption

Siebel applications allow customers to encrypt sensitive information stored in the Siebel Database. As a result, sensitive information is only viewed through the Siebel application. All sensitive information should be properly protected using Advanced Encryption Standard (AES) encryption when sensitive information is stored in the Siebel Database.

---

8 CMS Core Security Requirement (CSR).

9 Ibid.

10 *Security Guide for Siebel eBusiness Applications,* Version 7.7, March 2004.

11 Ibid.

5.4.6.5 Recommendation 13 – Use RSA SHA-1 Password Hashing

Password hashing should be used for Siebel applications.

Rationale

Siebel administrators can enable password hashing. Hashing uses a one-way hashing algorithm. The default password hashing method is RSA SHA-1 and should be used to store passwords.

5.4.7 Cookies

5.4.7.1 Recommendation 14 – Disable Auto-Login Credential Cookies

The System Administrator should disable the feature for auto-login credential cookies. Only session cookies should be allowed.

Rationale

The session cookie is non-persistent and is stored in memory only. It stays in the browser for the duration of the session, and is deleted when the user logs out or is timed out. The auto-login credential cookie remembers the user ID and password. This feature should NOT be used.

5.4.8 Port Usage

5.4.8.1 Recommendation 15 – Minimize Number of Open Ports Between Components

The number of open ports should be minimized at all times.

Rationale

It is very important to determine which ports should be open between each of the components that comprise the entire Siebel application. Ranges of ports should not be open between systems, especially across the zones. Network traffic to Application Object Managers on Siebel Servers goes through static, configurable TCP ports. Each Siebel Server listens on one TCP port only. Only the minimum ports should be open between components.

Acronyms

ADS	Active Directory Server
AES	Advanced Encryption Standard
AOM	Application Object Model
API	Application Programming Interface
CGI	Common Gateway Interface
CIA	Confidentiality, Integrity, and Availability
CMS	Centers for Medicare & Medicaid Services
COTS	Commercial Off-the-Shelf
CSR	Core Security Requirement
EAI	Enterprise Application Integration
EIM	Enterprise Integration Management
EJB	Enterprise Java Beans
ETL	Extract, Transform and Load
FSM	File System Manager
HTTP	HyperText Transport Protocol
IA	Internet Architecture
IP	Internet Protocol
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
JBDC	Java Database Connectivity
JDB	Java Data Bean
JMS	Java Message Service
JNI	Java Native Interface
JRE	Java Runtime Environment
JSP	Java Server Page
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
NIST	National Institute of Standards and Technology
NSA	National Security Agency

ODBC	Open Database Connectivity
RDBMS	Relational Database Management System
SCBroker	Siebel Connection Broker
SISNAPI	Siebel Internet Session Application Programming Interface
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SWSE	Siebel Web Server Extension
TCP	Transmission Control Protocol
UAN	Universal Applications Network
UDB	Universal Database (IBM product)
UI	User Interface
VBC	Virtual Business Component
WAP	Wireless Application Protocol
WSDL	Web Service Description Language
XML	eXtensible Markup Language

List of References

1. *CMS Internet Architecture*, CMS-CIO-STD-INT01, Centers for Medicare & Medicaid Services, July 2003.
2. *CMS Enterprise Messaging Infrastructure*, CMS-CIO-STD-INT02, Centers for Medicare & Medicaid Services, December 2003.
3. *CMS Web-Enabled Application Architecture*, CMS-CIO-STD-INT03, Centers for Medicare & Medicaid Services, March 2004.
4. *CMS Target Architecture*, CMS-CIO-STD-ARC01, Centers for Medicare & Medicaid Services, September 2004.
5. *CMS Information Systems Security Policy, Standards and Guidelines Handbook (The Handbook)*, Version 1.2, Centers for Medicare & Medicaid Services, July 19, 2004.
6. *Security Guide for Siebel eBusiness Applications*, Version 7.7, Siebel Systems, Inc., March 2004.
7. *Deployment Planning Guide*, Version 7.7, Revision A, Siebel Systems, Inc., May 2004.
8. *Siebel System Administration Guide*, Version 7.7, Revision A, Siebel Systems, Inc., August 2004.
9. *Siebel Installation Guide for UNIX: Servers, Mobile Web Clients, Tools*, Siebel Systems, Inc., Version 7.7, Revision B, September 2004.