Application Integration Architecture: Agile PLM PIP for Oracle E-Business Suite

Security Guide

Release 3.5

E72741-01

March 2016

ORACLE

Application Integration Architecture: Agile PLM PIP for Oracle E-Business Suite Security Guide, Release 3.5

E72741-01

Primary Author: Oracle Corporation

Contributing Author: Edlyn Sammanasu

Contents

Preface

The integration between Agile PLM and Oracle E-Business Suite is designed to enable the product development process, as well as address the primary use cases around the synchronization of product content information between Agile Product Collaboration and Oracle Manufacturing.

Audience

This document is intended for administrators of the Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite: Design to Release.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at 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. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

Oracle's Agile PLM PIP for Oracle E-Business Suite documentation set includes Adobe® Acrobat PDF files. The Oracle Technology Network (OTN) Web site http://www.oracle.com/technetwork/documentation/agile-085940.html contains the latest versions of the Agile PLM PDF files. You can view or download these manuals from the Web site, or you can ask your Agile administrator if there is an Agile PLM Documentation folder available on your network from which you can access the Agile PLM documentation (PDF) files.

Conventions

The following text conventions are used in this document:

- **AIA**: Application Integration Architecture
- **Agile (PLM)**: Agile Product Lifecycle Management
- **EBiz**: E-Business Suite

- **Agile PIP for EBiz**: Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Document Scope

This document provides Oracle Agile PIP for EBiz administrators with the information needed to understand Agile PIP for EBiz security.

Documentation Audience

This document is written for IT users and Oracle Agile PIP for EBiz administrators who will be setting up Oracle Agile PIP for EBiz. It is assumed that those reading this documentation have a solid understanding of security concepts. The audience should also have basic knowledge of Oracle Agile PIP for EBiz.

Guide to this Document

This guide provides information needed to help you to understand Oracle AIA Agile PLM for Oracle EBS security.

The guide is organized as follows:

- "Understanding Security for Agile PIP for EBiz" on page 2-1 gives an overview of security fundamentals related to Agile PLM for EBiz.
- "Security Implementation for Agile PIP for EBiz" on page 3-1 provides the necessary details on how to implement security for Agile PIP for Ebiz.

2

Understanding Security for Agile PIP for EBiz

This chapter describes the fundaments of security related to Agile PIP for Ebiz.

Agile PIP for EBiz Overview

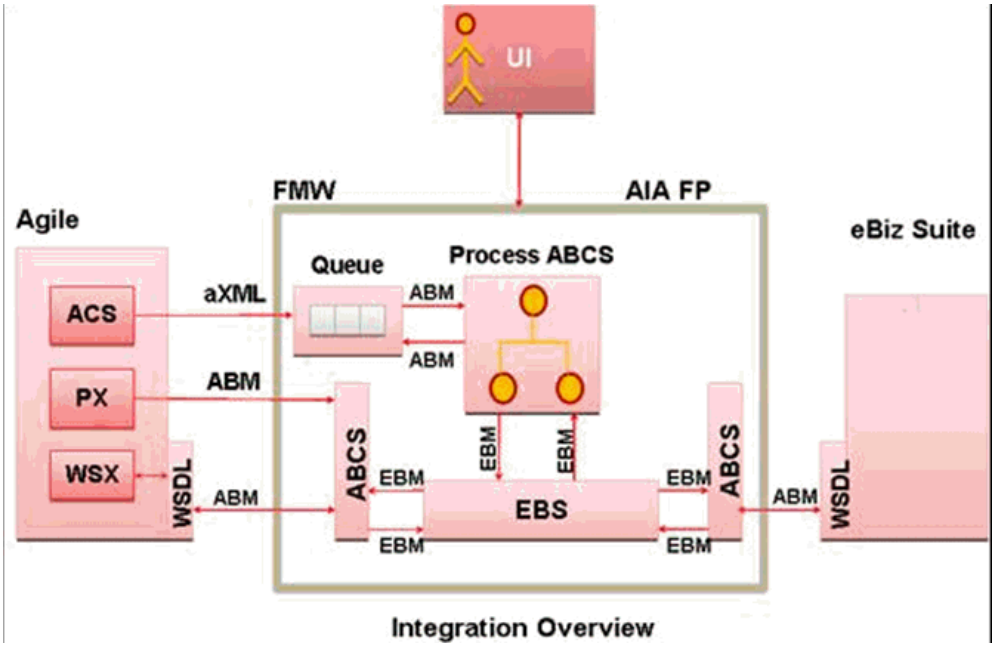
The integration between Agile PLM and Oracle E-Business Suite is designed to enable the product development process and address the primary use cases around the synchronization of product content information between Agile Product Collaboration and Oracle Manufacturing. This allows for rapid implementation of Oracle's next-generation integrated enterprise PLM processes that help the customers reduce costs and any risks associated with typical third-party and custom integrations.

