



Siebel eBusiness Applications Application Security & Controls

ISACA Puget Sound Chapter – Seattle – November 19, 2002



Contact Information:

Peter Rosenzweig
Deloitte & Touche LLP
Enterprise Risk Services
Los Angeles, California
Phone: (213) 996-4838
Email: prosenzweig@deloitte.com



Table of Contents

Chapter 1	-	Siebel System Architecture
Chapter 2	-	Siebel Visibility
Chapter 3	-	Siebel User Authentication & Registration
Chapter 4	-	Siebel Configurable Controls



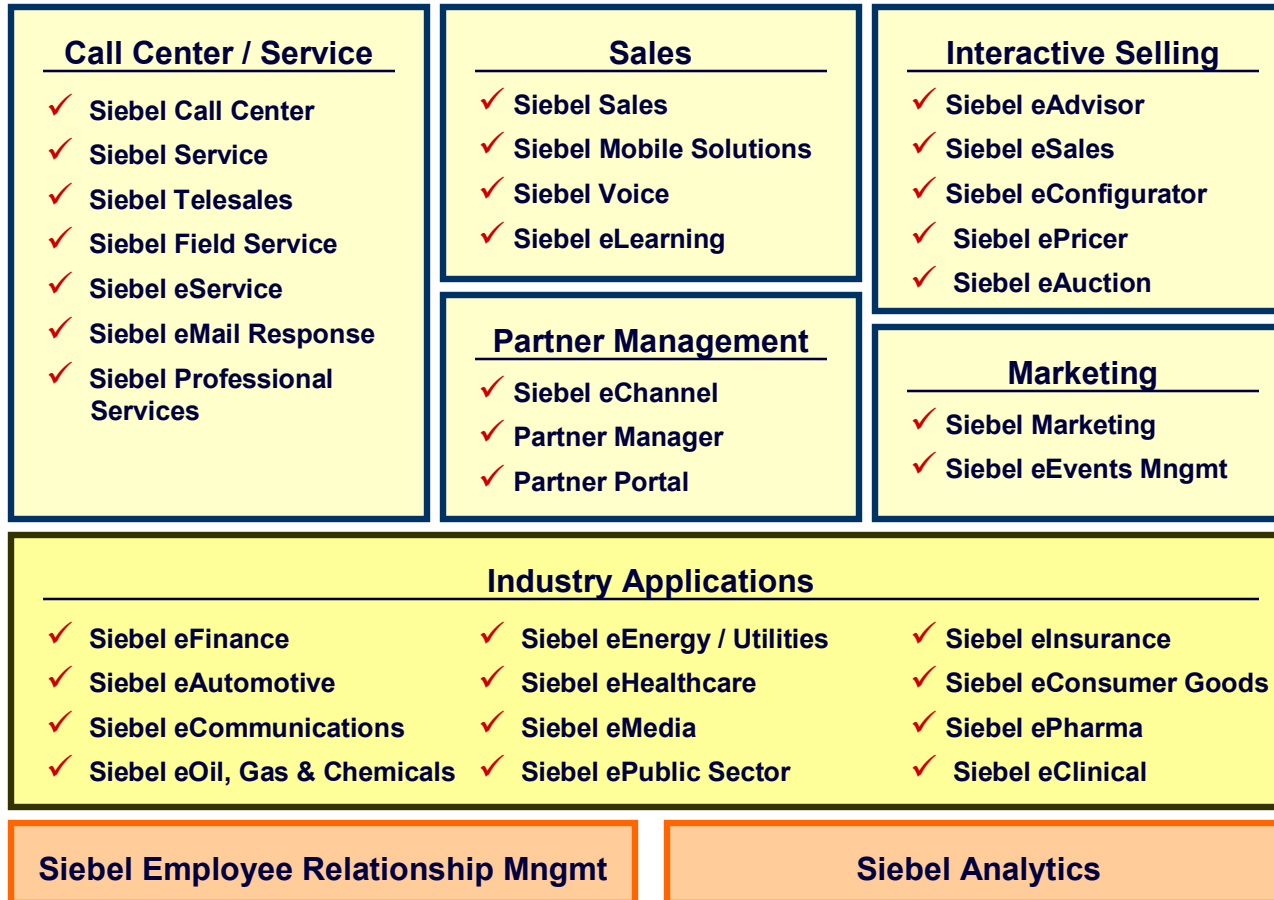
Chapter 1

Siebel System Architecture



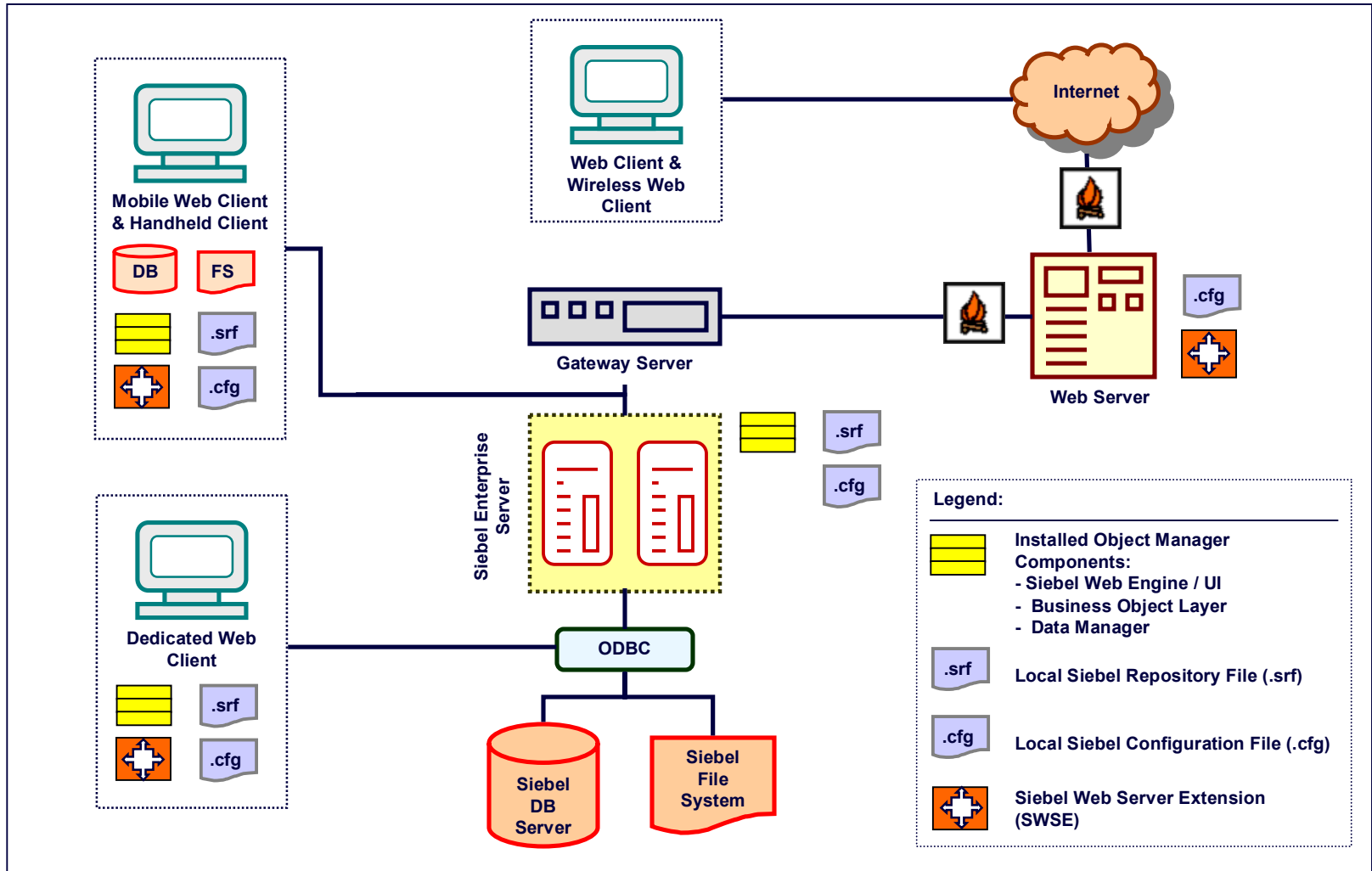
Siebel System Architecture – Application Overview

Siebel eBusiness consists of a suite of integrated applications, which are geared to support multiple customer communication channels:*



* Check www.siebel.com for updated information on available applications and industry solutions

Siebel System Architecture – Client-Server Options





Siebel System Architecture – Object-Based Data Model

Siebel's object-based system architecture is designed to provide flexibility concerning the collection and processing of information. Three different data layers allow an organization to structure information to meet specific business and reporting requirements.

