IBM® Workplace Forms™

Version 2.6.1

IBM Workplace Forms and Entrust Integration Guide

S325-2599-00

Note
Before using this information and the product it supports, read the information in "Notices," on page 7.

First Edition (September 2006)

This edition applies to version 1, release 2.6.1 of Workplace Forms and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces version 1, release 2.6 of Workplace Forms.

Contents

IBM Workplace Forms and Entrust Integration Guide

This document is intended to assist system administrators with integrating Workplace Forms™ with an Entrust infrastructure. Before attempting to carry out any integration, you should read this document thoroughly, determine which steps you need to perform, and ensure you have the appropriate software on hand.

This document assumes that the reader has an existing Entrust infrastructure and is familiar with the Entrust products and tools.

About the Integration

The Workplace Forms™/Entrust integration has the following goals:

1. To allow users to sign and verify forms with Entrust signatures.
2. To allow Entrust TruePass to secure both forms and form-processing applications.

In general, an integration impacts both the client and server components of your network, as follows:

Client side — Your users need both Workplace Forms Viewer and Entrust Entelligence installed on their computers. The Viewer allows users to view and complete forms, while Entrust Entelligence enables them to use Entrust signatures.

Server side — Forms are generally processed by a server-side application, such as a CGI script or a Java™ servlet. These applications are written using the Workplace Forms Server - API, which provides all of the functionality required to read and work with XFDL documents. However, the application also requires access to a server profile that it can use when working with Entrust signatures. Additionally, you can use Entrust TruePass to secure both the application and any forms that are stored on the server.

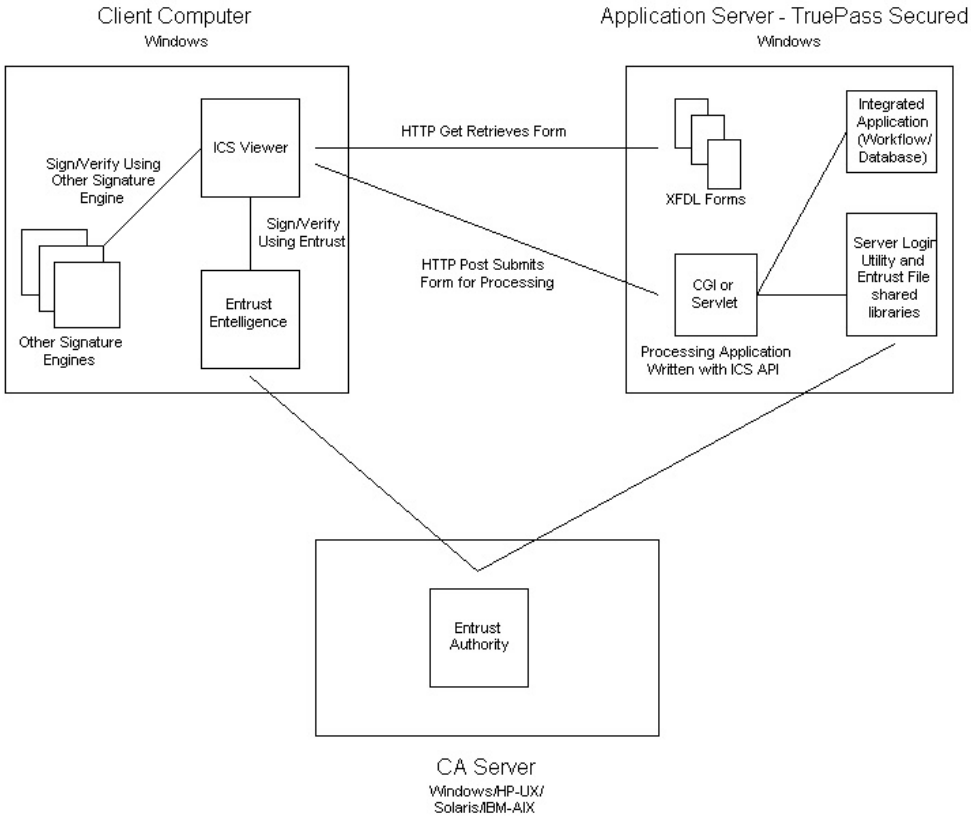
Steps to Integration

The following table lists the steps that are required for a typical integration and refers you to the page that describes that step:

Step	Section
Familiarize yourself with the typical system architecture	"System Architecture" on page 2
Create forms that use Entrust signatures.	"Creating Forms that Use Entrust Signatures" on page 3
Develop a server-side application that processes the forms.	"Developing a Server-Side Application that Processes Forms" on page 3
Set up your server to work with Entrust signatures.	"Working With Entrust Signatures on a Server" on page 4
Secure your application server with Entrust TruePass.	"Securing Your Application Server With Entrust TruePass" on page 6
Distribute the Viewer to your users.	"Distributing the Viewer to Your Users" on page 6

System Architecture

The following diagram illustrates a typical Workplace Forms/Entrust integration:



System Overview

A typical system contains three components:

Client Computer —Each client computer has the Viewer and Entrust Entelligence installed. Users retrieve, complete, sign, and submit forms from client computers.