The Agile PLM pre-built integration for Oracle E-Business Suite includes the following functions:

- Manufacturing release of new product definition and product launch.
- Change management of previously launched products.
- Bidirectional synchronization of engineering change status and material attribute information from Oracle Manufacturing to Agile PLM.
- Monitoring and control of the change processing and validation queues.

Figure 2–1 illustrates the Agile PLM to Oracle E-Business Suite integration architecture.

Figure 2–1 Agile PLM Business Process Flow



For more information, see the *Oracle Application Integration Architecture Agile Product Lifecycle Management Integration Pack for Oracle E-Business Suite: Design to Release Implementation Guide*.

Introduction to Security

Agile PIP for EBiz is based on the Foundation Pack. The Foundation Pack is a part of the AIA framework, so AIA security can be applied to Oracle Agile PIP for EBiz.

AIA provides support for all security-related functions including:

- Identification
- Authentication (verification of identity)
- Authorization (access controls)
- Privacy (encryption)
- Integrity (message signing)
- Non-repudiation
- Logging

The service-oriented architecture (SOA)-based integration approach allows for clear separation between the interface and the actual business logic. This provides the security architect with a number of choices in deploying security for SOA and web services.

For example, a SOAP web service interface, such as ProcessEngineeringChangeOrderAgileReqABCS, can be hosted as a proxy instead of the real endpoint that hosts the business logic implementation. The gateway proxies communication to and from the web service, and performs security functions on behalf of the service endpoint. The actual endpoint is virtualized. Even though the

client thinks it is talking directly to the service provider, it communicates through the proxy.

Service-to-Service Security

Because a typical interaction in the Oracle AIA framework is part of multiple discrete interactions involving a service requester, client-specific Application Business Connector Service (ABCS), Enterprise Business Service, server-specific ABCS and the service provider, choosing a security model plays a critical role.

Oracle AIA architecture enables you to choose one over the other at the implementation time for each of the transactions.

Adoption of the industry-standard WS-Security security model is possible, provided that all participating applications in the transactions provide inherent support.

Transport-Level Security

Existing technologies such as SSL can be used to secure the transport channel. SSL enables two applications to securely connect over a network and authenticate each other. It also enables you to encrypt the data exchanged between the applications. In Oracle's Web Services Security model, this transport security mechanism can be used to provide point-to-point security, data integrity, and data confidentiality.

See *Fusion Middleware Concepts and Technologies Guide for Oracle Application Integration Architecture Foundation Pack* for more information.

Message-Level Security

Oracle AIA places strong emphasis on message-level security. For a web service, XML encryption provides security for applications that require a secure exchange of data. While SSL was considered the standard way to secure data exchanges, it has limitations. For example, assume that a document visits several web services before hitting its eventual endpoint. By using XML encryption, the document can be encrypted while at rest or in transport. Encrypting only portions of a document instead of the whole document is also possible.

Oracle AIA leverages web service administration tools such as Oracle Web Services Manager (OWSM) in a non-intrusive manner to ensure the validity, as well as safety, of the XML messages exchanged between services. This methodology ensures that no enforcement of web services security is in silo mode. Integration architects and developers can focus on integration logic, and the security architects and administrators can focus on security and management. Having security policies enforced through a centralized tool enables the administrators to ensure that the corporate rules are applied, as well as to apply the policy changes centrally instead of applying them in each of the web services.

A typical web service security can have multiple policies attached that can:

- Decrypt the incoming XML message
- Extract the user's credentials
- Perform an authentication for this user
- Perform an authorization check for this user and this web service
- Write a log record of the preceding information
- Pass the message to the intended web service, if all steps are successful

3

Security Implementation for Agile PIP for EBiz

This chapter gives a general picture of PIP security, and describes how PIP security interacts with Agile and Ebiz Web Services.