User Interface Layer

(graphical representation of data)



Business Object Layer

(business-specific representation of data (i.e., business logic))



Data Object Layer

(logical – vendor-independent representation of data)





Siebel System Architecture – User Interface Layer – Screens

Within Siebel, **Screens** represent groupings of associated tasks that are needed as part of certain job functions.

The *Opportunities Screen*, for instance, is an accumulation of functions, which are needed as part of the opportunity administration/processing.

Screen – Tab Bar

The screenshot displays the Siebel user interface for the Opportunities screen. At the top, there is a menu bar with options like File, Edit, View, and Help. Below that is a navigation bar with tabs for Home, Accounts, Contacts, Households, Employees, Service, Assets, Orders, Campaigns, Opportunities, Quotes, and Communications. The Opportunities tab is selected and circled in red. Below the navigation bar is a search and history section. The main content area is divided into two parts: a list of opportunities and a detailed view of a selected opportunity. The list of opportunities has columns for Name, Account, Primary, Revenue, Sales Stage, and Close Date. The detailed view shows fields for Name, Sales Method, Committed, Close Date, Sales Team, Sales Stage, Revenue, Organization, Territories, Account, Probability %, Lead Quality, Description, Site, Expected Value, and Source. A red box highlights the 'Screen (Opportunities)' label in the detailed view, and another red box highlights the 'Opportunities' tab in the navigation bar.

New	Priority Flag	Name	Account	Primary	Revenue	Sales Stage	Close Date
		1000 Users of Siebel	Puma Sports, Inc.	TSMYTHE	\$500,000.00	02 - Potential Lead	9/21/2002
		Call Center	Rossi e Associati	IT_MSTE	€870,000.00	07 - Selected	7/31/2002
		Call Center	Ital No	IT_MSTE	€993,000.00	02 - Potential Lead	7/31/2002
		Call Center - 150 Se	Harley-Davidson Fir	TSMYTHE	\$600,000.00	03 - Qualification	8/20/2002
		Call center	Tele Italia	IT_MSTE	\$580,000.00	08 - Negotiation	7/31/2002
		Centro supporto Clie	Giannelli Editori	FITTIO	€350,000.00	02 - Potential Lead	7/31/2002
		Contact Center	Marriott Internationa	IT_MSTE	€960,000.00	04 - Opportunity	7/31/2002

Screen (Opportunities)

***Name:** 1000 Users of Siebel
Sales Method: [Dropdown]
Committed:
***Close Date:** 9/21/2002
Sales Team: TSMYTHE
Sales Stage: 02 - Potential Lead
Revenue: \$500,000.00
Organization: Siebel Americas
Territories: [Dropdown]
Account: Puma Sports, Inc.
Probability %: 10%
Lead Quality: 2-Very High
Description: SALES ANALYSIS DEMO
Site: Call Center
Expected Value: \$50,000.00
Source: [Dropdown]



Siebel System Architecture – User Interface Layer – Views

Siebel uses **Views** to determine the level of functionality that is accessible to users within a given screen.

Views can also be used to better segregate the access to data by distinguishing the range of data, which is accessible (e.g., *My Opportunities* vs. *All Opportunities*).

The screenshot shows the Siebel CRM interface. At the top, there is a menu bar with 'File', 'Edit', 'View', and 'Help'. Below it is a navigation bar with tabs for 'Home', 'Accounts', 'Contacts', 'Households', 'Emails', 'Campaigns', 'Opportunities', 'Quotes', and 'Communications'. A 'Show' dropdown menu is highlighted with a red box and labeled 'Show Drop-Down'. Below the navigation bar is a table of Opportunities. The table has columns for 'New', 'Priority Flag', 'Name', 'Account', 'Primary', 'Revenue', 'Sales Stage', and 'Close Date'. The table contains several rows of data. Below the table is a 'View - Tab Bar' with tabs for 'More Info', 'Activities', 'Assessments', 'Attachments', 'Campaign Leads', 'Contacts', 'Notes', 'Organization Analysis', 'Profile', 'Quotes', and 'R'. The 'More Info' tab is highlighted with a red box and labeled 'View - Tab Bar'. Below the tab bar is a form for editing an Opportunity. The form has several fields: 'Name' (1000 Users of Siebel ePricer Puma), 'Sales Method' (Standard Sales Process), 'Committed' (checkbox), 'Close Date' (9/21/2002), 'Sales Team' (TSMYTHE), 'Sales Stage' (02 - Potential Lead), 'Revenue' (\$500,000.00), 'Organization' (Siebel Americas), 'Territories', 'Account' (Puma Sports, Inc.), 'Probability %' (10%), 'Lead Quality' (2-Very High), 'Description' (SALES ANALYSIS DEMO), 'Expected Value' (\$50,000.00), and 'Source'. A red box highlights the 'View (All Opportunities)' tab in the tab bar.

New	Priority Flag	Name	Account	Primary	Revenue	Sales Stage	Close Date
		1000 Users of Siebel ePricer Puma	Puma Sports, Inc.	TSMYTHE	\$500,000.00	02 - Potential Lead	9/21/2002
		Call Center	Rossi e Associati	IT_MSTE	€370,000.00	07 - Selected	7/31/2002
		Call Center	Ital No	IT_MSTE	€993,000.00	02 - Potential Lead	7/31/2002
		Centro supporto Clienti	Giannelli Editori	FITIO	\$600,000.00	03 - Qualification	8/20/2002
		Contact Center	Marriott International	IT_MSTE	\$580,000.00	08 - Negotiation	7/31/2002
					€350,000.00	02 - Potential Lead	7/31/2002
					€960,000.00	04 - Opportunity	7/31/2002



Siebel System Architecture – User Interface Layer – Applets

Applets drive the graphical display of Siebel data.

List Applets are commonly used to provide a list-like appearance of multiple data records

Form Applets take selected records and conveniently display the relevant data fields next to each other. This format supports data entry and maintenance.

The screenshot displays the Siebel user interface. At the top, there is a menu bar with 'File', 'Edit', 'View', and 'Help'. Below it is a navigation bar with tabs for 'Home', 'Accounts', 'Contacts', 'Households', 'Employees', 'Service', 'Assets', 'Orders', 'Campaigns', 'Opportunities', 'Quotes', and 'Communications'. A 'Show:' dropdown and 'History:' buttons are also present. The main content area is titled 'Opportunities' and shows a list of records. A red box highlights the 'List Applet (Lists)' section, which contains a table with columns: 'New', 'Priority Flag', 'Name', 'Sales Method', 'Revenue', 'Sales Stage', and 'Close Date'. The table lists several opportunities, including '1000 Users of Siebel ePricer Puma Sports, Inc.' with a revenue of \$500,000.00. Below the table, a red box highlights the 'Form Applet (Forms)' section, which displays the details for the selected record. The form includes fields for 'Name', 'Sales Method', 'Sales Stage', 'Account', 'Site', 'Committed', 'Probability %', 'Expected Value', 'Close Date', 'Organization', and 'Lead Quality'. The 'Name' field contains '1000 Users of Siebel ePricer Puma', 'Sales Method' is 'Standard Sales Process', 'Sales Stage' is '02 - Potential Lead', 'Account' is 'Puma Sports, Inc.', 'Site' is 'Call Center', 'Committed' is '\$500,000.00', 'Probability %' is '10%', 'Expected Value' is '\$50,000.00', 'Close Date' is '9/21/2002', 'Organization' is 'Siebel Americas', and 'Lead Quality' is '2-Very High'.

