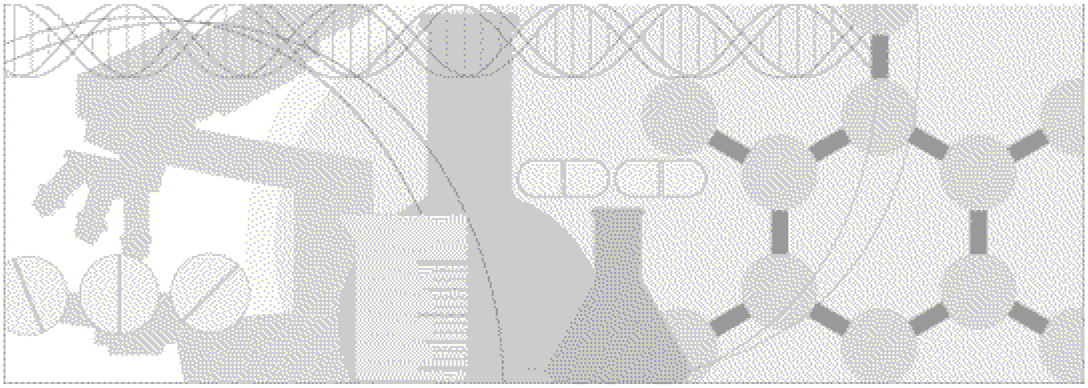
Secure Development Guide

Oracle® Health Sciences InForm Adapter
Release 1.3.9



Part number: E92701-01

Contents

Chapter 1

CHAPTER 1
Secure development for the InForm Adapter

In this chapter

Overview of InForm Adapter secure development

The *Secure Development Guide* provides an overview of the security options provided with the InForm Adapter application that help mitigate some of the common security risks. The recommendations in this document are not exhaustive and there is no guarantee that implementing all the suggestions provides sufficient protection for all security threats, as you cannot delegate responsibility for secure application development to a third party or a single document. This document is to help developers who know the security tools and features that they can use to implement application security. This document does not replace a formal code review process.

The InForm Adapter software provides the following web services that can be called by client applications:

- ODM interface
- Discrepancy interface

Transport layer protection

If your client is calling InForm Adapter web services that are hosted by Oracle, you must use Transport Layer Security (TLS) 1.1 or above to avoid man-in-the-middle attacks. In general, it is more secure to use TLS 1.2 for any client calling the InForm Adapter web services. Web client developers should enforce encrypted data transport when the application transports sensitive data and should validate that all certificates are legitimate and signed by public authorities.

Ciphers should be restricted to modern implementations.

Web service authentication

To address web service client authentication attacks, the InForm Adapter software supports username token and X.509 client certificate authentication. To ensure the integrity of web client authentication, the proper handling of the authentication artifacts should be followed.

The ODM and Discrepancy interfaces support username token authentication. Refer to the *Interfaces Guide* for information on how to invoke the ODM and Discrepancy web services using username token authentication. Make sure you refer to the correct section for the interface you are calling from your client.

To ensure that the web client authentication is secure, the password for the username token should be treated with the utmost care, as password exposure can compromise the authentication mechanisms. The InForm Adapter software does not store the password in clear-text on the file system and does not log the password. As such, the client web service password should be protected in the same fashion. The password should always be stored in an encrypted form. To reduce password exposure during password exchange, do not transfer the password through unencrypted side channels between web service endpoint parties. The authentication of each side channel endpoint is also a concern during the password exchange and is open to social engineering attacks if not done properly.

The Discrepancy Enhanced interface and ODM Export interfaces also support X.509 certificate authentication. The client application must sign the message with the X.509 private certificate and the public X.509 certificate must be installed on the InForm Adapter application server. The X.509 Certificate Authentication is based on the signature generated from the SHA256 signature algorithm. For the X.509 certificate authentication, a trusted public certification authority (CA) should be used to validate the legitimacy of the organization controlling the web service client endpoint. The use of a trusted public CA reduces the chances of social engineering attacks based on username token password handling. Public CAs provide different levels of organization checks, depending on the costs of their services. More organization checks ensure fewer chances of a social engineering attack.

For examples on how to sign the message with an X.509 certificate, see the ODM Sampler's source code: SignXml method in \certificate\MyClientMessageInspector.cs.

SQL injection

SQL injection issues occur when an SQL query is built using input from an untrusted source. This could allow an attacker to modify an SQL statement or to execute dangerous SQL commands.

The InForm Adapter interface web service uses bind variables and does not dynamically generate SQL, which makes SQL injection impossible.

XML injection

XML injection issues occur when the data used to construct XML code, which may contain XML metacharacters, is not encoded properly. The InForm Adapter software handles this by using standard XML processing components that construct the XML documents. It is recommended that the client code also uses standard XML processing components to ensure that data is properly encoded. If XML is constructed manually, the developer should ensure that any untrusted data is properly encoded to prevent XML injection.

Secure misconfiguration

Consult the *Secure Configuration Guide* to ensure the product API is locked down appropriately.

About the documentation

Where to find the product documentation

The product documentation is available from the following locations:

- My Oracle Support (https://support.oracle.com)—Release Notes and Known Issues.
- Oracle Help Center (https://docs.oracle.com)—The most current documentation set.

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc).

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support or Support Cloud. For information, visit ***http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs*** or visit ***http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info*** if you are hearing impaired.