Market Requirements Document

Feature Name: Code Signing

Version: 1 **Date Submitted:** 03/11/09 **Completed By:** Leon Guzenda

Description of the Problem

Background

Organizations are becoming increasingly concerned with the security of their data and infrastructure. Several customers have expressed concern that Objectivity/DB code, updates and patches arrive without a secure means of verifying that it has in fact come from Objectivity, Inc.

Code signing is becoming an increasingly popular way of ensuring that code is not interfered with en route from the provider to the user. Microsoft Office, Mac OS X and most Linux distributions are protected by code signing.

Definitions

"Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash." - Wikipedia.org.

Problem

Objectivity/DB code, updates and patches are currently distributed without any real means of verifying the true source of the material.

Description of the Requested Feature

1. Support for a digital code signing mechanism, such as a Verisign code signing certificate.

Part of an existing feature or does it require another feature, if so, which one?

1. This is an addition to all existing digital material that we distribute.

How is this problem being solved now, and why isn't that acceptable?

1. It isn't and users are starting to regard this as a potential security vulnerability.

What languages must support this capability?

The capability is independent of languages.

Which platforms must be supported?

- All

Do any competitors already have this feature?

- The major RDBMS vendors already use code signing.

Customers who require this feature

- This was an issue at Fugro-Jason.

Revenue at risk, or which could be won

- There is no imminent risk of revenue loss, however, a security breach caused by interception of an electronic deliverable and the insertion of malware could be very damaging to our reputation.

When is this required?

- Release 10+.

Additional Notes

1. We will also need:

- Updated marketing collateral and a mention on our web site.
- Updated Release Notes.
- New QA material to prove that the mechanism works.

2. Licensing costs are to be determined.

3. **There may be export restrictions** because the mechanism involves data encryption.