Integration Guide

iPlanet BillerXpert 4.6 B2B Edition / Identrus Trustbase

May 2002

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

CETTE DOCUMENTATION EST FOURNIE “EN L'ÉTAT”, ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

About This Document

The *iPlanet BillerXpert B2B Edition / Identrus Trustbase Integration Guide* describes how to integrate iPlanet BillerXpert B2B Edition with the Identrus Trustbase application for the purpose of an additional authentication mechanism. It also lists the system requirements and describes the preinstallation and postinstallation tasks that you must perform to ensure a successful installation.

This preface contains the following sections:

- Audience
- What's in This Document
- Documentation Conventions
- The Document Online
- Related Documentation
- Product Support

Audience

The audience for this document is system administrators who will install and configure the BillerXpert product. The system administrator will be responsible for maintaining the various servers and will also need to have access to root user ID and some experience with UNIX administration as the root user. You must have access to the iPlanet Application Server (iAS) documentation:

```
http://docs.iplanet.com/docs/manuals
```

You need to use this manual if you are integrating BillerXpert with Identrus Trustbase authenication services.

Before You Begin

This guide is written with the assumption that you have an understanding of relational databases and the operating system on which you are running this software. The documentation is also written with the assumption that you have some basic background including:

- a general understanding of the Internet and the World Wide Web
- experience in setup and management of web services
- experience in setup and administration of relational databases

In addition to the documentation provided by iPlanet, you may find it helpful to read and review:

- your operating system manuals
- your relational database manuals

Required Documents

When integrating BillerXpert, you may need to refer to the *iPlanet Web Server Plug-in for Trustbase Services Install, Configuration and Developer Guide* for information about setting up the web server.The document can be found online at: `http://docs.iplanet.com/docs/manuals`

You will also need to have read or have available the following iPlanet Application Server (iAS) documents:

- *iAS Java Programmer's Guide* — Provides background information about using the iAS programming constructs upon which BillerXpert was developed. `http://docs.iplanet.com/docs/manuals`

What's in This Document

The following table summarizes what each section in this book covers.

Table 1 Content Summary

If you want to know about this	See this section
Describes the contents of this guide; listing of documentation set; information on product support.	"About This Document"

Table 1 Content Summary

If you want to know about this	See this section
Provides general information about Identrus, including how iPlanet has integrated other products with this application.	"Introduction to Identrus"
Provides information and guidelines for using Identrus as an additional authentication mechanism, including the architecture for BillerXpert and Identrus.	"Authentication"
Provides information on the cookie generator, including how the cookie is generated and the format of the cookie.	"Cookie Generator"
Provides information on how the certificate is mapped and how the users and roles are defined.	"Identity Mapping"
Provides information in the form of a diagram which describes the login flow process for authentication.	"Login Flow"
Describes the setup instructions for integrating BillerXpert and Identrus, including: • System Requirements • Web Server Plug-in • Configuration	"Setup Instructions"

Documentation Conventions

This document uses the following conventions:

- The `monospace` font is used for sample code and code listings, Application Program Interface (API) and language elements (such as method names and property names), file names, commands, path names, directory names, Hypertext Markup Language (HTML) tags, and any text that must be typed on the screen.
- The *italic* font is used in code to represent placeholder parameters (variables) that should be replaced with an actual value, or items that require *emphasis*.
- Brackets ([]) are used to enclose optional parameters.
- A slash (/) is used to separate directories in a path. (Windows NT supports both the slash and the backslash.)

The Document Online

An electronic version of this document and its accompanying release notes are available at:

```
http://docs.iplanet.com/docs/manuals/
```

Related Documentation

The BillerXpert documentation set includes:

- *Release Notes*—Contains important information on the current release of BillerXpert. Read this document before working with the new BillerXpert release.
- *Administrator's Guide*—Provides reference information and instructions on administering a fully-installed BillerXpert system.
- *Installation Guide*—Provides instructions for installing the BillerXpert product and its enabling software.
- *Customization Guide*—Provides guidelines and instructions for customizing the BillerXpert system.

Documentation for all iPlanet products can be found at the following web site:

```
http://docs.iplanet.com/docs/manuals/
```

Product Support

If you have problems with your BillerXpert system, contact iPlanet customer support using one of the following mechanisms:

- iPlanet online support web site at:

  ```
  http://www.iplanet.com/support/online/
  ```

  From this location, the CaseTracker and CaseView tools are available for logging problems.

- The telephone dispatch number associated with your maintenance contract

So that the technical support staff can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

Integrating Identrus and BillerXpert

This guide will help you to understand the process of integrating the iPlanet BillerXpert and Identrus Trustbase applications. In this scenario, Identrus Trustbase is being added as an additional authentication mechanism.

This guide contains the following sections:

- Introduction to Identrus
- Authentication
- Cookie Generator
- Identity Mapping
- Login Flow
- Setup Instructions

Introduction to Identrus

Identrus is a scheme based on Public Key Infrastructure (PKI) that can be used to perform authentication, authorization, and non-repudiation. It is based on a private Certificate Authority (CA) scheme and has been developed by multiple business partners with a strong emphasis on B2B product integration.

iPlanet has previously taken steps to integrate Identrus into their products, most notably, the iPlanet Portal Server and the iPlanet Web Server. The BillerXpert B2B Edition product has been integrated with Identrus, beginning with the authentication feature. This document will explain the integration of iPlanet BillerXpert and the authentication application.

