HRMS to CRMOD Data Synchronization

## High Level Design

### Business Overview

The new internal support system is going to have trouble tickets provided by Seibel Customer Relationship Management On-Demand (CRMOD). There is certain pieces of user data that the Human Resources Management System (HRMS) is the owner of. This is information like which department an Oracle employee belongs to. The purpose of this sub-project is to create a link between the HRMS system and the CRMOD system so when user data is updated in HRMS, that same data gets updated in the CRMOD system.

### Technical Overview

The most efficient mechanism to provide the above stated requirements is to create an intermediary process that programmatically pulls the data from HRMS and pushes that data into the CRMOD. This will be a batch process writen in standard J2EE, that uses a JDBC connection into HRMS to pull the required data. Data transformation will occur inside this batch process. Then finally CRMOD web services will be called to insert the data into the CRMOD system.



### Feature Details

#### Full Versus Incremental (Delta) Updates

Initially a full update will be required to populate all the user information in CRMOD. After the initial load, only changes to user information in HRMS need to be propagated to CRMOD. HRMS data has a 'last updated' field that will be used to determine which records need to be processed.

#### Security

It is important, from a security perspective to understand how, when and where HR data is used. There are three areas we must consider. The first is the link between the HRMS system and the batch processor. The second is the link between the batch processor and the CRMOD. And the final place that we must consider is inside the batch processor itself.

The communication to the HRMS system will be over JDBC. This communication will occur only inside the intranet. An application SQL username and password will be used for connecting to the HRMS system. The HRMS system will have a record of the batch processor host that communicates to it and will allow communications only from that particular host.

When HR data leaves the batch processor to go into the CRMOD system it will be done over an encypted channel (https). This communication leaves the intranet, and therefore must be encrypted. It's end point, CRMOD, will be protected by Oracle Corporate SSO. An application identity will need to be created in the Corporate LDAP to fulfill this requirement.

The final place we need to ensure data security is in the batch processor itself. In some corporate systems integrations, intemediary batch files or databases are used for integration. Unfortunately both those antiquated integration techniques introduce additional targets for security breaches. Since the two systems we are integrating to provide interfaces the batch processor can interface with, namely JDBC and Web Services, we can avoid using intermediary batch files or staging databases. All data will be stored in the processes memory, not persisting to any offline storage. When the batch process finished processing a record, it will be removed from memory, and when the process stops running there will be no HR data stored anywhere outside of HRMS and CRMOD.