New	Priority Flag	Name	Sales Method	Revenue	Sales Stage	Close Date
		1000 Users of Siebel ePricer Puma Sports, Inc.	TSMYTHE	\$500,000.00	02 - Potential Lead	9/21/2002
		Call Center Rossi e Associati	IT_MSTE	€870,000.00	07 - Selected	7/31/2002
		Call Center Ital No	IT_MSTE	€993,000.00	02 - Potential Lead	7/31/2002
		Call Center - 150 Se Harley-Davidson Fir	TSMYTHE	\$600,000.00	03 - Qualification	8/20/2002
		Call center Tele Italia	IT_MSTE	\$580,000.00	08 - Negotiation	7/31/2002
		Centro supporto Clienti	FITTIO	€350,000.00	02 - Potential Lead	7/31/2002
		Contact Center Marriott International	IT_MSTE	€960,000.00	04 - Opportunity	7/31/2002

Form Applet (Forms)

***Name:** 1000 Users of Siebel ePricer Puma
Sales Team: TSMYTHE
Territories:
Description: SALES ANALYSIS DEMO
Sales Method: Standard Sales Process
Sales Stage: 02 - Potential Lead
Account: Puma Sports, Inc.
Site: Call Center
Committed: \$500,000.00
Probability %: 10%
Expected Value: \$50,000.00
***Close Date:** 9/21/2002
Organization: Siebel Americas
Lead Quality: 2-Very High
Source:



Chapter 2

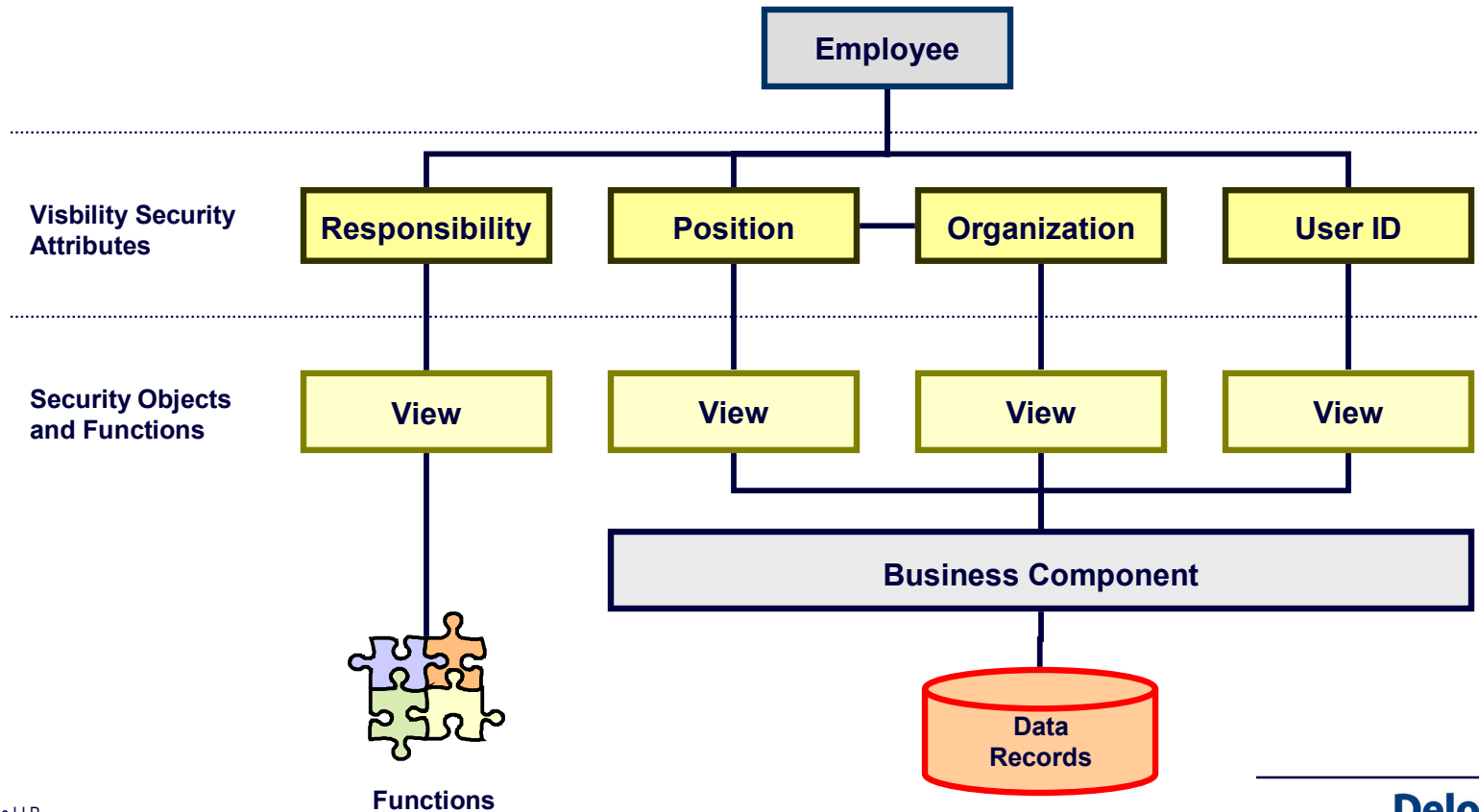
Siebel Visibility



Siebel Visibility – Overview

The Siebel Visibility concept is comparable to what is commonly referred to as Application Security. It is a first layer of access restrictions, which defines the organizational slice of data as well as functions made available to system users.