Overview of PIP Security

The AIA framework provides the following methods to secure the service-to-service interaction:

- Identify clients through authentication.
- Secure messages through encryption.
- Avoid message tampering with digital signatures.
- Encrypt the channel through SSL.

Figure 3–1 High-level Security Architecture

Agile PIP for EBiz 3.5 is shipped with this security implemented, except SSL, which needs manual configuration. OWSM already helps PIP to implement the security methods, and OWSM provides multiple policies to protect web services. The following sections focus on which policies are used in Agile PIP for Ebiz, and how to operate with Agile/Ebiz security.

PIP Security Policy

Since PIP is based on the AIA framework, all AIA policies can be used by PIP. The following is a list of policies which are used in Agile PIP for EBiz:

- Global Service Policy applied:

  oracle/aia_wss_saml_or_username_token_service_policy_OPT_ON - This is a cloned copy of oracle/wss_saml_or_username_token_service_policy with Local

Optimization set to ON. This is needed for local optimization to work when both client and service composites are co-located.

- Global Service Client Policy applied:

  oracle/aia_wss10_saml_token_client_policy_OPT_ON

- Other Service Policies applied:
  - oracle/aia_wss_saml_or_username_or_http_token_service_policy_OPT_ON - This is a cloned copy of oracle/wss_saml_or_username_token_service_policy with Local Optimization set to ON and HTTP basic authentication added as an additional option. Clients such as ODI that do not have the infrastructure to use web services security can call this service using HTTP basic authentication.
  - oracle/no_authentication_service_policy - The oracle/no_authentication_service_policy policy is to those services that do not need authentication.
- Other Service Client Policies applied:
  - oracle/aia_wss_saml_or_username_or_http_token_service_policy_OPT_ON
  - oracle/aia_wss10_saml_token_client_policy_OPT_ON
  - oracle/wss_username_token_client_policy
  - oracle/wss_http_token_client_policy

Interoperability with Agile Web Service Security

Agile 9.3.4 and 9.3.5 provide a tool to enable security for Web Services in running time. Refer to the *Agile Product Lifecycle Management Security Guide* and follow the steps to enable/disable the security for Agile PLM web services.

When interacting with an Agile web service that is enabled for WS-security, you must add a security header in the SOAP header with all the information needed for security functions. Based on the security of the Agile service, you must add information for any combination of authentication, encryption and integrity. The following table lists the certified policies:

Table 3–1 Certified Policies

Composite Name	Service Name	Certified Policies
ProcessEngineeringChangeOrderAgileReqABCSImpl	ChangeABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
ProcessItemListInitialLoadAgileABF	BusinessObjectService ItemABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
SyncBillOfMaterialsConfigurationListAgileProvABCSImpl	ConfiguratorTerminationService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy

Table 3–1 (Cont.) Certified Policies

Composite Name	Service Name	Certified Policies
UpdateEngineeringChangeOrderListAgileProvABCSImpl	ChangeABSService ChangeStatusService MergeABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
UpdateItemBalanceListAgileProvABCSImpl	ItemABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
UpdateItemListAgileProvABCSImpl	ItemABSService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy
ValidateEngineeringChangeOrderListAgileReqABCSImpl	ChangeABSService TableService	oracle/wss_http_token_client_policy oracle/wss_username_token_over_ssl_client_policy

Note: The out-of-box policy for Agile web services is oracle/wss_http_token_client_policy. If you are running Agile PLM in a non-Web Services Security environment, the Web Services Security Configurator does not need to be run. For more detailed steps, refer to the *Oracle AIA Agile PLM for Oracle EBS: Design to Release Install Guide*.

Interoperability with Ebiz

When interacting with an EBiz web service that is enabled for WS-security, you must add a security header in the SOAP header with all the information needed for security functions. Based on the security of the EBiz service, you must add information for any combination of authentication, encryption and integrity. The following table lists the certified policies:

Table 3–2 Certified Policies

Composite Name	Service Name	Certified Policies
GenerateItemNumberService	GenerateItemNumberService	oracle/wss_username_token_client_policy

Note: The out-of-box policy for EBiz web services is oracle/ wss_username_token_client_policy.