Application Server —The application server contains the blank forms that users retreive and complete, the application that processes the forms, and a number of Entrust components that allow the application to work with Entrust signatures. Additionally, the application server may use Entrust TruePass to secure both the forms and the form-processing application.

CA Server —- The CA server contains a working installation of Entrust Authority, which both the client computers and the application server use when working with Entrust signatures.

A Typical Processing Scenario

In a typical scenario, a user works on a client computer in a web browser. The user first connects to the application server and opens a blank form in their Viewer by clicking a link to the appropriate form. Next, the user fills out the form and applies a signature. During the signing process, the Viewer relies on fuctionality provided by Entelligence, which communicates with Entrust Authority on the CA Server. Finally, the user submits the form for processing.

When the application server receives a completed form, it directs the form to the appropriate application. The application then reads the form and verifies the signature. During verification, the application relies on the Entrust File shared libraries and Server Login Utility to communicate with Entrust Authority on the CA Server and carry out the verification process. Once Entrust verifies the signature, the application proceeds. For example, it may simply archive the form in a database, or it may forward the form to a workflow process.

Securing Your Application Server with Entrust TruePass

If you choose to secure your application server with Entrust TruePass, your users will have to login to TruePass before they can access the protected resources on the application server. These resources may include both the blank forms and the form-processing application.

The authentication process places a sessional cookie in the user's browser. Once this cookie is in place, the user is free to open or submit forms. However, if the user attempts to open or submit a form before logging in, one of the following scenarios will occur:

- **Retrieving forms before logging in** —If users attempt to retrieve a secured form before logging in, TruePass redirects them to a login page. Once they have successfully logged in, TruePass redirects them to the form that they originally tried to retrieve.
- **Submitting forms before logging in** —If users attempt to submit a form before logging in, TruePass redirects them to a login page. In this case, the original submission is lost and they must resubmit the form once they have successfully logged in.

Creating Forms that Use Entrust Signatures

Users sign forms by clicking signature buttons in the form. Forms can contain any number of signature buttons, just like a paper document can require any number of signatures. Each signature button is configured to use a particular signature engine. For example, one button might use the generic RSA engine while another button might use the Entrust engine.

To ensure your users sign your forms with Entrust signatures, you must configure each signature button to use the Entrust signature engine. There are two ways to do this:

- If you are using Workplace Forms Designer to create your forms, you can simply choose which engine to use in the appropriate dialog. For more information, refer to the Designer Help.
- If you are creating your forms in a text editor, you must add the appropriate XFDL options to each signature button. In general, this includes setting the button's signformat option to use a MIME type of **application/vnd.xfdl** and the **Entrust** engine.

Developing a Server-Side Application that Processes Forms

To develop a form-processing application, you must use Workplace Forms API. The API provides a tool set that you can use to work with XFDL forms.

Form-processing applications are usually specific to each organization. For example, you might want an application that simply verifies the signatures in a form and then archives the form in a database. Optionally, you might want to

parse all of the data out of the form and populate one or more tables in that database, or pre-populate forms with information from the database.

Regardless of your specific application, you can use the API to read forms, extract information from them, verify signatures, and so on.

The API is available in C, Java, and COM development environments. For more information about installing and using the API, refer to the *IBM® Workplace Forms Server - API: Installation and Setup Guide*.

Once you have developed an application, copy it to your application server.

Verifying Entrust Signatures on the Server

To verify Entrust signatures, use the standard VerifySignature function provided in the API. This function works for all signature types.

Note: Before you can verify an Entrust signature on a server, you must first configure the server appropriately. See "Working With Entrust Signatures on a Server" for more information.

Working With Entrust Signatures on a Server

Once you have copied your form-processing application to your application server, you must configure the server to use a specific Entrust profile when working with signatures. This requires you to:

- Create an Entrust profile that the API can use to work with Entrust signatures.
- Set up Entrust software on your application server that will enable the API to access a server profile and communicate with Entrust Authority.