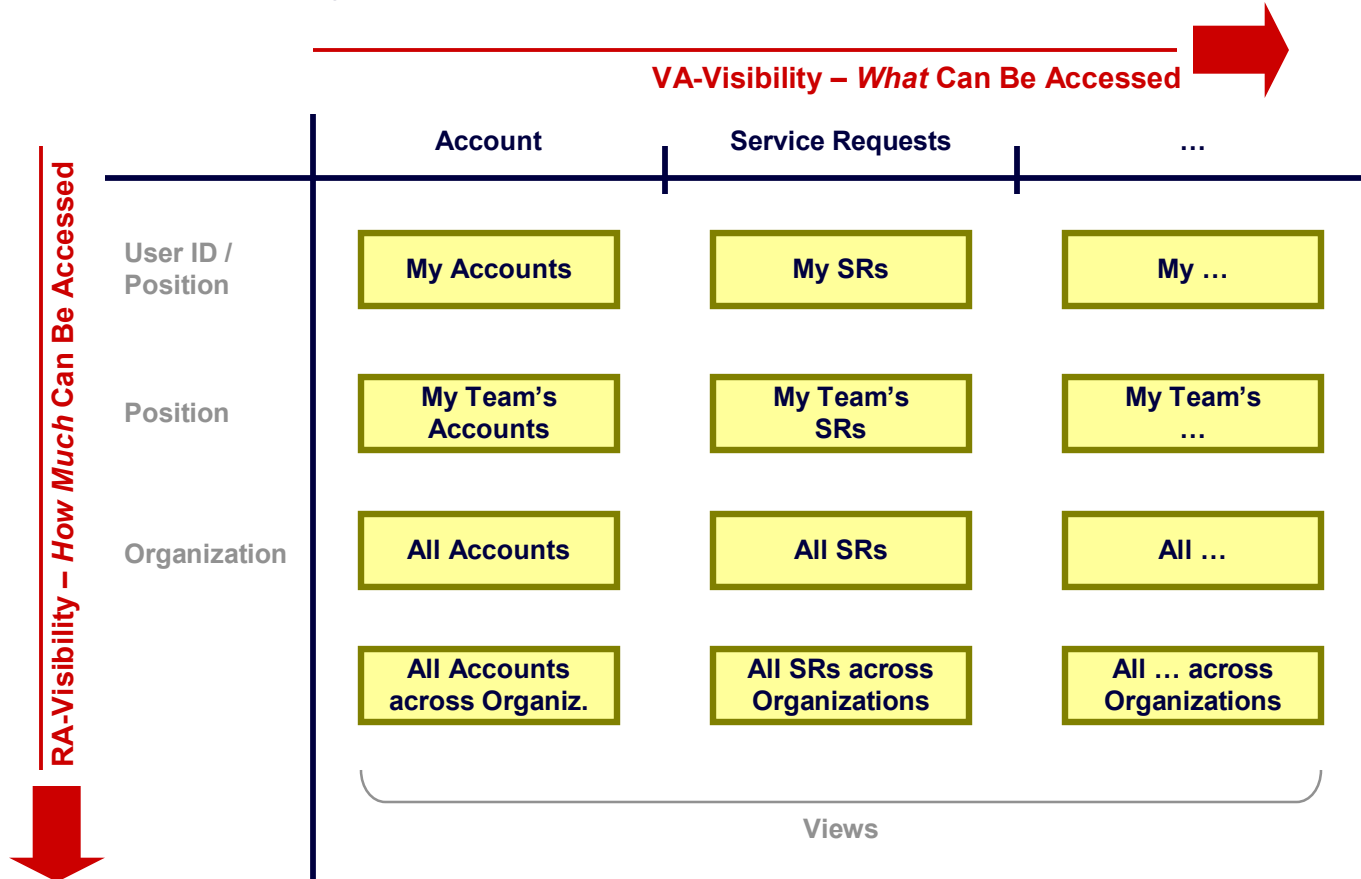
Visibility is defined by assigning Positions and Responsibilities to Employee records.





Siebel Visibility – View-Access vs. Record-Access Visibility

Siebel Visibility can be broken down into two components. View-Access Visibility drives access rights to Siebel Views. Record-Access Visibility uses Views in combination with User IDs, Positions, and Organizations and determines the number of records that are accessible.





Siebel Visibility – View Access Visibility – Responsibilities

Responsibilities define access rights to particular views and should be organized based on particular job responsibilities / tasks (e.g., Account Administration).

If a View is not assigned to a user record, the following restrictions apply:

- A) The View is not listed on show drop-down and Sitemap menus
- B) The system removes the View from the tab bar
- C) Hyperlinks loose their functionality if they refer to a View, for which access has not been granted

Users can have multiple Responsibilities assigned, which form cumulative access rights.

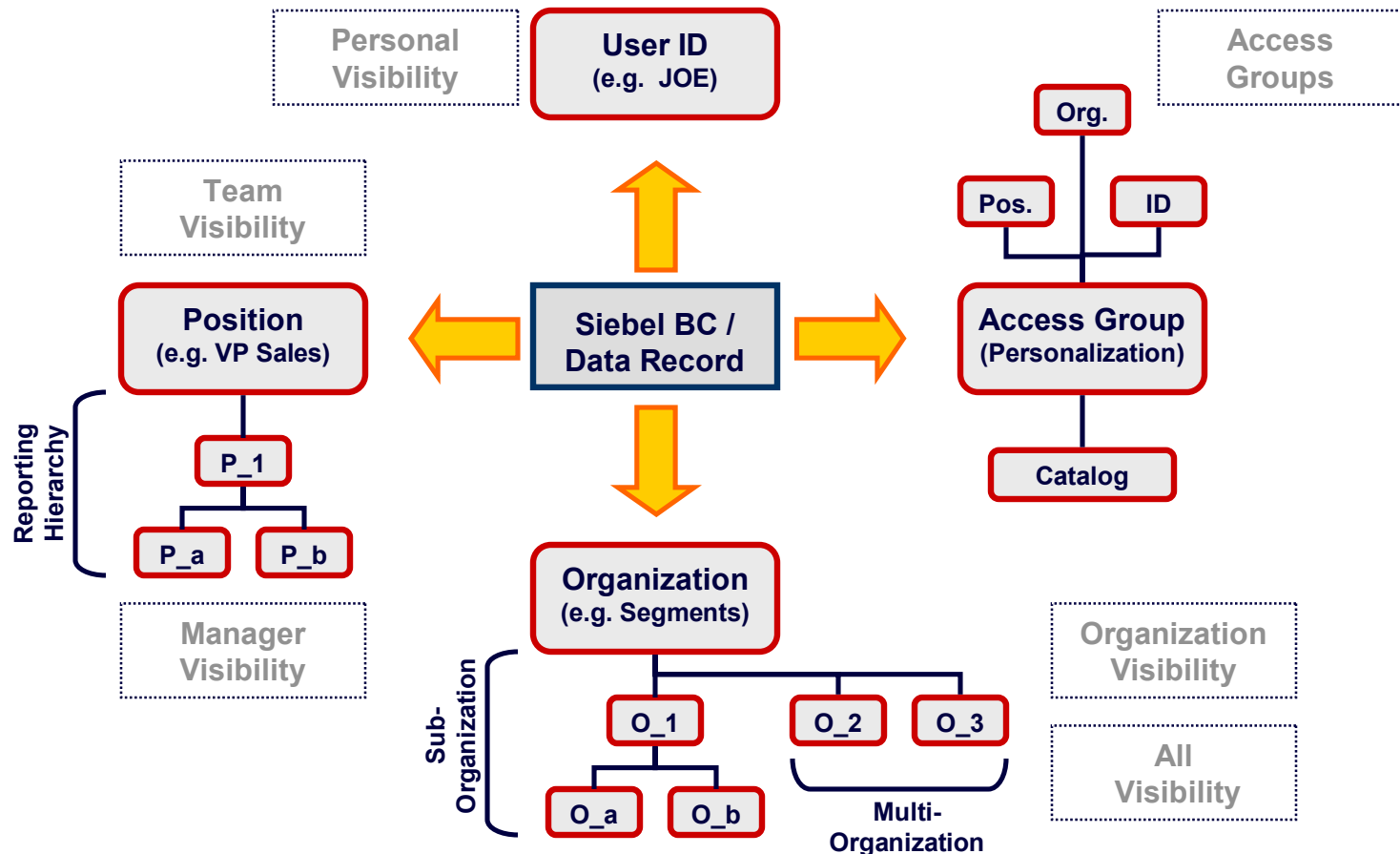
The screenshot shows the Siebel CRM interface with the 'Contacts' view active. The 'Show:' dropdown menu is set to 'My Contacts'. The 'More Info' tab is selected in the bottom navigation bar. The 'Account' column in the contacts table is highlighted with a red circle, and the 'AEP Communication' entry is circled in red. Red arrows point from the labels A, B, and C to these specific elements.