For information regarding the Web Server & Identrus integration, please refer to the *iPlanet Web Server Plug-in for Trustbase Services Install, Configuration and Developer Guide*. The document can be found online at: `http://docs.iplanet.com/docs/manuals`

Authentication

Identrus authentication is performed by the web server component. The iPlanet Web Server (iWS) plug-in for trustbase authentication provides a means to authenticate a user to the Identrus system. The details of installing and setting up the plug-in is described in the *iPlanet Web Server Plug-in for Trustbase Services Install, Configuration and Developer Guide*. The documet can be viewed online at `http://docs.iplanet.com/docs/manuals`

BillerXpert B2B Edition treats Identrus as an additional authentication mechanism, supporting three types of authentication:

- Userid Password
- Client Certificate Authentication
- Identrus Authentication

Identrus Authentication

Identrus Authentication is performed between the client (browser) and Identrus via the HTTPS channel. The browser may be optionally authenticated using SSL client authentication (browser/client certificificate), however, this is not a typical requirement.

Identrus authentication will be provided by the Identrus Integration project with the iPlanet Web Server. To perform identrus client authentication using certificates, the additional system requirements are as follows:

- The browser needs a smart card plug-in reader
- The browser needs a smartcard with a valid Identrus certificate on it.

NOTE For information on obtaining an Identrus certificate, please refer to `http://www.identrus.com`.

As a result of successful Identrus authentication, a cookie generator will be called to issue a cookie to the browser. The cookie generator generates and sends back a cookie to the redirect URL. The description of the cookie is discussed in the next section, Cookie Generator.

Once the cookie is generated, the client is redirected to the URL from which it came from. Both Process Manager and BillerXpert will map the Identrus identity (certificate DN, certificiate Serial Number) to a BillerXpert identity. Upon successful mapping, a BillerXpert / Process Manager authentication cookie will be re-issued and will contain the BillerXpert identity. On subsequent requests, the cookie will be verified and used until it's expiration date. When it expires, the user will be forced to sign on via Identrus again at which point the process will repeat.

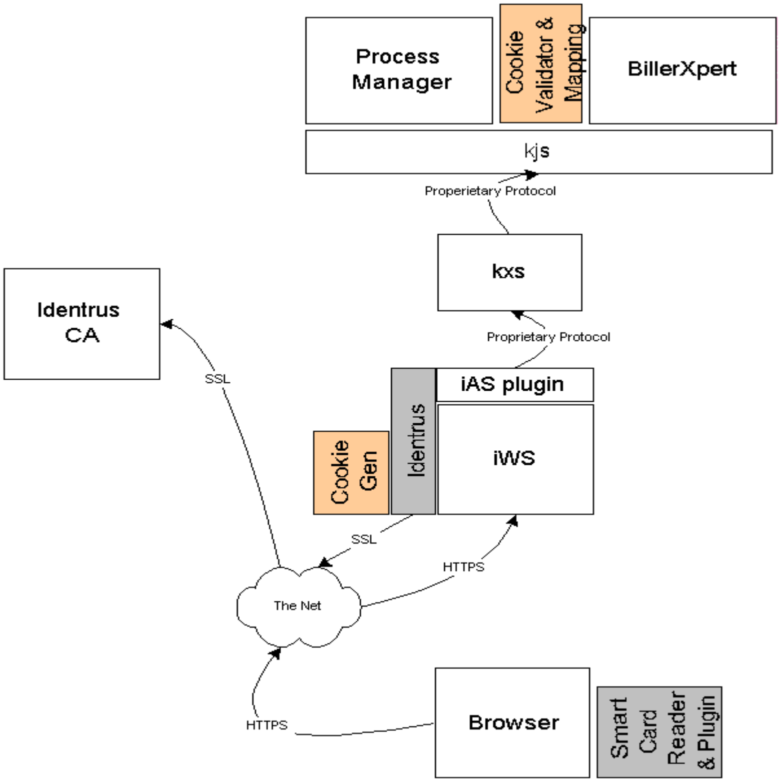

Figure 1 BillerXpert / Identrus Architecture

The grey areas in Figure 1 represent components which are delivered by the Identrus Integration:

- Identrus
- Smart Card Reader and plug-in

The tan areas represent the components which BillerXpert must supply in order to work with the Identrus scheme:

- Cookie Validator and Mapping
- Cookie Generator

Cookie Generator

The `com.netscape.security.AuthToken` class is used to generate the cookie. This is already used by the BillerXpert / Process Manager login mechanism; the class is able to generate an HTTP cookie from a key/value pairs of data, attach an expiration date, and checksum the cookie. The format of the cookie data is described in Table 2:

Table 2 Cookie Format

Component	Key	Data	Description
Data	certificate	<Identity cert>	Base 64 encoded identity certificate
	Type	Identrus	
	issuerDN	<issuer DN>	
	serialnumber	<identrus certificate serial number>	
	subjectDN	<subject DN>	
Validity	_e	<expiration date of this cookie>	The expiration value of this cookie; should be short (i.e.: 1 or 2 minutes)
	_m	<checksum of data>	The MD5 checksum of the cookie

Both Process Manager and BillerXpert are able to identify this cookie and map the passed Identrus identity to a BillerXpert user.