Requirements

The following setup assumes that you have three computers available to you:

1. **Client Computer** —This computer has a working Entrust Entelligence installation that is configured to work with your CA Server.
2. **Application Server** —This server runs your the API application.
3. **CA Server** —This server has a working Entrust Authority installation.

In addition, you will need the following software:

- **Entrust Server Login Utility** —You will install this on your application server. This package contains the Binder utility, which you will use to bind the server to a particular profile.
- **Entrust File Toolkit** —You will install this on your application server and copy certain files to your application directory.

Set Up Instructions

Setting up Entrust requires that you install and work with certain Entrust components. Then you must configure the API to access the correct Entrust certificate.

Please refer to the documentation that came with your Entrust products as necessary.

Setting Up Entrust on Your Server

Follow these steps to configure your application server to work with Entrust signatures:

1. Ensure that you have a working Entrust Authority installation (your CA server).
2. Using Entrust Authority, create a profile for Server Login use.
   - Be sure that the assigned user policy has the ″Permit Server Login usage″ policy attribute checked.
3. Copy the entrust.ini file from your client computer to the following directory on your application server:
   - /WINNT/
4. Copy the profile that you created on your CA server to the default Entrust Profile directory on your application server.
   - You may need to create this directory. You can check the entrust.ini file to determine the correct location for this directory.
5. Install the Entrust File Toolkit on your application server.
6. Copy the shared libraries (entapi32.dll, etfile32.dll, and enterr.dll) from your Toolkit installation to the following directory:
   - Under C, the directory in which you placed your the API application.
   - Under Java, the directory in which Java is installed.
7. Install the Entrust Server Login Utility on your application server.
8. Run the Entrust Binder that was installed as part of the Entrust Server Login Utility.
   - This binds the profile you created to the server, ensuring that the server is alway logged in with that profile.

Configuring the API to Use an Entrust Profile

You must make a configuration setting so that the API will know which Entrust profile to use. The steps for this vary depending on which version of the the API you are using.

If you are using the Workplace Forms Server API version 2.5 or later::

1. Locate the appropriate copies of the prefs.config file. This file may exist in the in the following directories:

   ```
   c:\Documents and Settings\<username>\Application Data\PureEdge\
         API x.x\Prefs\prefs.config
   c:\Documents and Settings\All Users\Application Data\PureEdge\
         API x.x\Prefs\prefs.config
   ```

   You only need to update the prefs.config files for profiles that will run the API with Entrust.
2. Open each configuration file in a text editor, and set the entrustProfile tag to equal the name of the profile you want the server to use. For example, if you wanted the server to use a profile called ″Server″, you would use the following setting:

   ```
   entrustProfile = Server
   ```

If you are using the PureEdge-Branded API version 6.0 or later::

1. Locate the appropriate copies of the prefs.config file. This file may exist in the in the following directories:

```
c:\Documents and Settings\<username>\Application Data\PureEdge\
      API x.x\Prefs\prefs.config
c:\Documents and Settings\All Users\Application Data\PureEdge\
      API x.x\Prefs\prefs.config
```

You only need to update the prefs.config files for profiles that will run the API with Entrust.

2. Open each configuration file in a text editor, and set the entrustProfile tag to equal the name of the profile you want the server to use. For example, if you wanted the server to use a profile called ″Server″, you would use the following setting:

```
entrustProfile = Server
```

If you are using a version of the PureEdge-Branded API earlier than 6.0::
Create the following environmental variable on your application server:

- For **Variable Name**, use **PE_ENTRUST_PROFILE**.
- For **Variable Value**, use the path to the profile you created (for example, c:\Entrust Profile\ServerVerify.epf).

Securing Your Application Server With Entrust TruePass

You can use Entrust TruePass to secure both blank forms on your site and any form-processing applications, as follows:

- To secure your forms, place them in a TruePass secured directory on your application server.
- To secure form-processing applications, list them in the TruePass .ini file.

For detailed instructions, refer to your Entrust documentation.

Distributing the Viewer to Your Users

Before your users can work with the forms on your application server, they must install Workplace Forms Viewer. They will also require Entrust Entelligence for signing if they do not already have it.

For more information about installing and using the Viewer, refer to the *IBM Workplace Forms Viewer User's Manual*.

Note: You can simplify the distribution and maintenance of the Viewer by using Workplace Forms Deployment Server (IDS). IDS allows you to automate the distribution process by downloading and installing the Viewer through the user's web browser.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Office 4360
One Rogers Street
Cambridge, MA 02142
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
IBM
Workplace
Workplace Forms

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Program Number:

Printed in USA

S325-2599-00