New	Last Name	First Name	Account	Middle
	Aamot	Gina	AEP Communication	
*	Abanilla	David	AEP Communication	
*	Abate	Laura	AEP Communication	
*	Abbolino	Glen	eBusiness Beratung	
*	Abdallah	Trey	AEP Communication	
*	Abel	Robert	AEP Communication P.	
*	Abelman	Brent	Alberta Treasury Br	



Siebel Visibility – Record-Access Visibility – Business Component View Mode

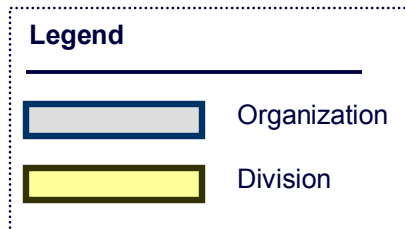
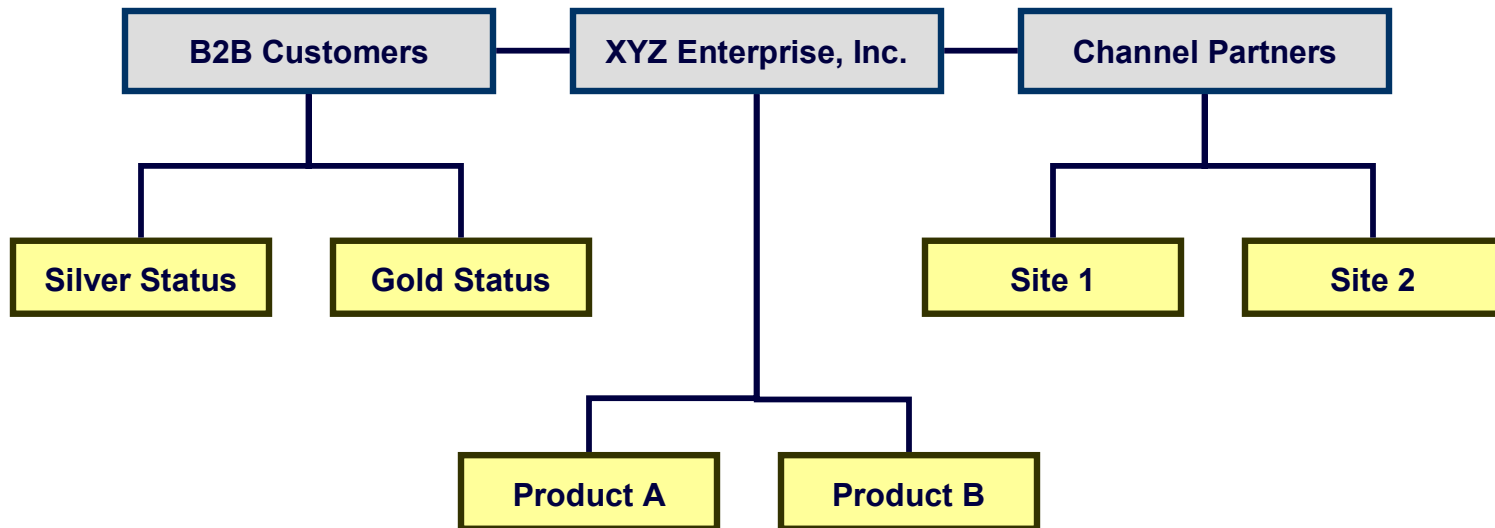
The type of Record-Access Visibility being available for data records can vary and is dependent on certain system settings. The following scenarios are possible:





Siebel Visibility – Record-Access Visibility – Organizations / Divisions

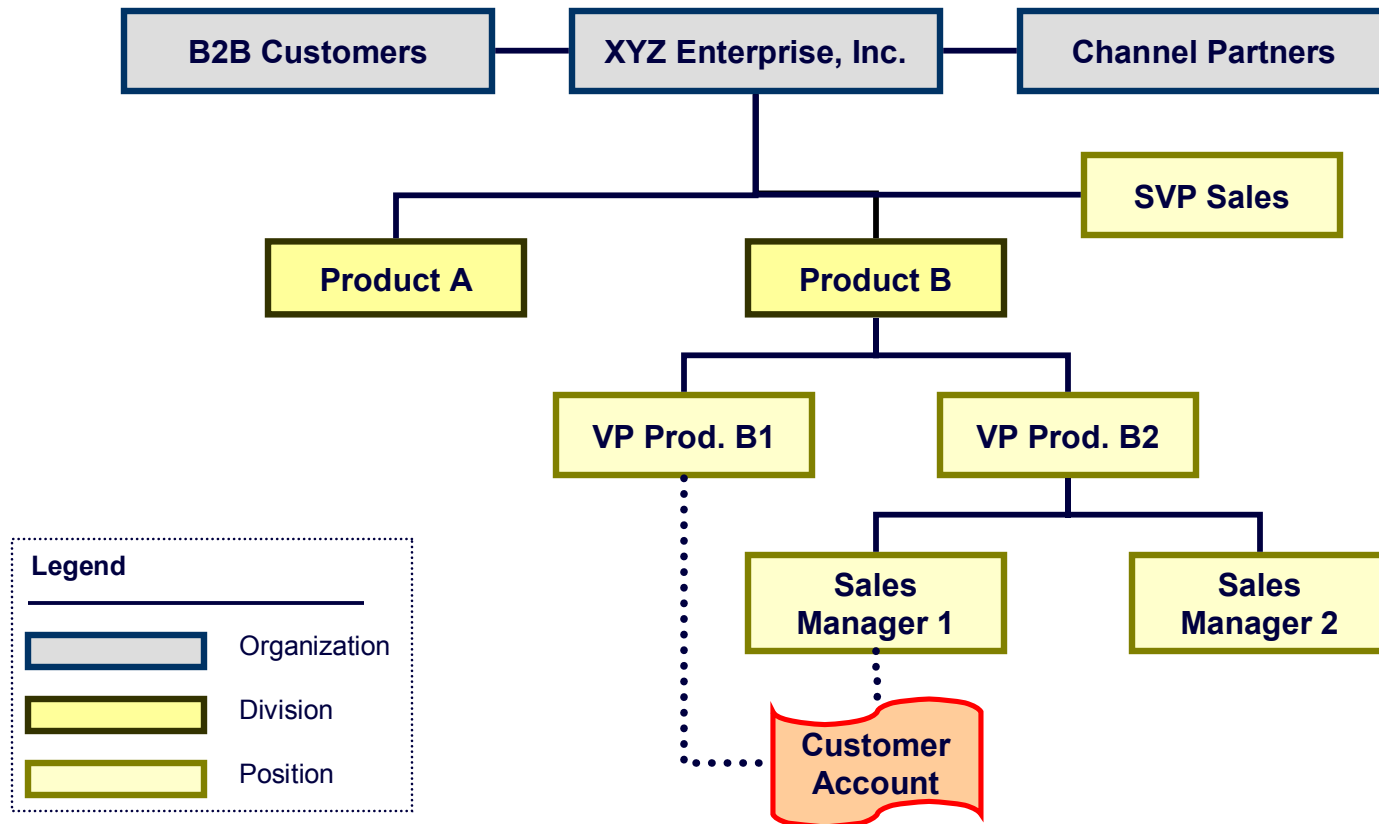
Within Siebel, *Organizations* are used to provide the highest level of data segregation based on specific business requirements (e.g., different price lists for certain business units). Siebel supports single or multi-organizational models. Divisions are subsets of Organizations, however, Divisions cannot be used as an attribute for data segregation (see positions).





