

## Security and Auditing

### Security

Producing secure software continues to be of paramount importance to CR Software. Software security is a continuous thread throughout our software development lifecycle. Titanium ORE not only addresses the security practices, standards, and protocols that you are being held to today ... but protects your data using the highest standards of security that you will be held to tomorrow and beyond. The many facets of security that Titanium ORE addresses are an investment that will allow you to meet the most stringent security requirements that your organization, your clients, and the law demand.

### Pluggable Authentication

Titanium ORE has the ability to plug in authentication mechanisms. It provides full integration with *Microsoft Active Directory* for enterprise wide logins and passwords that are stored and administered centrally through your *Active Directory* system. Titanium ORE can also authenticate against any JDBC enabled database as well as several other directory server implementations out of the box.

### Granular Authorization

A key security feature of Titanium ORE is the ability to define the user roles for all those needing access. You can define an unlimited number of specific roles for collectors, payment personnel, supervisors, or executives (to name a few). Then you can add specific privileges as required to your personnel roles. Titanium makes use of a declarative authorization model and exposes over 1000 specific privileges that can be either granted or denied based on role associations.

### Masking

Within Titanium ORE, key fields such as credit card, bank account, driver's license, and social security numbers can be masked when they are shown to users without sufficient privileges to see the unmasked version of the data.

### Encryption

All data in transit (network communications between the Titanium client and mid-tier as well as between the mid-tier and database) are encrypted using Transport Layer Security (TLS). The underlying data within the Titanium ORE database can be fully encrypted while at rest. In addition, specific data elements (including passwords) that are deemed extremely sensitive are encrypted at the field level.

### Code Signing

Titanium ORE uses a code signing package to guarantee both the authenticity and integrity of the compiled files that are run from a user's workstation. This ensures that the Titanium ORE client application has not in any way been tampered with by a malicious user or outside attacker.

### Audit Logging

Titanium ORE tracks user and record audit information at the request level and the data instance level to provide robust auditing and traceability throughout the entire system. It can track all changes made to the system as well as the complete history of the changed data over time. Now you never have to worry about being able to backtrack to find out who did what, where, and when ... Titanium ORE provides this information to you.

### Monitoring

Monitoring can be set up on the internals of the Titanium ORE software, on the log output, on the database, on the JMS queues, on the network traffic, on the web servers, and on many aspects of the application server internals (including transaction times, data source management, performance statistics, etc.). These hook points can be used to send alerts and notifications to your IT and management personnel based on the events and information you are interested in.