Identity Mapping

The certificate is mapped to a user in LDAP. An attribute (nsCertificate) is defined for the userProfile, which keeps the user DN and serial number from the certificate. If the certificate is mapped in LDAP, then BillerXpert logs in as the user. The actual authentication is performed by Identrus, via the web server plug-in. Once the user is logged in, everything works as before: ACL are assigned based on BillerXpert users and roles. BillerXpert LDAP is consulted for group membership of that user, etc.

Login Flow

Figure 2 depicts the authentication process flow.

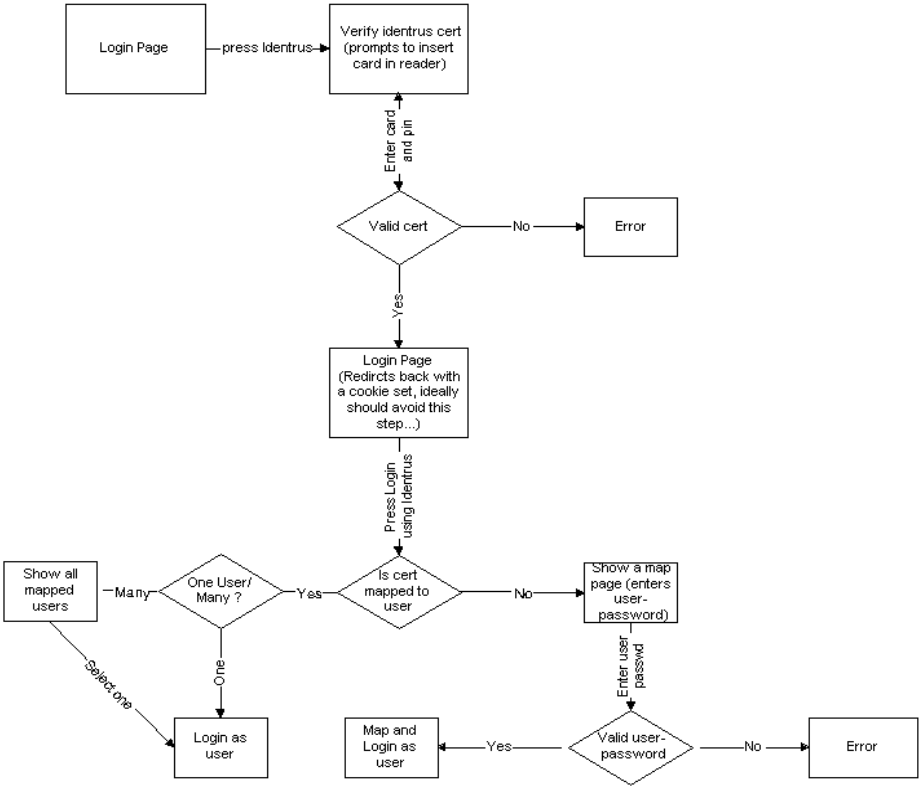

Figure 2 Login flow diagram for Identrus

Setup Instructions

System Requirements

The system requirements in addition to those of BillerXpert B2B Edtion, are that you must have a Smart Card Reader.

Web Server Plug-in

Please refer to the *iPlanet Web Server Plug-in for Trustbase Services Install, Configuration and Developer Guide* for information on how to set up the web server plug-in. The document can be found online at:
`http://docs.iplanet.com/docs/manuals`

Configuration

The following configuration setup should be performed following the installation of the web server plug-in:

1. Modify `authservlet.properties` in your web server instance config directory:

    - set CookieGenerator=BillerXCookie (in AuthServlet section, should be set by default)
    - set CookieGenerator=`com.netscape.security.BillerXCookieGenerator` (in CookieGeneratorFactory section, should be set by default)
    - set `BillerXCookie.Property`=Domain=DOMAIN

      For example, `red.iplanet.com`

2. Modify `$BX_HOME/java/billxb2b.conf`

    - set authentication_url to something like this:
      "`https://HOST.DOMAIN:PORT/errors/certificate_nouser.jsp?redirectFile=`"

This is the url to the web instance on which you installed plug-in.

- set `identrus_switch` as ON (by default).

  This switch enables/disables identrus at system level.

3. In LDAP, click your biller name, set values of attribute `nsLoginOption` to any combination of USERID-PASSWORD, SSL-CA, IDENTRUS. This can also be done through the admin front end, in biller profile. The biller can setup the login options that can be available to its customers.

4. An additional step that needs to be performed for SSL communication:

   - Change the `EventServerProperties.conf` file and set up the following:
     - keyStore=KeyStore file
     - keyStorePassword=KeyStore password
     - debug=no

Please refer to `http://java.sun.com/products/jsse/index-102.html` for information on setting up SSL communications.