Siebel Visibility – Record-Access Visibility – Positions

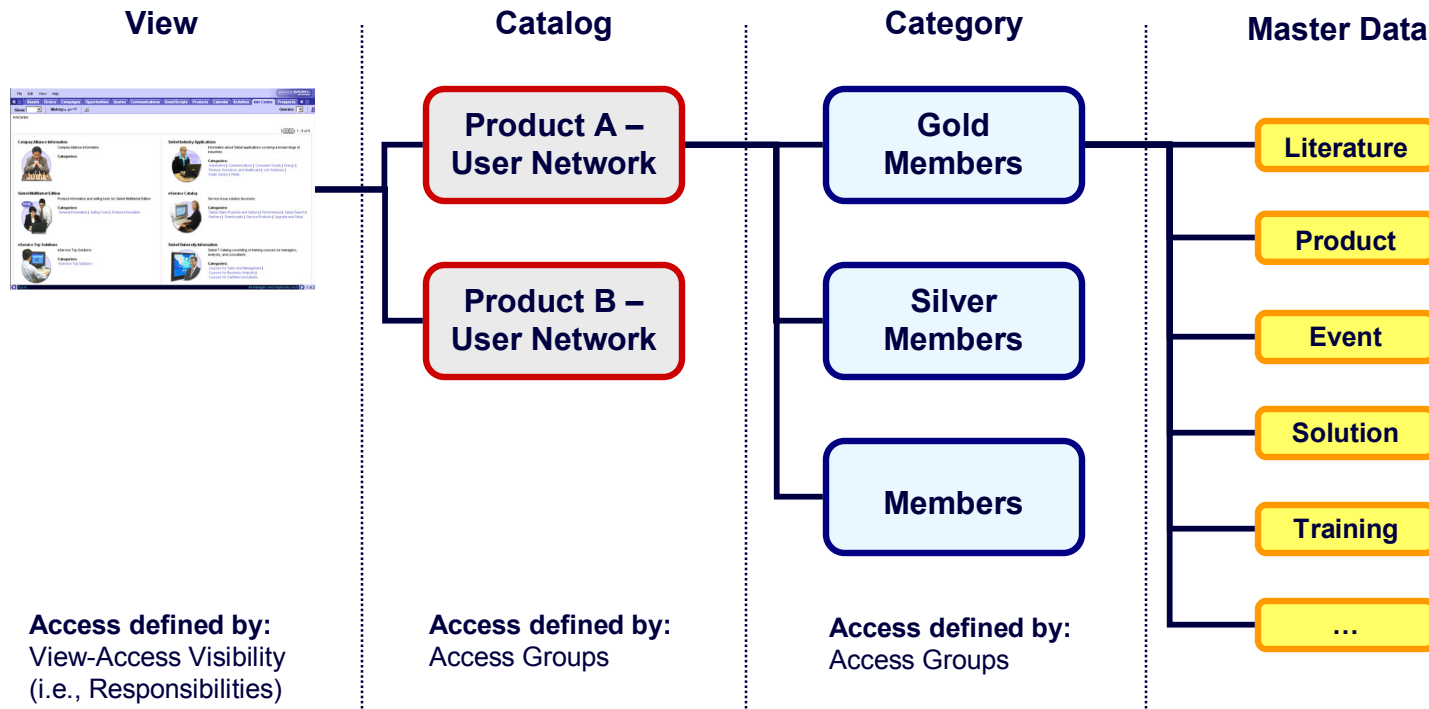
If certain data within Siebel is configured to support *Team Visibility*, Positions can be used to further segregate access privileges. The graph below illustrates a model, which uses markets (i.e., Product A vs. Product B) as a means to split the data pool into distinct categories:





Siebel Visibility – Access Groups, Catalogs, Categories

Access Groups, Catalogs, and Categories are new features in Siebel 7.0, and are designed to provide an additional access control mechanism for master data (i.e., literature, products, event information, product solutions, and training information).





Chapter 3

Siebel User Authentication & Registration



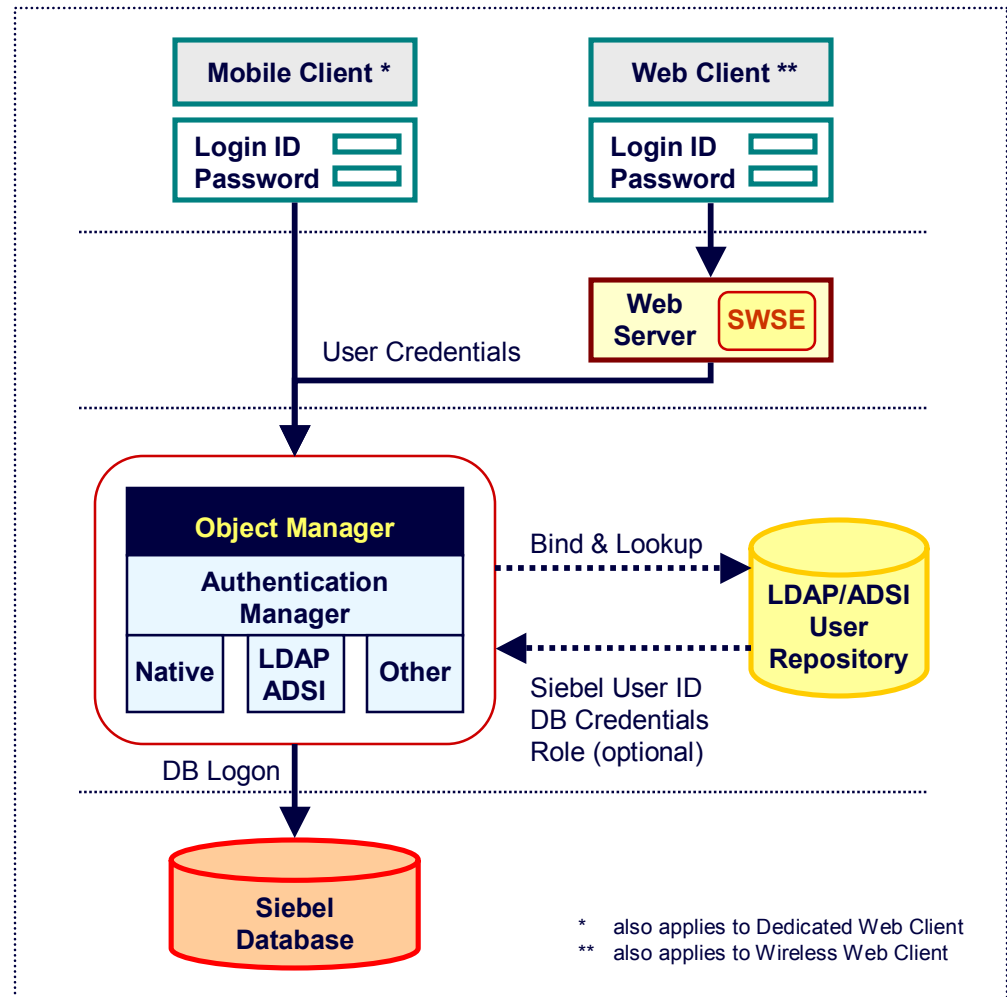
Siebel User Authentication & Registration – Overview

Siebel provides an open security architecture to support the integration of standardized protocols (e.g., LDAP), as well as customized solutions.

As part of the Siebel's Object Manager, the **Authentication Manager** support the following three authentication strategies:

- ✓ Database Authentication
- ✓ External Authentication
- ✓ Single-Sign On (SSO)

Database authentication relates to Siebel's standard authentication model. External authentication and SSO – on the other hand – require additional configuration work, as well as additional investments in soft- and hardware infrastructures.





Siebel User Authentication & Registration – Comparisons

The pros and cons for each authentication method can be summarized as follows:

External and/or SSO Authentication

Pros

- ✓ Is optimized for user administration functions and supports complex password configuration rules.
- ✓ Supports user account creation through Siebel, eliminating the need for direct access to the LDAP repository or database (i.e., clear segregation of database and user administration).
- ✓ Can be used to enable self-service (i.e., account registration and password administration through users) functions.
- ✓ Provides quick ROI due to centralization of administration and support responsibilities.

Cons

- ✓ Requires additional configuration efforts to integrate directory and authentication service with Siebel.
- ✓ Will require additional investments in hardware and software.
- ✓ Might require adjustments of existing policies and procedures concerning user administration.

Database Authentication

Pros

- ✓ Is standard Siebel (out-of-the-box) authentication mechanism.
- ✓ No integration of additional third-party components necessary (i.e., authentication & directory service).

Cons

- ✓ Often, cannot be used to enforce corporate IT security policies regarding password configuration and management (incl. tracking of failed login attempts).
- ✓ User administrators require access to the same database, which contains sensitive product and marketing information.
- ✓ Will require the use of Siebel's password encryption tool, further complicating the account administration.
- ✓ Will not support long-term strategies for Single Sign-On and Self-Service functions.
- ✓ Requires two-step process (account administration in Siebel and underlying database) to create user accounts.



Siebel User Authentication & Registration – Registration Options

Siebel's applications provide multiple options to support the registration of user accounts. These options, however, are also dependent on the underlying system architecture and deployed application components. The following three functionalities are available:

Self-Registration

Users can create their own user accounts. This approach only applies to customer and partner applications and is not supported if database authentication is used. It also allows users to maintain their passwords and request new credentials using 'challenging questions'. It also uses workflow processes to support registration and administration procedures.

Internal Registration

A user administrator within an organization is responsible for setting up new accounts. This approach can be used with database and/or external authentication.

Delegated Administration

An external party (i.e., user administrator belonging to a channel partner) has the privileges to create new user accounts. This approach requires the use of Siebel's security adapter and an external user repository (i.e., LDAP and/or ADSI).

In customer applications, delegated administrators can only administrate users that are associated with the same (customer) accounts that the administrator is associated. In partner applications, access is restricted within the associated partner organization.

Note that registration options can be combined as long as the underlying infrastructure supports it.



Chapter 4

Siebel Configurable Controls



Siebel Configurable Controls - Overview

While Siebel Visibility provides a first layer of protection to adequately secure access to data, configurable controls can establish either further access restrictions or enforce work rules and policies.

The following Siebel features are commonly used to automate preventative internal control procedures.

Field, Applet, and BC Property Settings *

These property settings provide functionalities to validate and restrict processing of data on the record and field level (CRUD)

Pick Lists and Multi-Value Groups *

MVG and pick lists can serve as controls by providing users with a static or dynamic selection of data

Siebel Workflow

This feature can be used to automate and enforce policies and procedures

Assignment Manager

This Siebel component assigns data objects to organizations, positions, and individuals based on skill set, association, and availability

Siebel State Machine

The State Machine is designed to enforce the sequence of state transitions within a specific business object

Audit Trails

Audit Trails allow monitoring of changes to certain data entities and specific field information

* these features require access to Siebel configuration tools



Siebel Configurable Controls – Field, Applet & BC Properties - CRUD

Siebel Visibility is designed to restrict access privileges to defined system functionalities and data records.

To account for more refined access controls, CRUD (create, read, update, delete) definitions allow developers to design action-based (e.g., read-only, no delete, etc.) access models, which can be applied to records and/or specific fields.

The screenshot shows the Siebel Service Requests interface. At the top, there is a navigation bar with tabs for Home, Accounts, Contacts, Households, Employees, Service, Assets, Orders, Campaigns, Opportunities, Quotes, Communications, and SmartS. Below this is a search bar with 'Show: My Service Requests' and a 'History' button. The main content area displays a table of Service Requests with columns for New, SR #, Status, Summary, Account, Site, Last Name, Work Phone #, and Owner. The table contains four rows of data. Below the table, there is a detailed view of a service request for SR # 2-1CR. The detailed view includes fields for Last Name (Pennington), First Name (Joan), Area (Upgrade), Subarea (Disk Drive), Priority (Medium), Severity (3-Medium), Owner (SADMIN), and various dates and times. Red circles and boxes highlight the 'Last Name' field in the table and the 'Last Name' field in the detailed view. Annotations indicate that the value in the table is determined by Siebel and the value in the detailed view is based on the Last Name.

New	SR #	Status	Summary	Account	Site	Last Name	Work Phone #	Owner
	2-1CR	Open	Intermittent error me	3Com	Headquarters	Pennington	(650) 534-9863	SADMIN
	1-1116501	Pending	Replace drive syste	Avaya Communicati	HQ	Abboline	(650) 295-5000	SADMIN
	1-3559557	Open	Drive Replacement	Caterpillar	Chicago	Akber	(847) 555-7601	SADMIN
	1-3				Chicago	Hanson	(510) 555-2300	SADMIN

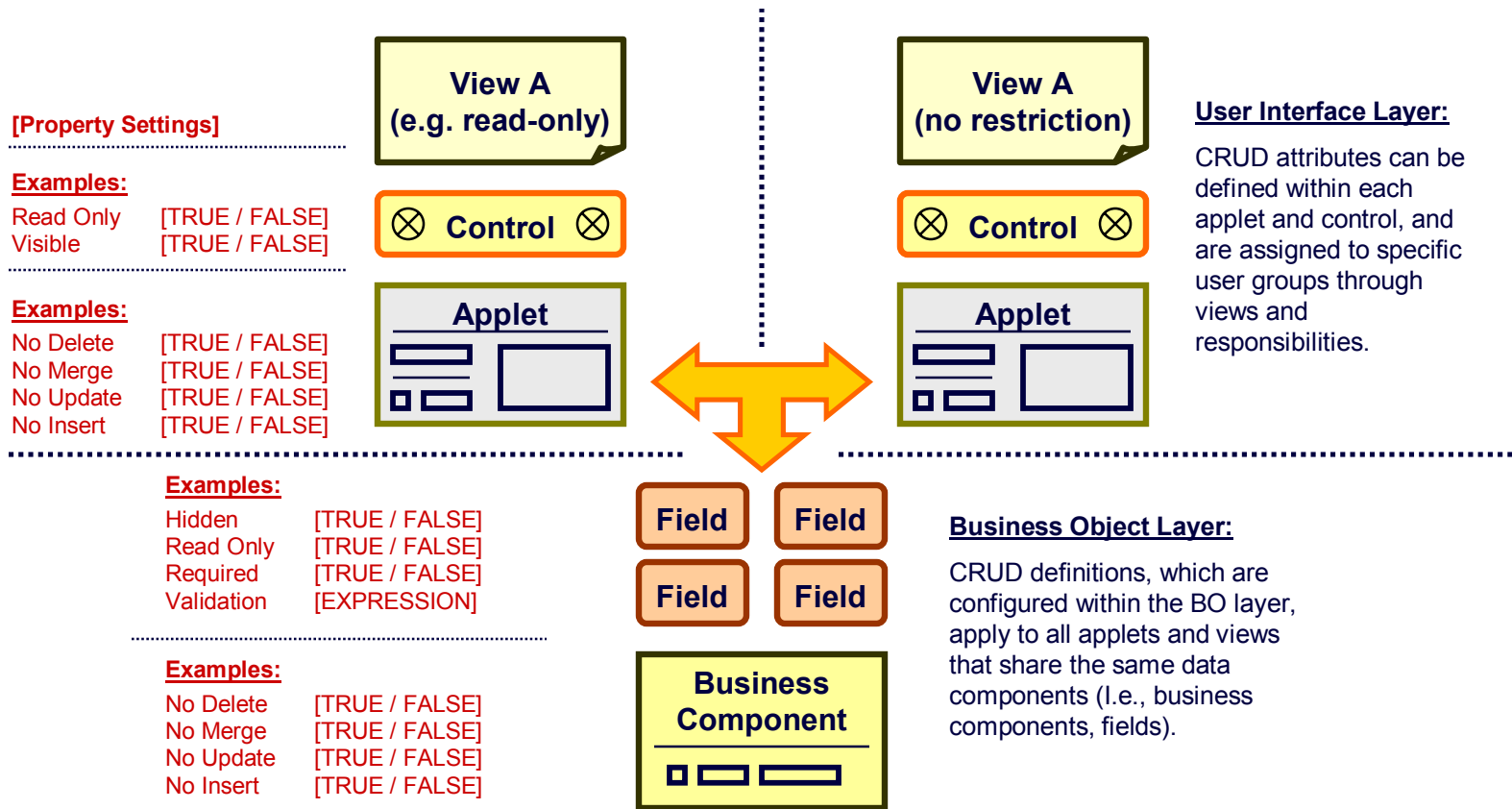
Read-Only – Value determined by Siebel

Read-Only – Value based on Last Name



Siebel Configurable Controls – CRUD Enablers / Components

CRUD definitions are configured by changing property settings within business components, fields, applets, and controls. Such changes require Siebel configuration knowledge and can require extensive validation and testing. The following graph outlines the different components that are available for CRUD configurations:





Siebel Configurable Controls – Pick Lists and Multi-Value Groups (MVG)

Pick lists and MVGs can be powerful tools to protect the integrity of information by forcing the user to work with a pre-selected or pre-configured set of information. Pick lists assume that a field can only be populated with one value, while MVG allow multiple values to be associated.

The screenshot displays a Siebel CRM form for 'Marriott International France'. A red box labeled 'Multi-Value Group (Applet)' points to a window titled 'Account Addresses - Microsoft In...'. This window contains a table with columns 'Primary', 'Address Line 1', and 'City'. A single row is visible with a checkmark in the 'Primary' column, '70 Avenue des Champs Elysée' in 'Address Line 1', and 'Paris' in 'City'. Another red box labeled 'Pick List (LOV or Applet)' points to a dropdown menu for the 'Country' field, which is currently set to 'France'. The dropdown list shows 'France', 'Germany', 'Hong Kong', 'Hungary', and 'Iceland'. The main form fields include 'Name' (Marriott International France), 'Address Line 1' (70 Avenue des Champs Elysée), 'Address Line 2' (empty), 'Zip' (75008), 'City' (Paris), and 'State' (dropdown).



Siebel Configurable Controls – Workflow

Siebel Workflow is an effective tool, which allows developers and system administrators to automate an organization's policies and procedures by embedding business rules into the processing of data.

The following examples document possible solutions that can be addressed through Workflow:

- ✓ **Automated processing of data based on pre-configured rules**
- ✓ **Automated routing and assignment of work**
- ✓ **Automated enforcement of authorization rules**
- ✓ **Automated escalation and notification**

Workflow utilizes three main modules to define the multiple criteria that drive a business process:

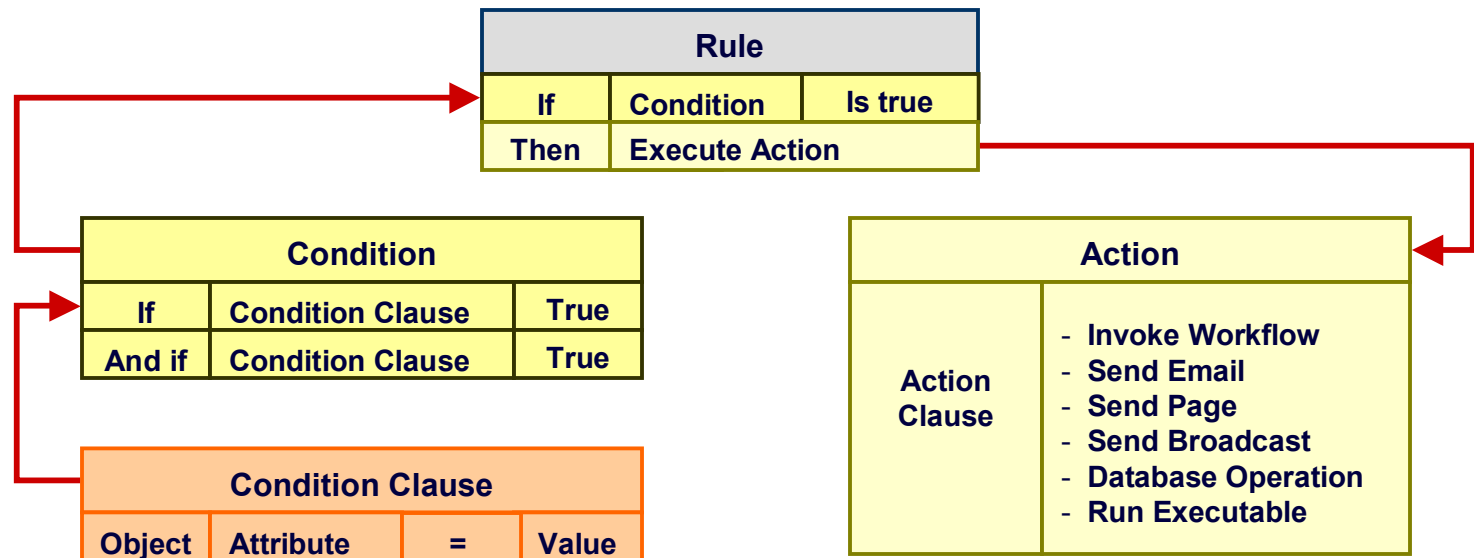
Policy Manager	Used to define policies and rules, which trigger certain processes
.....	
Workflow Processes	Used for the definition of automated processes, sub-processes, decision points, and tasks
.....	
Siebel State Machine	Used to define permissible states and state transitions for business objects



Siebel Configurable Controls – Workflow – Policy Manager

The Policy Manager is used to design the rules and conditions, which trigger certain workflow processes.

The functionality of the Policy Manager depends on the configuration and interaction of rules, conditions, and related actions, which take effect once the system identifies compliances with these conditions.





Siebel Configurable Controls – Audit Trails – Administration

This new feature allows system and security administrators to monitor changes to various data entities (i.e., Business Components). Siebel conveniently separates the audit trail configuration (i.e., administration) from the actual review screen. The graph below provides a screenshot of the audit trail administration view:

The screenshot shows the 'Audit Trail Buscomp' administration interface. It features a table of Business Components and a list of fields to be monitored. Red boxes and arrows highlight specific areas:

- Business Component:** A red box highlights the 'Buscomp' column header in the table.
- Monitored Changes:** A red box highlights the 'Update', 'New', 'Delete', and 'Copy' columns in the table.
- Monitored Fields:** A red box highlights the 'Field' column header in the lower section, with arrows pointing to the 'User', 'Position', and 'Responsibility' filter options.
- Audit trails can be restricted based on certain user, position, or responsibility filters.** A text box with an arrow pointing to the filter options.

Buscomp	Restriction Type	Update	New	Delete	Copy	Start Date	End Date
Service Request	No Restriction	✓	✓	✓	✓	11/30/2000 6:34:10	
Agreement	No Restriction	✓	✓	✓	✓	12/11/2000 7:32:34	
Order Entry - Orders	No Restriction	✓	✓	✓	✓	12/11/2000 7:34:34	
Order Entry - Line Items	No Restriction	✓	✓	✓	✓		
FS Invoice	No Restriction	✓	✓	✓	✓		
Incentive Compensation Plan	No Restriction	✓	✓	✓	✓	5/2/2001 7:45:54 PM	
Incentive Compensation Component	No Restriction	✓	✓	✓	✓	5/2/2001 7:46:59 PM	

Field
Commit Time
Owner
Priority
Severity
Status

In Siebel 7.0, audit trailing is enabled by default and writes information to the S_AUDIT_ITEM table. An uncontrolled growth of this table can create performance issues. Various methods are available to disable this functionality (see Siebel Alert 0494).